Trust Evaluation in Computer Networks Based on Machine Learning Methods

1st Yusuf Alptigin Gün
Computer and Informatics Engineering
Istanbul Technical University
Istanbul, Turkey
gun18@itu.edu.tr

2nd Emine Darı
Computer and Informatics Engineering
Istanbul Technical University
Istanbul, Turkey
dari18@itu.edu.tr

3nd Şule Beyza Karadağ
Computer and Informatics Engineering
Istanbul Technical University
Istanbul, Turkey
karadagsu18@itu.edu.tr

***Abstract*—The use of computer networks have risen substantially with the improvements of technology. Simultaneously, this surge in network utilization has made these networks more susceptible to malicious attacks. Given the vast amounts of data inherited in these networks, security of these networks have become an important topic for discussion. In order to handle these threats, various machine learning methods have been proposed. In this paper, we describe what trust evaluation is and outline traditional and machine learning based methods. We also provide a review of machine learning based methods on three different topics; namely OSNs, VANETs and IoT. Finally, we discuss the challenges and open problems of trust evaluation using machine learning methods.**

***Index Terms*—OSN, VANET, IoT, trust evaluation, machine learning,**

I. Introduction

Trust evaluation is a pivotal concern for any person. Even at a fundamental level, a person's subjective judgment of another person can be influenced by the collective opinions of others. The cumulative feedback given for a person can be conceptualized as the trust evaluation for the person in question. This gives insight on the idea of trust evaluation, defining it as a system with similar process, aiming to provide highly accurate predictions for the evaluated entities. In trust evaluation, just like in the given example, attributes related to trust are used to quantify trust for a final decision. Trust evaluation is also important since it is very widely used to facilitate decision-making processes [1].

Nowadays, with technology being as important as it has ever been in our lives, trust evaluation has ascended the use of itself in peer to peer communication and became an important topic in entity to entity communication in computer networks. Computer technologies have been making rapid progress in this big data era of network technology [2]. As with the increasing usages of the computer networks and the huge amount of sensitive data that they enclose, the security of these computer networks have become a very important topic of discussion. Specifically, evaluating the trust of these networks with different methods to prevent security threats have become a must for the safety of computers networks. Trust has been shown to be a key factor on the reliance people have of automated systems. Also, a correlation linking the trust level of a system and the users' reliance on such system has been found [3]. Machine learning is one of the methods used in these evaluations. Machine learning methods have become one of the more increasingly ever-present tools to help decision making in various domains, ranging from law, medicine to public pol icy [4]. Computer networks are no different from these domains, as machine learning methods are also used very widely in the trust evaluation of computer networks.

This survey aims to provide an outline on what trust evaluation is, different machine learning methods used in the process of trust evaluation; specifically for trust evaluation in OSNs, VANETs and IoT; and the challenges that come with such trust evaluation methods. Particularly, the contributions of the survey can be listed as follows:

1) An outline for what trust evaluation is and how it was being dealt with before and now.
2) An all around review of machine learning methods used for trust evaluation in OSNs, VANETs and IoT that cover solutions up to the year 2021.
3) Discussion of the challenges and open problems related to trust evaluation using machine learning.

The survey from here on out is constructed as follows: Section II discusses what trust evaluation is and the past/present methods used in such evaluations. Section III presents machine learning methods used in trust evaluation; specifically for OSNs, VANETs and IoT; followed by a discussion of challenges of the machine learning based methods for trust evaluation in section IV. Section V discusses the open problems and future research directions, while section VI presents the conclusions of the paper. In Figure 1, the outline of our survey paper can be seen.

II. Trust Evaluation

According to common use, trust evaluation includes any process of quantifying trust between interacting parties. In general, trust is the measured confidence that an entity will behave as the expected manners, thus it is a key property to maintain trustworthy connections among entities and to provide secure services and applications [5].

In a social network [6], trust evaluation improves the quality of networking by helping to build secure social relationships, and in addition to that, the level of trust determines the reliability of information sources or trusted entities to share

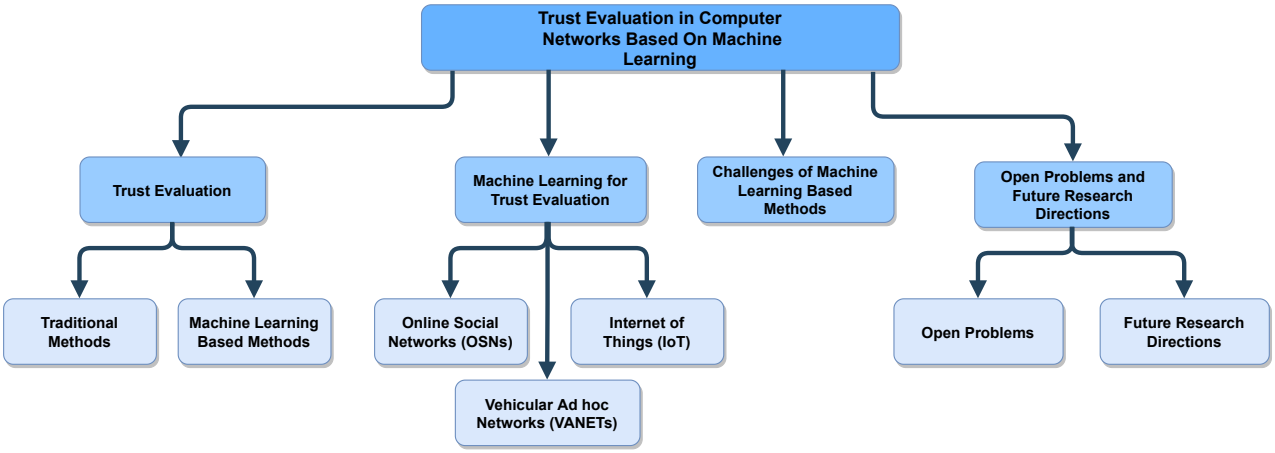

Fig. 1. Outline of the paper

information with or accept information from. In a vehicular ad hoc network (VANET) that is based on communication of vehicles that continuously exchange messages, security and evaluation of trust is a key element [7] in terms of trustworthiness of the information or the established communication itself. In Internet of Things [8], a great number of varying entities are connected to each other to operate individually or in unison, which are dependent on the exchanged information. Thus, the sensitivity of the data is also subject to security issues.

In the scope of this paper, we divide the trust evaluation methods into two, namely traditional and machine learning based methods.

A. Traditional Methods

As the definition of trust evaluation suggests, traditional trust evaluation methods make use of the attributes related to trust for assessments. Unlike intelligent methods, the attributes are hand-picked, which affect the accuracy of the results, such as using different formulations or different attributes leading to different interpretations of measured trust value. Previous work on traditional methods conducts data analysis and literature analysis [9], uses Bayesian inference models [10], game theory models [11], fuzzy logic [12], cloud models [13] and blockchain [14], [15].

The drawbacks and inapplicable scenarios for traditional methods include the occasions where there is no interaction experience between the trustee and trustor, the data used for evaluation is incomplete, the calculations to determine the weights of trust factors are difficult, large amount of data causes the structure to be too complex to systematically and effectively process, or the environment is no longer suitable for computationally efficient calculations by the traditional methods. Traditional methods lack the ease of operations provided by intelligent and dynamic systems. Hence, these methods are no longer preferred by researchers and ongoing studies are directed to machine learning based methods, which are explained in detail in the following subsection.

B. Machine Learning Based Methods

Broadly speaking, machine learning relates to pattern recognition, statistical learning or to any learning scenario where the goal is to analyze the previous data and produce models that can reason about the present/new situations. As models show promising results, machine learning is applied in many research fields as well as trust evaluation. There are numerous learning algorithms that can be categorized by the characteristics of the input information, such as supervised learning, unsupervised learning, semi-supervised learning and reinforcement learning models, or the type of the model outputs, such as classification and regression models.

Machine learning based methods overcome the difficulties faced when traditional methods are used, such as solving the zero knowledge or cold start problem by using the available features, providing computationally efficient and accurate methods when processing big data due to the nature of algorithms that are advantageous in dealing with big data, and the algorithms are intuitive and easier to follow when compared with complex traditional methods. Machine learning models try to simulate the process of human decision-making and reasoning, by making use of existing experiences, which is also easier to understand. Above all, as the field of machine learning keeps growing, many automated shortcuts are easily implemented to fine-tune the models according to the problem environment and achieve better results.

As there are different application scenarios for evaluating trust as well as varying problem settings, the comprehensive survey by [16] provides a categorized approach to determine the criteria for requirements of the methods for trust evaluation to be considered preferable, which are briefly listed as follows:

Effectiveness. To prove effectiveness, an evaluation method must produce accurate evaluation results that can be assessed by metrics such as recall, precision, accuracy, and F-score.

Appropriate Data and Algorithm. Two crucial parts of a machine learning algorithm are the training data and the algorithm. Therefore, the evaluation method must be appropriate for the problem at hand to achieve an accurate evaluation.

Robustness. A rust evaluation method should be able to prevent the attacks from affecting the results of the evaluation.

Privacy Protection. A trust evaluation method should be able to guarantee a secure data processing and protection for the sensitive or private input data.

Context-Awareness. A trust evaluation method should be able to sense and adapt to the changes in the environment dynamically.

Subjectivity. To be realistic, a trust evaluation method should be able to represent the subjectivity of trust.

III. Machine Learning For Trust Evaluation

In this section, we concentrate on three major fields where an evaluation of trust is required, which are Online Social Networks (OSNs), Vehicular Ad-hoc Networks (VANETs) and Internet of Things (IoT). In Table I, a summary of the trust evaluation methods based on machine learning can be seen.

A. Trust Evaluation for Online Social Networks

1) Security Requirements: In such networks like OSNs, where individuals or entities such as organizations are considered as participants/nodes, and interactions or relationships between them are considered as links/edges, trust has a crucial role in building successful and steady operations [17]. Requirements for a secure OSN include the separation of untrustworthy or irrelevant data, protection against spams and attacks, as well as providing privacy of shared messages or sensitive information.

2) Threats: The detailed study [18], where the threats that OSN users can be exposed to are listed, describes the threats mainly as information harvesting, where the harvested information related to personal issues can be used for tailoring advertisements, harming individuals by spreading the information, or obtaining further information of an individual based on their connection with the victim of harvesting are classified into 4 main divisions namely classic, modern, combination threats and threats targeting children.

3) Current Studies & Solutions: On the Internet, one of the most frequently visited place is Online Social Networks (OSNs). These places are where most people interact and strengthen their connections with other people. Because of this interaction and connection, trust is one of the most important factors while using Online Social Networks [19]. In this section, we discuss the machine learning methods used for trust evaluation in OSNs that deals with these trust issues.

In [20], the importance of managing trust in an Online Social Network between users and presents a model that has subjective logic as its basis is emphasized. The model calculates trust in three main categories; namely confirmation, similarity, and recommendation. The results are then converted according to the subjective logic model to be combined for the final result. To evaluate the model, a dataset consisting of random data and data extracted from LinkedIn and Facebook is used. Precision of the model is evaluated using the Leave-One-Out method. Calculated metrics such as recall and precision show that the model proposed is an improvement over other method.

Since OSNs are the most popular communication platforms; people are frequently exposed to fake content, which creates a trust issue, says [21]. It also suggests that existing work related to solving such trust issues revolve around creating trust networks of users rather than analyzing such users' features. By considering several user features, they proposed a framework empowered by machine learning that makes decisions easier for humans. User features were divided into four different groups, and a lightweight approach to feature selection was used to find the best combination of features. Trust analysis was formalized into a classification problem for a simpler verification process. The results were compared with existing research that contained four different feature sets and another four more traditional methods of trust evaluation. The machine learning approach proposed performed better when tested with a dataset from the real world.

Previous works about trust in OSNs are discussed by [22], stating that most decide on the trust value by only considering several factors related to trust with weights assigned to them. It also states that the weight given to these trust factors is hard to decide, since their influence on the final result is never certain. To tackle this issue, a machine learning method is proposed. The trust-related factors are gathered in a feature vector, and then training is done on the collected data that includes the feature vectors and trust ratings. With this approach, a broad framework on trust evaluation is proposed at the network level. The results show that this way of creating a trust classifier achieves a fairly high accuracy of predictions.

It is suggested by [1] that the trust evaluation between two connected users in an OSN creates challenges that require careful care when evaluating. One of these challenges is the possible overlapping of different paths, which creates a path dependency problem. Another challenge is the trust decay that can occur in each node while propagating through a path. To solve these challenges, the trust evaluation problem that consists of trust decay and path dependency is generalized into a problem of network flow. Then a solution is proposed in the name of GFTrust, which is a trust evaluation process that links the leakage in each node with trust decay while also using network flow to address path dependency. Their results show that GFTrust has high accuracy when tested on the OSN data sets named Advogato and Epinions.

A model for social networks using machine learning that calculates the trust value for each node is built by [23]. To train the machine learning algorithm, trust value calculation results of traditional methods for nodes, edge information, and some supporting information is used. Then, trust value calculations are made for nodes by using logistic regression as the model. After training, a filtering algorithm that is user collaborative calculates the trust value for the nodes. Simulations were used to compare the performance of the

TABLE I
SUMMARY OF TRUST EVALUATION METHODS USING MACHINE LEARNING

Ref.	Field	Type	Remark
[1]	OSN	Research	Linking each node with trust decay, GFTrust
[20]	OSN	Research	Subjective logic based trust evaluation between users
[21]	OSN	Research	Analyzing user features for trust evaluation
[22]	OSN	Research	Using feature vectors that contain trust-related factors
[23]	OSN	Research	Node by node trust value calculation
[24]	OSN	Research	Identify trustworthy users by Bayesian networks with hidden variables
[25]	OSN	Research	Pairwise trust prediction
[29]	VANET	Research	An entity centric model for trust evaluation
[30]	VANET	Research	Data-oriented malicious node detection
[31]	VANET	Research	Misbehavior classification
[32]	VANET	Research	k-NN and SVM for plausability check
[33]	VANET	Research	SVM-based intelligent detection model
[39]	IoT	Research	Using classification on trust features
[40]	IoT	Research	Network Lasso problem solved with models trained on MEC-environments topology
[41]	IoT	Research	Nodes that can calculate another nodes trust value
[42]	IoT	Research	A trust management (TM) model
[43]	IoT	Research	A method using QoS (Quality of Service) trust properties
[44]	IoT	Research	Time-aware trust prediction
[45]	IoT	Research	Trust feature extraction for computations
[46]	IoT	Survey	A taxonomy of IoT threats and solutions

method to the traditional ones, and it showed that the improved method reached higher accuracy than that of the trust values calculated by the traditional formula.

In [24], to identify trustworthy users, a model based on Bayesian networks with hidden variables is proposed. Parallel to the drawbacks of traditional methods we stated in Section 2, this study also emphasizes the advantages of using machine learning methods and transforms trust prediction into a classification task in order to avoid the problems raised such as trust decay or path selection. The article utilizes user features to train a classifier, and determines the trustworthiness of a person according to their past records. This process is formalized by defining a graph structured model, specifically Bayesian networks, which is one of the most prevalent probabilistic graphical model. In this model, the trust rating of a user is obtained by evaluating the possible rating of each hidden component, which are actually user features in historical data that are abstracted into high-level components. The study claims to be more flexible and efficient than the traditional methods as it tries to model a pattern related to trust, and proves their argument by the experiments carried out on Facebook and Twitter datasets, achieving relatively superior and stable scores in different accuracy metrics.

Being a barely studied trust computation approach, pairwise trust prediction is proven to be capable of learning trust relations in [25], where a pair relates to the relationship between two users of OSNs. Main properties of pairwise trust are summarized as subjectivity, meaning trust evaluation is based on personal preferences thus it is a biased assessment, contextuality, meaning that the computations are dependent on the context, dynamism, meaning trust needs to be also reconsidered in case of new evidence arrivals or the context changes. In this study, trust evaluation is modeled as pairwise trust being an edge of the graph that is constructed by users being the vertices. Then, trust features are classified considering the view of both the trustor and the trustee. Providing a detailed revision of existing machine learning algorithms, the studies that present trust prediction using these methods are examined, and those studies are shown as indicators of the accurate and improved predictions. Thus, pairwise trust prediction which is modeled as a classification problem is claimed to be more effective.

B. Trust Evaluation for Vehicular Ad hoc Networks

1) Security Requirements: A secure VANET must guarantee that attackers can not modify exchanged information or insert in faulty messages, as the implementation and use cases of VANETs affect the safety of the people. Due to its nature, wireless communication, guarding against or avoiding attackers are harder and many challenges rise caused by the characteristics of VANETs [26]. Some of the challenges listed in [27] include the network size, which can be geographically unbounded and dynamic, information verification, which is subject to frequent exchanges of information that need to be trusted before operating on, key distribution, which is crucial to a secure mechanism and forwarding algorithms, which needs to be the most suitable in terms of casting the transmitted packets. These challenges form the requirements for a secure and functioning network architecture.

2) Threats: VANETs can be exposed to threats to wireless communication, such as DoS, malware, spam and man in the middle attacks, threats to sensors on the vehicle, such as illusion or jamming, and infrastructure related threats such as unauthorized access, session hijacking or repudiation [27].

3) Current Studies & Solutions: Vehicles associated with an Internet of Vehicles (IoV) trade data using Vehicle-to-Vehicle (V2V) Vehicular Ad-hoc Networks (VANETs). Harmful clients in these networks can create mayhem by deceiving the interchange of data between vehicles. This kind of information misrepresentations attacks are important security issues

in VANETs that need to be dealt with [28]. In this section, we discuss the machine learning methods used for trust evaluation in VANETs to deal with these security issues.

In [29], it is suggested that it is challenging to find an optimal solution for transferring data reliably in vehicular networks because of their dynamic character. Although the difficulty of such solution is suggested, the importance of an efficient and reliable solution is emphasized. An entity centric model is used to evaluate trust values. Trust calculation rules are derived using decision trees as the classification model and self-training is done by neural networks on vehicular nodes. Metrics involving distances like Euclidean distance and multifaceted role are used for trust estimation. Carried out comparative analyses show that the proposed model performs better when compared to other entity centric models.

Trust models have been an important and reliable source when trying to detect malicious nodes in Vehicular Ad-hoc Networks (VANETs) says [30]. They propose a data-oriented model. Direct trust is defined, which is the trust metric to be calculated using the data from a transmitted message. This trust value is computed by two parameters; namely speed and received power. K-NN algorithm is then used to determine whether the vehicle is malicious or not, depending on the messages it transmits in relation to the direct trust value. Experiments with different positioning of vehicle concluded that the proposed method is effective in finding malicious nodes, achieving the highest accuracy in the validation experiment with %95,4.

An approach to use machine learning in classifying various misbehaviors in Vehicular Ad-hoc Networks (VANET) by using behavioral and concrete features of the nodes is proposed in [31]. Different misbehaviors are created by tampering with the data transmitted in packages. These misbehaviors are of different types like dropped packets, received signal strength (RSS), number of packets delivered etc. Binary classification is used when all misbehaviors are considered to be one single "misbehaviour" while multi-class classification is used when the misbehaviors are categorized. NCTUns-5.0 simulator is used to extract the features of the nodes sending the packets and the proposed model is assessed using WEKA. The approach is proved to be efficient in finding multiple misbehaviors in a VANET. Results of the experiments show that J-48 and Random Forest classifiers have performed the best.

In [32], it is said that the Vehicular Ad-hoc Networks' (VANET) safety comes from the safety of the data transmitted between vehicles. In order to securely transmit data, this paper suggests using machine learning models with feature vectors being plausibility checks. By using the machine learning algorithms k-NN and support vector machines (SVM), they are able to improve overall plausibility check precision by more than %20. They are also able to keep recall less than %5. They also come to the conclusion that a misbehaviour can be classified into already known types of misbehaviors when they are detected. This allows the algorithm to be more decisive when on the counterattack, improving the systems' ability to protect itself.

Two main reasons that make Vehicular Ad-hoc Networks (VANET) harder to protect are their mobile nature and the limited resources they carry says [33]. CEAP is the model introduced in this paper to tackle these issues, as it has minimal overhead and high detection rate. Monitoring is done on the vehicles to create a data set to be analyzed by the support vector machine (SVM) method that classifies the vehicles as malicious or cooperative. Also, VANET QoS-OLSR, a clustering protocol, is introduced for the model to be able to adapt to high mobility situations. Their simulation results showcase that CEAP is able to have higher accuracy and less false positives when tested with high mobility in comparison to classical SVM-based models.

C. Trust Evaluation for Internet of Things

1) Security Requirements: Trust in IoT can be described as the reliability of interactions among members of the networks, which are devices of different types of purposes [34]. As there is no standardized model for IoT networks, there is also no single security protocol that needs to be satisfied for all, but the issues are context-dependent instead. Roughly, the connections between devices, the user management and the devices themselves must be robust to attacks from third parties threatening security, reliability, confidentiality and authenticity of data being transmitted in an IoT network [35].

2) Threats: As research and surveys [35]–[37] on trust evaluation and management indicate, IoT threats are different from common networks. First of all, IoT devices have limited capacity in terms of memory and computational power. However, the devices that have access to Internet are powerful computers and servers that are secured by different complex protocols that can not be applied to IoT devices due to unaffordability. These shortcomings rise various attack types that can threaten the security and privacy of the data exchanged, functioning of devices and operations to provide services to users.

3) Current Studies & Solutions: Internet of Things (IoT) can be characterized as heterogeneous technologies coming together, making it so that the provisioning of these services coincided. This creates a scenario where the privacy and security requirements like data confidentiality, trust among things and users, enforcement of the privacy and security policies are very important [38]. In this section, we discuss the machine learning methods used for trust evaluation in IoT to deal with these security and privacy issues.

In [39], it is suggested that the coming of the Internet of Things (IoT) has created a large amount of sensitive data to be accessed in every participant objects in an IoT ecosystem and that access to such sensitive data creates various risks. They touch on the importance of the trust concept to overcome this issue, while also saying that it is still difficult to set up a foundation of trust in a cyber world where there are many factors to take into account. It is said that the existence of an accurate computational model is greatly important, and therefore they propose a quantifiable assessment model. In this model, different attributes related to trust are numerically

calculated. Then, a machine learning algorithm is used for classification on the trust features to generate a final trust value after combining them. The machine learning model was tested through simulations and it showed that their method was more effective than different aggregation methods.

An evaluation method for the trustworthiness of Internet of Things (IoT) services based on Mobile Edge Computing (MEC) sensor services is proposed in [40]. A problem called Network Lasso is introduced. To solve this problem, they propose a machine learning algorithm that trains on a MEC-environments topology. This way, simultaneous clustering is achieved while also optimizing the process for higher scale graphs. Also, another method called Alternate Direction Method of Multipliers (ADMM) is used in an attempt to create a more suitable solution for IoT systems based on MEC. The results are presented both as a simulation and analytically, which shows the validness and effectiveness of the proposed model.

According to [41], Internet of Things (IoT) has led to a paradigm where each object is capable of having autonomous social relationship. This paradigm leads to the objects seeking each other for services. The paper focuses on the malicious attack types that effect IoT and propose a model that is designed to overcome the such attacks. They propose a model where each node in the IoT has the ability to calculate and store another node's information, making each node have its own idea of the general network of nodes. This way, if the malicious attacks were to have a shift in behaviour, it is easily detected. Their simulation results show that with adequate increase in the processing that makes the model converge, almost all threatening nodes in the network can be found.

The Social Internet of Things (SIoT) popularity growth is related to the trustworthiness of the interaction between SIoT nodes by [42]. Moreover, the challenge in finding a Trust Management (TM) model to establish security measures is discussed while also touching on the ineffectiveness of already established TM models. In regard to this, a TM model is proposed that recognizes trustworthy nodes and also one that detects and stops hostile attack. The proposed machine learning based TM model can spot malicious attacks by training on trust features obtained from the behaviour of malicious nodes. Experimental results on the proposed model with data sets based on real time data show the effectiveness of the proposed model.

Malicious devices in an Internet of Things (IoT) devices create threats in the IoT environment says [43] and that trust is an important security measure for detecting such malicious devices. To solve such issues, an evaluation method empowered by machine learning is proposed. The proposed method, for an IoT device in the network, uses the network QoS' (Quality of Service) trust properties to aggregate them by using some deep learning algorithm to create a behavioral model. Trust value is found by comparing the network behaviors predicted by the model with the actual network behaviors and computing the similarities. Also, the trust is expressed as numerical values. Experiments show that the method proposed has promising results.

Bringing out another fundamental problem of establishing trustworthy relationships, [44] focuses on the behavior of a connected object as the time passes. Denoted as a time-aware approach, the proposed trust evaluation model uses machine learning to predict the behavior of an object and decide whether a connection should no longer be trusted or that the connection still trustworthy. The information related to the connected object is collected as a set of triplets, which are information about the object's friends, object's social interest communities and co-work relationship. Then this information is used to quantify the trust of the subject object towards the connected object at a given time interval by formulating the combination of the collected information as a parameter for computing trust. After the computations, the final decision whether to trust the object or not is given by accumulated trust scores with a machine learning-driven model. Experiments show that following this approach produces accurate results and introduces an efficient to computer trust over a period of time.

In [45], to extract trust features of individuals, a trust computational model is proposed which is based on a machine learning approach. Similar to [44], computed trust scores are used to distinguish trustworthy and untrustworthy nodes in a SIoT network, to prevent possible risks coming from the connections made with malicious objects. Computation of trust is divided into two parts as direct and indirect trust, where direct trust is computed utilizing the direct connection between the nodes and indirect trust needs to be computed by requesting information from mutual friend nodes. Trust scores are then obtained, by aggregating the results of computation with a machine learning based model, chosen as k-means clustering in this study. In addition, a dimensionality reduction technique, Principal Component Analysis (PCA), is used to ease the process of feature visualizing. This way, a trust prediction pipeline is formed that learns from individual trust features to compute the trust score for a specific node.

A generic taxonomy of machine learning algorithms and the IoT threats reported to be guarded against is provided by [46], compiling the past twelve years literature. As the paper indicates, the security challenges and threats get more sophisticated with the improvements in technology and access to sources. Accordingly, integration of machine learning algorithms into improving IoT infrastructure, like smart sensors and IoT gateways, also become widespread. Machine learning algorithms show improvements when used to protect device data and user privacy, as proven in the literature. The authors examine existing solutions in two divisions of security efforts and privacy efforts, and the machine learning algorithms used to prevent and detect attacks include LSTM (Long Short-Term Memory), Softmax, SVM (Support Vector Machine) and deep learning algorithms that occasionally performed better than machine learning algorithms. As a result, a comprehensive list of machine learning algorithms applied to security and privacy issues prove that preferring machine learning methods provides effective solutions when compared to traditional

methods.

IV. Challenges of Machine Learning Based Methods

In this section, we identify some challenges of using machine learning methods and discuss them.

A. Paradigm Shift

By definition, paradigm shift means "the significant change of the usual way of thinking about or doing something to a new and unfamiliar way". Thus, transitioning from traditional methods to machine learning algorithms is a different path for the researchers that requires domain-specific knowledge. Though the studies showing promising result of machine learning based evaluation methods, there is a barrier of knowledge that needs to be overcome for researchers coming from a field unrelated to background of machine learning algorithms. Another concern is the misuse of these algorithms, in terms of context of the problems, type of the data or the required output, causing misleading results or loss of time.

B. Inconsistency of Data Type

Stated as a research challenge in [37], the structure of machine learning algorithms are highly data-driven, as they try to extract a pattern by examining previous experiences. Therefore, inputs and outputs of each step in the algorithm must be exactly defined to continue the process and perform calculations that affect the final predictions. This might not be feasible in every setup, for example, in the context of IoT. For IoT networks, where each and every device might be of a different type, ensuring a secure data exchange is sufficient in the scope of secure networking. However, each device might generate varying types of data which is not suitable for a machine learning algorithm to process. Choosing data of a single type might cause loss of significant data, and the predictions might be affected due to that loss. In addition, efforts to solve this problem by collecting data is a time-consuming and expensive process when considered the manpower, storage and planning spent on the process. The collected data might still be lacking to represent and cover real-life situations.

C. Feature Engineering

Feature engineering is one of the challenges of machine learning algorithms, which is almost the beginning step before the training process essential to the algorithm. As machine learning algorithms can not process the raw data, a feature extraction step must be performed by experts to define features that best represent each instance. In general, quality of features determine the quality of the predictions and eventually the success of the project. Well-engineered features compensate the time spent in training the model, interpreting the results and making the project scalable [25]. Thus, it is a challenge that turns into an advantage when implemented carefully. Feature extraction typically requires domain-specific knowledge, time and effort to achieve the predictions in the most efficient manner.

V. Open Problems and Future Research Directions

In this section, we identify some open problems and future research directions regarding the above literature review and the analysis we conducted.

A. Open Problems

One of the most important problems with machine learning based trust evaluation is in the way the most of the algorithms are used to evaluate trustworthiness of an entity. Most of the existing work treats the trust evaluation process as a classification problem. Even though these types of solutions are pretty fast and effective, it divides the trust evaluation process into a yes or no question where an entity can be just trustworthy or not. This kind of classification does not adequately reflect the uncertainty and subjectivity of trust. No method used to capture trust can fully achieve this goal as trust is essentially vague and subjective. Representation of trust in a quantitative way inevitably results in missing influential variables. Because of this, trust values are essentially all uncertain [47].

Another problem is the fact that a generic solution for trust evaluation has not been found. The trust domain has a great challenge in which there still does not exist a generic framework that evaluates trust, which would motive already existing systems solutions to adopt its concept [48]. As an artificial intelligence branch, machine learning enables machines to skillfully carry out their jobs using intelligent software. Methods of statistical learning create the backbone of the intelligent software that improves its performance continuously using structures of existing knowledge [49]. Trust evaluation methods we have covered show us that trust evaluation based on machine learning is a very powerful tool in many different areas; such as the ones we have covered like OSNs, IoT and VANETs; and in many different cases like complex, big, sparse data etc. In spite of all of this, the problem that arises here is that most of the trust evaluation methods based on machine learning are applied to the more popular research areas such as OSNs and IoT. Our review shows that there is still a lack of a general method that can be applied to different various field.

Thirdly, in the trust evaluation process, the selected machine learning algorithms, their integration with the trust evaluation problem and the features selected etc. need to be explored for classification of their effectiveness. Feature selection is considered to be one of the methods to improve the classifier performance [50]. While choosing a different algorithm, adding new features, creating different algorithms are all things that can be done to change the effectiveness of the solution, it can also go in the opposite direction as the effectiveness of the solution might be hindered. There are also other things to worry about like computation time, solution complexity etc. This creates the problem that with everything in mind, there could be an infinite number of solutions for a particular trust evaluation problem and that the most optimal solution for a problem may never be found. This makes the

topics of choosing the correct algorithm, combining the must effective methods, selecting efficient features etc. a worthwhile study.

Another problem arises from the fact that in general, the machine learning methods used for trust evaluation don't take into account the privacy of the used data. As machine learning has been developing faster and faster, security risks are also rising. To train and predict, machine learning models use large amounts of data that inevitably contains private and sensitive information [51]. Most of the data used in trust evaluation requires some sort of private information that is related to the entity it is coming from. Because of this, one of the most important things to consider when creating a machine learning based algorithm is privacy. None of the existing literature that we have reviewed touch on the importance of privacy while creating their algorithm. Beyond data privacy, there should also be consideration on what kind of malicious threats or attacks can target their methodology. Again, many of the existing literate also lack in proving whether their proposed method is reliable against these attack. Problems regarding security and privacy are heavily overlooked when designing algorithms, but should be highly considered since they are such important topics.

Fifth, the results given in existing works generally tends to only be tested in a specific dataset/database. By not testing the developed methods with more data set or real time data, such solutions lack trustworthiness as these methods might not be as accurate as they look or they might not be suitable for real world applications. There is also the fact that many researches do not necessarily touch on how their method is created, but only broadly explain their methodology. This also creates a trustworthiness issue as it is unclear that an actual solution is being tested or if the perceived method is being used the way it is being explained. One of the main problems with machine learning is the quality of the methods and that the trust in the predictions given by the machine learning algorithms are difficult to measure [52]. By trying the methodologies with different inputs and providing clear explanations, the trustworthiness of the machine learning methods used in trust evaluation can increase drastically.

Finally, researches generally tend to address only how accurate their solutions are. This leads to most researches overlooking the fact that even though their solutions may be accurate, the performance of such solutions still have to be evaluated to find an optimal algorithm for trust evaluation. Any overheads that may arise in computation are serious issues that must be looked into. As a consequence, machine learning methods used for trust evaluation should consider evaluating the complexity of their solutions. They also should have a healthy balance between quality attributes such as precision, accuracy etc. and the algorithm computational time.

B. Future Research Directions

In this section; based on the literature review, analysis we have conducted and the open research problems we have discussed, we will be discussing some of the future research directions for trust evaluation based on machine learning. From our research and the open problems discussed, we believe that there are many important issues that need attention moving forward.

Firstly and most importantly, further research must include trust evaluation based on machine learning methods that are open to subjectivity. It was already discussed that the general classification of existing algorithms that base an entity only on being trustworthy or not, do not adequately reflect trust. To provide more accurate results, traditional methods of trust evaluation can be used in combination with machine learning algorithms to make the results more effective and relevant. In addition to this, more dynamic approaches in trust evaluation using machine learning can be taken to reflect the subjectivity of trust as well. Distinctive characteristics of some networks, such as a dynamic environment, require different approaches when evaluating trust [53]. More researches should either try to create the subjectivity of trust using these methods, or they should try and well define the trust concept used in their methods. Besides traditional methods, other methods that compute trust can be used in combination with the machine learning algorithms to create more accurate and dynamic results.

Another future research topic should be finding better ways of selecting algorithms and their features. Most of the current work chooses their algorithms and features specific to the scenario of their problem. This lacks union, as it provides a different solution for each scenario. It also lacks effectiveness, as it is impossible to determine if the way the solution method used is the best solution that can be achieved. New studies should explore new ways of feature and algorithm selection to create a common solution that would be both effective and not case-specific. Solutions like using machine learning to select algorithms and features could be used. Creating more layers in the problem solution process and automating it like this would provide more effective solutions.

Thirdly, the security and privacy concerns regarding the machine learning methods should be deeply delved into and explained with the method process. To create machine learning models with high-quality, there is a constant collection of personal data. This direct access to rich personal data, in turn, has created a growing concerns regarding security and privacy [54]. In feature works, the private data that is inevitably used in the machine learning process should be carefully sought out, and their privacy should not be in jeopardy. Feature works should specify what kind of private data they are using and what they will be doing with them. There is also the fact of security. None of the existing research touch on how the machine learning model they are using would deal with outside threats. There are many different types of threats and attacks that can affect a model, and future research should be carefully detailing the types of threats they might encounter and the countermeasures that they would be using in such cases. Current work lacks a lot to be desired regarding security and privacy and future research should carefully examine and report cases that arise with these topics.

More researches that provide more information regarding the machine learning model is expected in feature studies. Most of the existing research tends to overlook the fact that there is more to a method than getting an accurate result. Computation complexity, practicality of the method, real world applications, computation cost, optimization requirements are just some of the few important points that needs to be addresses with the general methodology of the machine learning methods. This would also help to create a more healthy balance for the attributes of the machine learning models, as they will be more thoroughly explored and documented. This would also benefit the general applicability of these models as by creating a more common ground for future research with more specific topics, creation of a generic machine learning model that can be used for trust evaluation can be achieved. If not so, combining different models from different domains could be another search area to create a more generic machine learning model.

Fifth, in future researches, different machine learning algorithms and more data sets should be used when evaluating trust. There are three main types of machine learning algorithms called supervised, semi-supervised and unsupervised. Researches done with machine learning algorithms tend to use supervised machine learning. Semi-supervised machine learning techniques are techniques where a small amount of data is labeled while a larger amount of data is unlabeled and unsupervised machine learning techniques are techniques where no data is labeled and ground truth data is used for evaluation [55]. New researches can have different approaches by using different semi-supervised and unsupervised machine learning algorithms to evaluate trust. Another approach that could also help in further researches is the use of more and better data sets for trust evaluation. Training and evaluating the machine learning algorithms will be beneficiary as with more data, advantages and disadvantages of the algorithms will be easier to spot. Also, real time data could be a very important resource in feature researches as the main purpose of creating such algorithms is to provide effective and accurate trust evaluation. Machine learning models that are harder to implement into the real world will be much less prominent than the ones that can scale into real world applications.

Clear explanations for the machine learning algorithms used for trust evaluation is another topic that needs to be addressed more in future researches. A person's perception of trustworthiness of an AI impact their behaviours and decisions regarding said AI [56]. Many of the existing researches give general definitions of what their solution is without defining trust, prerequisites, construction of their methodology etc. By giving more insight into what is going on in the process of building their models, more trustworthy and applicable solutions can be created.

Lastly, integrating machine learning methods used in trust evaluation with other state-of-the-art technologies such as informed machine learning [57], cloud theory [58], bionic mechanism based solutions [59], blockchain based solutions [60], dynamic solutions [61], knowledge fragments [62], deep learning [63], extreme learning machine [64] in future researches would be an innovative way of approaching trust evaluation.

VI. Conclusion

Initially, the study introduced the foundational trust evaluation concept, presenting the employed methodologies. The methods were then divided into two parts as traditional and machine learning based methods. Following a comparative analysis of the two concepts, machine learning based method for trust evaluation were delved into. Mainly, three types of computer networks were discussed; Online Social Networks (OSNs), Internet of Things (IoT) and Vehicular Ad-hoc Networks (VANETs). Explanations on security requirements, threats and current studies & solutions regarding these computer networks were given, followed by a discussion regarding the challenges of using machine learning methods for trust evaluation. Finally, a discussion about the open problems and future research regarding the use of machine learning models in trust evaluation was presented. This survey contributes to presenting the conceptual foundations of trust evaluation, including traditional and machine learning-based methods. A broad review of machine learning methodologies applied to trust evaluation is given for OSNs, IoT and VANETs, discussing the challenges and open problem related to using machine learning models for trust evaluation.

References

[1] W. Jiang, J. Wu, F. Li, G. Wang and H. Zheng, "Trust Evaluation in Online Social Networks Using Generalized Network Flow," in IEEE Transactions on Computers, vol. 65, no. 3, pp. 952-963, 1 March 2016, doi: 10.1109/TC.2015.2435785.

[2] Jiang, D. Application of Artificial Intelligence in Computer Network Technology in big data era. *2021 International Conference On Big Data Analysis And Computer Science (BDACS)*. pp. 254-257 (2021)

[3] Yu, K., Berkovsky, S., Taib, R., Conway, D., Zhou, J. & Chen, F. User Trust Dynamics: An Investigation Driven by Differences in System Performance. (2017,3)

[4] Yin, M., Wortman Vaughan, J. & Wallach, H. Understanding the Effect of Accuracy on Trust in Machine Learning Models. *Proceedings Of The 2019 CHI Conference On Human Factors In Computing Systems*. pp. 1-12 (2019), https://doi.org/10.1145/3290605.3300509

[5] Sherchan, W., Nepal, S. & Paris, C. A Survey of Trust in Social Networks. *ACM Comput. Surv.*. **45** (2013,8), https://doi.org/10.1145/2501654.2501661

[6] Ghafari, S., Beheshti, A., Joshi, A., Paris, C., Mahmood, A., Yakhchi, S. & Orgun, M. A Survey on Trust Prediction in Online Social Networks. *IEEE Access*. **8** pp. 144292-144309 (2020)

[7] Soleymani, S., Abdullah, A., Hassan, W., Anisi, M., Goudarzi, S., Rezazadeh Baee, M. & Mandala, S. Trust management in vehicular ad hoc network: a systematic review. *EURASIP Journal On Wireless Communications And Networking*. **2015** (2015)

[8] Truong, N., Jayasinghe, U., Um, T. & Lee, G. A Survey on Trust Computation in the Internet of Things. *THE JOURNAL OF KOREAN INSTITUTE OF COMMUNICATIONS AND INFORMATION SCIENCES (J-KICS)*. **33** pp. 10-27 (2016,1)

[9] Yan, Z., Zhang, P. & Vasilakos, A. A survey on trust management for Internet of Things. *Journal Of Network And Computer Applications*. **42**, 120-134 (2014)

[10] Wang, G. & Wu, Y. BIBRM: A Bayesian Inference Based Road Message Trust Model in Vehicular Ad Hoc Networks. *2014 IEEE 13th International Conference On Trust, Security And Privacy In Computing And Communications*. pp. 481-486 (2014)

[11] Mehdi, M., Raza, I. & Hussain, S. A game theory based trust model for Vehicular Ad hoc Networks (VANETs). *Computer Networks*. **121** pp. 152-172 (2017), https://www.sciencedirect.com/science/article/pii/S1389128617301573

[12] Alnasser, A. & Sun, H. A Fuzzy Logic Trust Model for Secure Routing in Smart Grid Networks. *IEEE Access*. **5** pp. 17896-17903 (2017)

[13] Zhang, T., Yan, L. & Yang, Y. Trust evaluation method for clustered wireless sensor networks based on cloud model. *Wireless Networks*. **24**, 777-797 (2018,4,1), https://doi.org/10.1007/s11276-016-1368-y

[14] Peng, L., Feng, W. & Yang, L. Social-Chain: Decentralized Trust Evaluation Based on Blockchain in Pervasive Social Networking. *ACM Transactions On Internet Technology*. **21** pp. 1-28 (2021,1)

[15] Yan, Z. & Peng, L. Trust Evaluation Based on Blockchain in Pervasive Social Networking. (2018)

[16] Wang, J., Jing, X., Yan, Z., Fu, Y., Pedrycz, W. & Yang, L. A Survey on Trust Evaluation Based on Machine Learning. *ACM Comput. Surv.*. **53** (2020,9), https://doi.org/10.1145/3408292

[17] Liu, L. & Jia, H. Trust Evaluation via Large-Scale Complex Service-Oriented Online Social Networks. *IEEE Transactions On Systems, Man, And Cybernetics: Systems*. **45**, 1402-1412 (2015)

[18] Fire, M., Goldschmidt, R. & Elovici, Y. Online Social Networks: Threats and Solutions. *IEEE Communications Surveys Tutorials*. **16**, 2019-2036 (2014)

[19] G. Liu, Q. Yang, H. Wang and A. X. Liu, "Trust Assessment in Online Social Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 994-1007, 1 March-April 2021, doi: 10.1109/TDSC.2019.2916366.

[20] Zohreie, M. & Shakeri, H. A Model for evaluating trust between users in social networks based on subjective logic. (2016,10)

[21] X. Chen, Y. Yuan, L. Lu and J. Yang, "A Multidimensional Trust Evaluation Framework for Online Social Networks Based on Machine Learning," in IEEE Access, vol. 7, pp. 175499-175513, 2019, doi: 10.1109/ACCESS.2019.2957779.

[22] K. Zhao and L. Pan, "A Machine Learning Based Trust Evaluation Framework for Online Social Networks," 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 2014, pp. 69-74, doi: 10.1109/TrustCom.2014.13.

[23] Yuji, W. The Trust Value Calculating for Social Network Based on Machine Learning. (2017,8)

[24] Chen, X., Yuan, Y. & Orgun, M. Using Bayesian networks with hidden variables for identifying trustworthy users in social networks. *Journal Of Information Science*. **46**, 600-615 (2020),

[25] Liu, S., Zhang, L. & Yan, Z. Predict Pairwise Trust Based on Machine Learning in Online Social Networks: A Survey. *IEEE Access*. **6** pp. 51297-51318 (2018)

[26] Hussain, R., Lee, J. & Zeadally, S. Trust in VANET: A Survey of Current Solutions and Future Research Opportunities. *IEEE Transactions On Intelligent Transportation Systems*. **22** pp. 2553-2571 (2021)

[27] Hasrouny, H., Samhat, A., Bassil, C. & Laouiti, A. VANet security challenges and solutions: A survey. *Vehicular Communications*. **7** pp. 7-20 (2017), https://www.sciencedirect.com/science/article/pii/S2214209616301231

[28] P. Sharma and S. Jain, "Review of VANET Challenges and Protocol for Architecture Design and Intelligent Traffic System," 2nd International Conference on Data, Engineering and Applications (IDEA), 2020, pp. 1-4, doi: 10.1109/IDEA49133.2020.9170685.

[29] El-Sayed, H., Ignatious, H., Kulkarni, P. & Bouktif, S. Machine learning based trust management framework for vehicular networks. *Vehicular Communications*. **25** pp. 100256 (2020), https://www.sciencedirect.com/science/article/pii/S2214209620300279

[30] Montenegro, J., Iza, C. & Aguilar Igartua, M. Detection of Position Falsification Attacks in VANETs Applying Trust Model and Machine Learning. *Proceedings Of The 17th ACM Symposium On Performance Evaluation Of Wireless Ad Hoc, Sensor, &; Ubiquitous Networks*. pp. 9-16 (2020), https://doi.org/10.1145/3416011.3424757

[31] Grover, J., Prajapati, N., Laxmi, V. & Gaur, M. Machine Learning Approach for Multiple Misbehavior Detection in VANET. *Communications In Computer And Information Science*. **192** pp. 644-653 (2011,7)

[32] S. So, P. Sharma and J. Petit, "Integrating Plausibility Checks and Machine Learning for Misbehavior Detection in VANET," 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), 2018, pp. 564-571, doi: 10.1109/ICMLA.2018.00091.

[33] Wahab, O., Mourad, A., Otrok, H. & Bentahar, J. CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. *Expert Systems With Applications*. **50** pp. 40-54 (2016), https://www.sciencedirect.com/science/article/pii/S0957417415008088

[34] Rashmi, M. & Raj, C. A Review on Trust Models of Social Internet of Things. *Lecture Notes In Electrical Engineering*. (2019)

[35] Chahal, R., Kumar, N. & Batra, S. Trust management in social Internet of Things: A taxonomy, open issues, and challenges. *Comput. Commun.*. **150** pp. 13-46 (2020)

[36] Sharma, A., Pilli, E., Mazumdar, A. & Gera, P. Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes. *Computer Communications*. **160** pp. 475-493 (2020), https://www.sciencedirect.com/science/article/pii/S0140366419319073

[37] Restuccia, F., D'Oro, S. & Melodia, T. Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. *IEEE Internet Of Things Journal*. **5**, 4829-4842 (2018)

[38] Sicari, S., Rizzardi, A., Grieco, L. & Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*. **76** pp. 146-164 (2015), https://www.sciencedirect.com/science/article/pii/S1389128614003971

[39] U. Jayasinghe, G. M. Lee, T. Um and Q. Shi, "Machine Learning Based Trust Computational Model for IoT Services," in IEEE Transactions on Sustainable Computing, vol. 4, no. 1, pp. 39-52, 1 Jan.-March 2019, doi: 10.1109/TSUSC.2018.2839623.

[40] P. Abeysekara, H. Dong and A. K. Qin, "Machine Learning-Driven Trust Prediction for MEC-Based IoT Services," 2019 IEEE International Conference on Web Services (ICWS), 2019, pp. 188-192, doi: 10.1109/ICWS.2019.00040.

[41] C. Marche and M. Nitti, "Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3297-3308, Sept. 2021, doi: 10.1109/TNSM.2020.3046906.

[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," 2021 International Wireless Communications and Mobile Computing (IWCMC), 2021, pp. 1465-1470, doi: 10.1109/IWCMC51323.2021.9498808.

[43] W. Ma, X. Wang, M. Hu and Q. Zhou, "Machine Learning Empowered Trust Evaluation Method for IoT Devices," in IEEE Access, vol. 9, pp. 65066-65077, 2021, doi: 10.1109/ACCESS.2021.3076118.

[44] Sagar, S., Mahmood, A., Sheng, Q., Zaib, M. & Zhang, W. Towards a Machine Learning-driven Trust Evaluation Model for Social Internet of Things: A Time-aware Approach. *CoRR*. **abs/2102.10998** (2021), https://arxiv.org/abs/2102.10998

[45] Sagar, S., Mahmood, A., Sheng, Q. & Zhang, W. Trust Computational Heuristic for Social Internet of Things: A Machine Learning-based Approach. *ICC 2020 - 2020 IEEE International Conference On Communications (ICC)*. pp. 1-6 (2020)

[46] Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. & Usman, M. Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures. *ACM Comput. Surv.*. **53** (2020,12), https://doi.org/10.1145/3417987

[47] H. L. J. Ting, X. Kang, T. Li, H. Wang and C. -K. Chu, "On the Trust and Trust Modeling for the Future Fully-Connected Digital World: A Comprehensive Study," in IEEE Access, vol. 9, pp. 106743-106783, 2021, doi: 10.1109/ACCESS.2021.3100767.

[48] López, J. & Maag, S. Towards a Generic Trust Management Framework Using a Machine-Learning-Based Trust Model. *2015 IEEE Trustcom/BigDataSE/ISPA*. **1** pp. 1343-1348 (2015)

[49] Y. Kumar, K. Kaur and G. Singh, "Machine Learning Aspects and its Applications Towards Different Research Areas," 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2020, pp. 150-156, doi: 10.1109/ICCAKM46823.2020.9051502.

[50] D. O. Ratmana, G. Fajar Shidik, A. Z. Fanani, Muljono and R. A. Pramunendar, "Evaluation of Feature Selections on Movie Reviews Sentiment," 2020 International Seminar on Application for Technology of Information and Communication (iSemantic), 2020, pp. 567-571, doi: 10.1109/iSemantic50169.2020.9234287.

[51] H. Xie, L. Wei and F. Fang, "Research on Privacy Protection Based on Machine Learning," 2021 International Wireless Communications and Mobile Computing (IWCMC), 2021, pp. 1003-1006, doi: 10.1109/IWCMC51323.2021.9498632.

[52] Schmidt, P. & Bießmann, F. Quantifying Interpretability and Trust in Machine Learning Systems. *CoRR*. **abs/1901.08558** (2019), http://arxiv.org/abs/1901.08558

[53] Jiang, J., Zhu, X., Han, G., Guizani, M. & Shu, L. A Dynamic Trust Evaluation and Update Mechanism Based on C4.5 Decision Tree in Underwater Wireless Sensor Networks. *IEEE Transactions On Vehicular Technology*. **69**, 9031-9040 (2020)

[54] Zheng, H., Hu, H. & Han, Z. Preserving User Privacy for Machine Learning: Local Differential Privacy or Federated Machine Learning?. *IEEE Intelligent Systems*. **35**, 5-14 (2020)

[55] Derhab, A., Alawwad, R., Dehwah, K., Tariq, N., Khan, F. & Al-Muhtadi, J. Tweet-Based Bot Detection Using Big Data Analytics. *IEEE Access*. **9** pp. 65988-66005 (2021)

[56] Toreini, E., Aitken, M., Coopamootoo, K., Elliott, K., Zelaya, C. & Moorsel, A. The Relationship between Trust in AI and Trustworthy Machine Learning Technologies. *Proceedings Of The 2020 Conference On Fairness, Accountability, And Transparency*. pp. 272-283 (2020), https://doi.org/10.1145/3351095.3372834

[57] L. von Rueden et al., "Informed Machine Learning - A Taxonomy and Survey of Integrating Prior Knowledge into Learning Systems," in IEEE Transactions on Knowledge and Data Engineering, 2021, doi: 10.1109/TKDE.2021.3079836.

[58] H. Cai, Z. Li and J. Tian, "A New Trust Evaluation Model Based on Cloud Theory in E-Commerce Environment," 2011 2nd International Symposium on Intelligence Information Processing and Trusted Computing, 2011, pp. 139-142, doi: 10.1109/IPTC.2011.42.

[59] S. Ma, X. Shuai, Z. Zhou and K. Qiao, "Bionic Mechanism Based Dynamic Trust Evaluation Method in Cloud Environment," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 136-141, doi: 10.1109/TrustCom/BigDataSE.2018.00030.

[60] D. Wang, X. Chen, H. Wu, R. Yu and Y. Zhao, "A Blockchain-Based Vehicle-Trust Management Framework Under a Crowdsourcing Environment," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1950-1955, doi: 10.1109/TrustCom50675.2020.00266.

[61] Y. Wang, J. Wen, W. Zhou and F. Luo, "A Novel Dynamic Cloud Service Trust Evaluation Model in Cloud Computing," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 10-15, doi: 10.1109/TrustCom/BigDataSE.2018.00012.

[62] G. Liu and L. Li, "Knowledge Fragment Cleaning in a Genealogy Knowledge Graph," 2020 IEEE International Conference on Knowledge Graph (ICKG), 2020, pp. 521-528, doi: 10.1109/ICBK50248.2020.00079.

[63] L. Liu, "Deception, Robustness and Trust in Big Data Fueled Deep Learning Systems," 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 3-3, doi: 10.1109/BigData47090.2019.9005597.

[64] Y. Wang and X. Tong, "Trust Prediction Based on Extreme Learning Machine and Asymmetric Tri-Training," in IEEE Access, vol. 9, pp. 64358-64367, 2021, doi: 10.1109/ACCESS.2021.3075952.