IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 15, 2021, accepted November 23, 2021, date of publication December 3, 2021,
date of current version December 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3132580

Trust Management Systems in Cloud Services Environment: Taxonomy of Reputation Attacks and Defense Mechanisms

SALAH T. ALSHAMMARI[1], KHALID ALSUBHI[1], (Senior Member, IEEE), HANI MOAITEQ ABDULLAH ALJAHDALI[1], AND AHMED MOHAMMED ALGHAMDI[2], (Member, IEEE)

[1]Department of Computer Science, College of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2]Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 21493, Saudi Arabia

Corresponding author: Salah T. Alshammari (salshammari0042@stu.kau.edu.sa)

This work was supported by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia, under Grant KEP-9-611-42.

ABSTRACT Using cloud data storage, large amounts of data can be stored by data owners in a flexible way and at low cost. Hence, there has been a major increase in online cloud service providers and their users. The privacy and security of data in the cloud computing environment is a major issue. Data privacy can be ensured by using a cryptographic access control method, so that data can only be accessed by authorized customers while keeping it inaccessible to unauthorized users. However, this type of cryptographic approach does not address the issue of trust. An integration between several trust models and cryptographic access control models has been presented in many research papers, the aim of which is to make data stored in cloud storage systems more secure. The objective of this study is to determine a solution that can suitably handle trust issues in access control models to decrease the risk as greater security to cloud storage systems, and the quality of decisions being made by data owners and cloud operators is improved. In this paper, we have presented a taxonomy for trust criteria and reputation attacks in cloud computing. Also, some of the fundamental concepts regarding trust management of services within cloud environments have been presented in this paper, along with the latest technologies. There are three layers in the model, and a series of dimensions are further determined for every layer (which are the assessment criteria), which serve as the benchmark to evaluate many research prototypes of trust models in a cloud computing environment by comparing these criteria when evaluating several trust models in a cloud computing environment. In this paper, a comparison of fifteen representative trust management research samples in cloud computing and the appropriate research domains were also carried out by employing this analytical model.

INDEX TERMS Access control, authorization, clouds, databases, information security, online services, security, secure storage, security management.

I. INTRODUCTION

Cloud computing technology is an Internet-based modality that provides online storage, delivering resources to consumers of cloud services on demand, and saving resources on cloud servers [1]. There has been an increase in the use of cloud services following the rapid evolution of Internet technology [2]–[4]. The technology of cloud computing is diverse and includes internal and external consumers and servers for Internet systems, storage, and cloud providers [5]. Cloud computing platform has gained dominance in the business because it incurs minimal operational and maintenance expenses. Cloud computing is used by service providers to offer rapid, reliable, and flexible services to their consumers [6]. Service providers need to prioritize the security and privacy of cloud data when providing these services to cloud consumers.

Various cloud services may be offered through the Internet by the different providers of cloud services, such as Infrastructure as a Service (IaaS), Software as a service (SaaS), or Platform as a service (PaaS), either separately, or in combination with each other in a public setting. Cloud service

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

providers can advertise their services through the Internet, such as those in search engines. Cloud service providers may also host their own services on cloud storage, which is typical for new startups that have limited funds. Feedback may be given via a cloud service provider, or they may put forward inquiries regarding consumer trust value to the trust management system. In a decentralized manner, interfaces are exposed by the nodes of a cloud trust model to obtain feedback from other service providers about cloud consumers' trust value [7]–[9]. The existing cloud services are discovered by the trust management system (TMS) through the Internet, which permits users to find new cloud computing services by searching. Users may also be marketed to on the value of trust by the TMS in the form of service through the Internet.

Since cloud services are usually offered in public domains, it is essential to ensure that they are secure [10], [11]. A large number of users can access public platforms, both within and outside the network, so it is vital to maintain the security of these services. In some situations, the owners of data kept in the cloud require extensive privacy from the public and from the cloud providers themselves. Access control techniques are used to provide security in this situation [12]–[14].

Various factors need to be taken into account when choosing a suitable access control model, such as affordability, cost-effectiveness, efficiency in preventing misconduct, security, and the trust developed as a consequence of using the model [14]. Trust is a very important element in securing cloud computing services [15], [16]. Trust is described in [1] as ''an implicit feature found in the backdrop instead of being explicit, which is clearly defined and measurable.'' These access control models consist of role-based access control (RBAC), attribute-based access control (ABAC), discretion access control (DAC), and mandatory access control (MAC) [17]–[19]. However, it is more convenient to incorporate trust with cryptographic task-role-based access control (T-RBAC) to provide security for data preserved in the cloud, and this increases cloud consumers' interactions with the roles and tasks related to owners' data. A control technique is also required to establish trust with respect to the tasks performed by individual users. A design that permits the integration of a trust model with a cloud storage system that employs a cryptographic T-RBAC approach has been presented in this approach [20], [21].

In this paper, we have defined a classification of all cloud service attacks, as a comprehensive classification to be a reference for all researchers in this field. Also, we have classified the trust models layers into three layers, and a series of dimensions are further determined for every layer (which are the assessment criteria), which serve as the benchmark to evaluate many research prototypes of trust models in a cloud computing environment.

A. PROBLEM STATEMENT

There are serious issues regarding authorization or authorized access to computers and computing devices owned by profit and non-profit organizations, and these can be experienced in open environment systems as well, such as cloud computing systems [22], [23]. Server applications for cloud computing platforms usually use access controls [24], [25]. However, it has been determined in previous studies that access controls are not totally reliable for distributed systems, mainly because there is a dynamic and complex population of consumers and their identities are not determined beforehand [26], [27]. Taking these concerns into account, integrated trust models with access controls are ideal for decentralized systems that have complex consumer bases [28]. Several specific models are created as an outcome of various efforts made by developers to create new trust models that can solve the most complex and sophisticated authorization problems. However, several access controls combined with trust models that have been presented previously [6], [29], [30] were unable to provide an adequate defense against certain attacks.

The advantages mobile cloud computing (MCC) can offer compared to traditional cloud services with fixed infrastructure have made mobile cloud computing a popular research topic in academia and industry [31], [32]. Based on the mobility of the nodes in the MCC, providing and requesting services still poses a challenge due to the mobility. Fixed infrastructure can provide some degree of this service, but there are still challenges due to the mobility of the nodes.

Having an execution platform located near the mobile devices can provide a variety of benefits, including lower latency, accessibility to context information, and lower latency for certain applications, such as augmented reality and augmented interface applications [33], [34]. Due to the presence of functional units such as sensors and high-resolution cameras in mobile devices, there is the potential to build novel crowdsourcing and collective sensing applications that use location data [35], [36].

As technology progresses, cloud computing will continue to dominate application delivery, although cloud applications will shift from typical web services to mobile smart applications that orchestrate several heterogeneous resources. These days, Mobile Edge Computing and Fog Computing are rising architectures which combine the capabilities of the cloud with the capabilities of wireless communication to deliver time-critical applications to the mobile user. An attack may be a combination of these categories in some situations to cause greater damage. These categories are explained in detail and further separated into subcategories [31].

These technology enables applications based on Internet of Things (IoT), social media, and business verticals. Moreover, a wide variety of applications are located across different geographical locations, which requires the use of multi-cloud architecture or cloud federation, involving the interaction between private and public clouds operated by different providers [34].

B. CONTRIBUTION

In this paper, we have presented a taxonomy for trust criteria and reputation attacks in cloud computing. Also, some of the fundamental concepts regarding trust management of

services within cloud environments have been presented in this paper, along with the latest technologies. There are three layers in the model, and a series of dimensions are further determined for every layer (which are the assessment criteria), which serve as the benchmark to evaluate many research prototypes of trust models in a cloud computing environment by comparing these criteria when evaluating several trust models in a cloud computing environment. In this paper, a comparison of many representative trust management research samples in cloud computing and the appropriate research domains was also carried out by employing this analytical model. Several taxonomies have been proposed to identify types of cloud attacks, some focusing on reputation attacks [37], others on both reputation and network attacks [38], [39]. In this paper, we proposed a comprehensive classification of all attacks on cloud services, moreover, we provide taxonomy and evaluation of all types of cloud computing trust models.

C. ORGANIZATION

The remaining parts or the remainder of this paper is organized in the following manner. In Section II, a taxonomy for cloud computing reputation attacks is presented. In Section III, we present overview of trust management models. In Section IV, qualitative analysis for trust managements is presented. In Section V, research prototypes are reviewed by us. The conclusion is presented in Section VI.

II. TAXONOMY OF CLOUD SERVICE REPUTATION ATTACKS

Every model of TMS is endangered by some security threats. These threats may either elevate the reputation of a unit with malicious intentions, or ruin that of a trusted one entirely. The security threats that threaten a TMS may sometimes arise from the consumers of the service themselves. Information concerning a user's experience can be obtained from feedback received [20], [21]. However, it can be very difficult to determine which kinds of activities are malicious.

The credibility of reputation systems can be damaged by the entities involved in those systems, intentionally or unintentionally, separately or together with others, based on the given application and social environment of the reputation system. There are basically two types of trust: recommendation trust (RT), which is the trust of the service provider in other service providers, and interaction trust (IT), which is the trust of the service provider in the consumers regarding the use of their services [20], [21]. Each type has many categories into which reputation attacks or misbehaviors of entities can be classified.

Inconsistent behavior: Inconsistent behavior may be strategically exhibited by entities, and their reputations may be estimated inaccurately. This allows them to keep misbehaving and maintain a good reputation. They can misbehave some of the time, demonstrate deception to only some entities, or abruptly change behavior.

Unfair recommendation: Unfair recommendations may be given to others by entities on their own or in collaboration with others to achieve the greatest impact. Unfair recommendations involve lying, misinterpreting the result of a transaction, or making an error during the recommendation process.

Identity management-related attacks: The attacks in this group are determined by the identity mechanism employed by a reputation system. For instance, when a single entity is allowed by the identity scheme to use multiple entities, a malicious entity can exhibit fraudulent behavior and then use its new identity to enter the system and avoid getting a low rating. In addition, when entity A is able to access or store a recommendation given by entity B for C without associating its identity or that of entity B with the recommendation, then it is possible for entity A to influence the rating by modifying or removing the recommendation value. If allowed by the system, entities can deny that they have given ratings, which means they can send unfair ratings without assuming responsibility, making the reputation system inaccurate.

An attack may be a combination of these categories in some situations to cause greater damage. These categories are explained in detail and further separated into subcategories. Depending on the geographical location of the node in MCC, some attacks can be detected, such as collusion attacks and Sybil attacks, where these attacks are often directed from the same geographical locations of the nodes [33]. In addition to the categories of attacks mentioned above that target the reputation system, a cloud reputation system faces the threat of attacks that are targeted toward the cloud systems themselves, for example, free-loading, denial of service (DoS), poisoning, and pollution attacks. Attacks specifically targeting cloud reputation systems are evaluated in this paper.

A visual taxonomy of these reputation attacks is summarized in Figure 1, illustrated as a tree structure. The hierarchy of the different groups of attacks is depicted by the hierarchy of the nodes, while the particular kinds of reputation attacks are denoted by the leaves. An improved understanding of the different kinds of reputation attacks is presented through this illustration, which can help a reputation system developer comprehend different threats so they can then determine the ways in which these threats can be handled.

A. INTERACTION TRUST (DIRECT TRUST)

The trust of service providers in their consumers based on their own interaction experiences is termed interaction trust (IT).

1) INCONSISTENT BEHAVIOR

As mentioned earlier, entities can exhibit inconsistent behavior to acquire a positive reputation while operating strategically. Inconsistency is indicative of either the transactional behavior shown by the attacker or the link between its transactional and recommending behavior, as depicted in the categories given below.

1) Interaction importance: To make the interaction value more accurate, the interactions of service

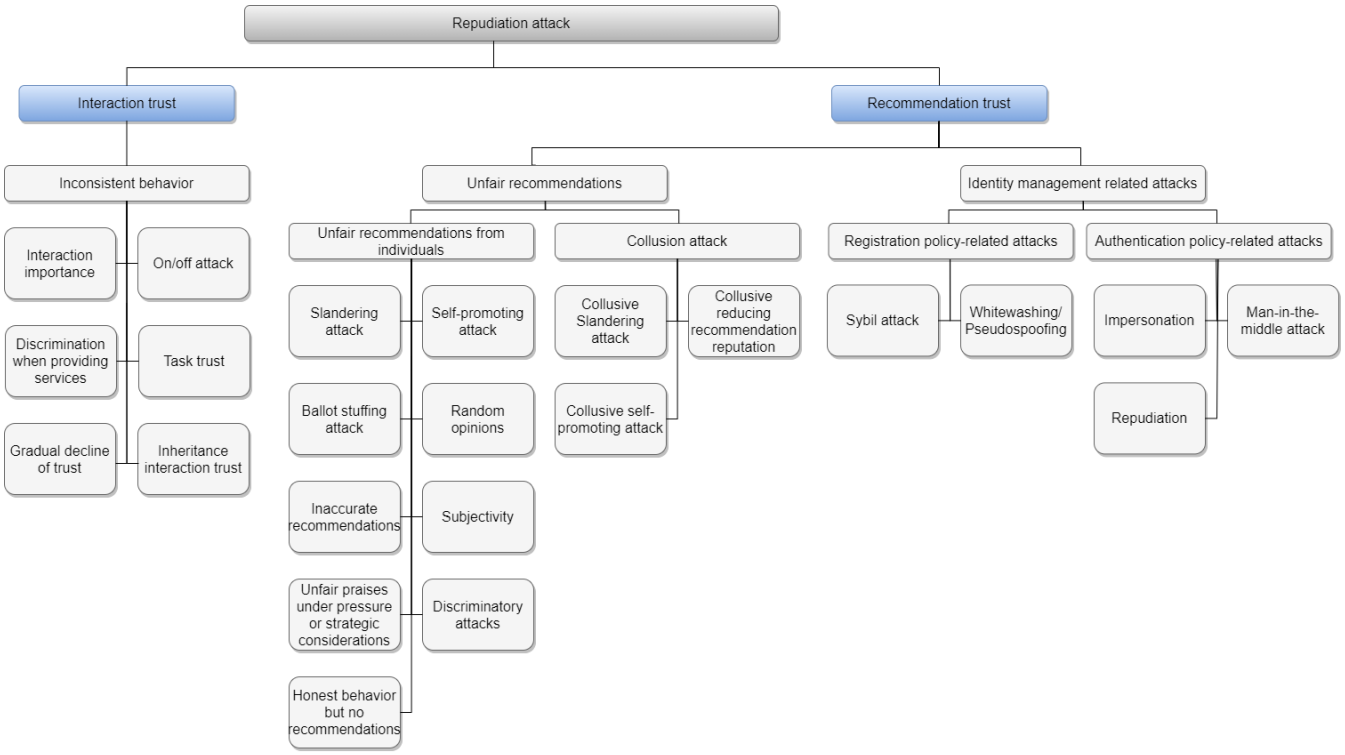

FIGURE 1. Taxonomy for cloud computing reputation attacks.

providers (SPs) are distinguished based on their sensitivity and importance. One of the most important aspects in evaluating trust is interaction importance. The interaction importance structure should be proposed in each trust evaluation model, which allows other service providers to provide recommendations based on interactions with their consumers as a percentage [29]. Researchers have introduced possible prototype models for the calculation of interaction trust. Among these, we have those that use aggregate positive and negative feedback to examine interaction trust, such as [40] and [41], in which the beta function stands out and includes the alpha and beta to evaluate interaction trust. All existing prototypes that use the beta distribution function for the calculation of consumer trust increment alpha by 1 for positive feedback and beta by 1 when feedback is negative. This methodology is not completely accurate, since it does not account for interaction importance. This problem can be solved by using the interaction importance methodology for calculations the trust value based on accurate feedback. In each trust model, the interaction feedback should be expressed in an ordered feedback set from 1 to n, in which 1 represents ''untrustworthy'' and n represents ''highly trustworthy.'' In other words, a feedback set contains n satisfaction levels that the service provider decides on for an interaction. The value for n is a whole number that is controlled by the service administrator of the system, and depends on the complexity of the trust value. This solution can register interaction trust and incorporate an SP's interaction importance into the process of trust evaluation.

2) On/off attacks: Cloud environments often experience on/off attacks in which certain entities first exhibit proper behavior for a given time period to generate a positive reputation. Once they have acquired the trust of other entities, they start their fraudulent activities. Malicious entities usually acquire the trust of the TMS by exhibiting proper behavior in transactions of low value [42]. When a larger opportunity comes their way in significant transactions, they act maliciously. For example, sellers on eBay take part in various small transactions to create a positive reputation, after which they deceive one or more buyers of an expensive item. Because of these abrupt changes in transactional behavior exhibited by an entity, other entities find it difficult to significantly diminish the attacker's reputation [43]. Oscillatory transactional behavior is also part of this category, whereby an entity keeps shifting from honest to malicious behavior, for which it is not easy to update the reputation of the attacker in a timely and effective manner.
3) Discrimination when providing services: Proper behavior may be exhibited by a malicious entity with most entities but then improper behavior toward one or a small group of them. In this way, it manages to get

a good reputation and still causes damage to a few selected targets without significantly harming its own reputation. For instance, a seller may offer good-quality products to all buyers, except a single one. It will appear from the recommendations that the seller is trustworthy, except for a single recommendation coming from the targeted buyer.

4) Task trust: Task trust is a very important item in the trust-based T-RBAC system, where owners of resources can give permissions for consumer roles and tasks. If there is a data leak, the trust model system stops these permissions. Each task represents one operation in any cloud computing service. In order to have a flexible system that is not interrupted, the system identifies the tasks in which data leaks have occurred and then messages owners to prevent users from accessing these tasks [44]. If the user of a role has caused a data leak involving one task, then the trust model will send feedback to other owners to stop this task from accessing resources.
5) Gradual decline of trust: In cloud environments where the trust of the entities directly determines the functionality of the cloud environment, any small hitch in the trust management service that negatively affects the trust of other entities may drive the environment into an uncontrollably rapid descent. In the event that a system defect within a trust management service compels its entities not to trust one another, further operations of the system might be halted [29]. A gradual decline in a system can cause entities to become suspicious that they have been victims of other malicious entities, which might have led to earlier incidents of leakage. The gradual propagation of such a problem leads to distrust in society at large. The whole trust management service can be paralyzed by malicious entities. Such an attack requires only a short period of time to cause the system harm. This issue can proliferate doubt among the entities of a system, and in this manner, malicious entities can incapacitate the entire trust model. To address this issue, rather than placing doubt on all entities, we need a method to diminish malicious entities' influence immediately. This problem can be reduced by establishing a mechanism that promptly decreases the reputation of adversaries when leakage incidents occur, instead of suspecting all entities.
6) Inheritance interaction trust: This is a moral conviction deduced from other roles' interaction histories and their relationships of inheritance with the role. To begin with, there is a need to look at inheritance trust, which considers only the descendant role's interaction history [25]. When a cloud service owner detects a behavior failure of a user with a role R's descendant sub-role, the feedback provided by the owner ought not to be to the descendant sub-role only, but should also impact the trust of the role (since the users who belong to the role are often accessing the data of the owner of a cloud service assigned to the sub-role too, and should also be suspected of initiating a fruitless interaction). This means that an evaluation of role R's trust ought to consider the interaction history from each of its descendant roles, not excluding the sub-role.

B. RECOMMENDATION TRUST (INDIRECT TRUST)

Recommendation trust is a service provider's trust in a consumer by accepting the proposals of other service providers who have interacted with the consumer previously.

1) UNFAIR RECOMMENDATIONS

Unfair recommendations are those that are not indicative of the actual quality of a transaction and do not present an honest review of the trustee's transactional behavior. Such recommendations are made by either a malicious or self-interested recommender, or by someone lacking complete information. Different kinds of attacks are part of this category, based on whether they are given by individual entities or by the strategically functioning collusion of entities. We have classified several types of attacks belonging to the unfair recommendations category as follows:

1) Unfair recommendations from individuals: Positive or negative recommendations (i.e., unfair praise or badmouthing), random perspectives, or incorrect recommendations may be given by individual entities. These include different kinds of attacks.
   - Slandering attack: This is also called a badmouthing attack, where slander can be carried out by a malicious entity (by giving them low recommendations) to unfairly decrease their reputation and, in the process, enhance their own reputation. There is a certain kind of badmouthing in which discrimination is shown when giving recommendations. Here, a malicious entity always gives recommendations in a fair manner, except for a certain entity. In this way, it is considered a good recommender, but can still cause harm to its target.
   - Self-promoting attack: In a self-promoting attack, a malicious entity increases its significance (by giving good recommendations for itself) to enhance its trust value, but then misbehavior is exhibited by the malicious entity. This attack can be managed by not permitting self-recommendations in the determination of trust.
   - Ballot stuffing attack: In a ballot stuffing attack, malicious entities give positive recommendations for other malicious entities in the same group, with the aim of manipulating their own reputation by fraudulently enhancing it. Here, fair recommendations are given by a malicious entity, except when it is for a particular entity. In this way, it is considered a good recommender while effectively enhancing the trust value of its target [45].
   - Random opinions: With respect to reputation systems that reward entities for giving

recommendations (e.g., [46]), random opinions may be given by selfish entities that are not consistent with the actual transactions for the sake of acquiring rewards. Random recommendations may also be given by entities about other entities rather than giving honest recommendations because honestly recommending a party's performance takes much more time and resources. In addition, when a highly reputable recommender gives honest (and positive) recommendations, the recommended entities gain an edge over the recommender because the recommended entity's reputation increases. Therefore, it is evident that when random and honest recommendations lead to the same reward, active participation does not lead to any incentive; rather, there is actually an incentive for giving inaccurate recommendations. Malicious entities could also provide several random opinions, with the intention of giving rise to a DoS attack. A significantly large number of recommendations would then be required by the reputation system, which would lead to a greater cost of communication and a decline in performance.

- Inaccurate recommendations: Inaccurate recommendations can be made when there is a lack of complete information. For example, an entity providing an opinion-based recommendation for another entity may not have much experience with it, and hence have poor confidence in the recommendation. This kind of recommendation is not considered accurate due to the high degree of uncertainty involved. If the provision of the recommender's confidence is supported by the reputation system, this attack can be managed during reputation estimation by different means, for example, disregarding it or not giving much value to recommendations with weak confidence. Sometimes, an incorrect opinion or rating is given by mistake, which may lead to inaccurate recommendations. Entities should be distinguished in accordance with their significance, popularity, and trustworthiness in the field of activity of which they are a part. This means that there is a lack of uniformity in the weight of the recommendations given by entities. It seems at the outset that humans would naturally give more attention to their own opinions and ideas instead of that of another person. Most of the time, an individual will give more importance to their own perspectives and feedback in comparison to the recommendation given by another individual. This means that a person may trust whoever has more skills and experience than themselves in the given field. In summary, individuals are more likely to trust the opinions of an expert in any field than their own views.
- Subjectivity: In some cases, we have more than one value of trust for the same entity. With regard to the differences in recommenders' opinions and experiences, a ''subjectivity'' problem is often encountered in a TMS. This way of thinking affects a number of parts of the TMS in most applications. Owing to the fact that the opinions and references of people concerning trust differ, the TMS experiences subjectivity problems [8]. Personal beliefs, emotions, and feelings influence people's evaluations, behaviors, and judgments. In this manner, an entity needs to change other recommenders' functional trust in any entity and make it in accordance with their own perspective.
- Unfair praise under pressure or strategic considerations: Better recommendations may be given by participants of reputation systems than those deserved by the trustee due to fear of retaliation or expectation of reciprocity. These phenomena were demonstrated empirically by Dellarocas *et al.* [47], using eBay as an example to identify the factors that drive trader involvement in the reputation system. It has been shown that reprisal fears and expectations of reciprocal behavior bring about an artificial increase in positive recommendations. For example, an unjustified positive recommendation can be made by a buyer or seller to encourage the transaction partner to give a positive recommendation in return. In the same way, a 'justified' negative recommendation may not be given by a participant due to fear of getting an 'unjustified' negative recommendation in response.
- Discriminatory attacks: This is also called a conflicting behavior attack, in which non-friends or entities that do not have strong associations (not having many mutual friends) can be selectively attacked by a malicious entity due to human nature or their inclination toward friends within cloud systems. When giving a recommendation for a target entity that is a friend or malicious node, the recommender can give a good service review (that is, carry out ballot stuffing attacks), even when good service is not provided by the target entity. A bad service recommendation may be given if the target is not a friend (which is a badmouthing attack), even when good service is provided.
- Honest behavior but no recommendations: There may be no incentive for honest entities to have a good reputation to offer recommendations, because enhancing others' reputations may not be advantageous for them. When an entity with a good reputation does not give recommendations to other entities, it does not offer them a competitive edge for being chosen as the service provider and instead maintains its own competitive advantage. This kind

of entity behaves like a free-rider by not making any contributions to the reputation system, despite using recommendation information obtained from other recommenders.

2) Collusion attacks: Trust management services are often threatened by collusion attacks, also known as collusive malicious feedback behavior [48], [49]. Collusion refers to an agreement by a collection of entities to establish biased or unrealistic recommendations. This attack takes place in the event that a group of people cooperate with one another through false recommendations aimed at ruining the reputation of someone else, which is known as a slandering attack, or increasing their own position, which is known as a self-promoting attack. The last type is collusive reducing reputation, where the recommendation reputation of honest entities can be decreased by coordinated malicious nodes by badmouthing only some of the entities they deal with. These are the categories of attacks that present threats when a group or groups of malicious entities try to control the system based on their own interests. More serious damage is caused to the reliability of a reputation system in most cases when multiple malicious entities work together than when malicious behavior is exhibited by every entity on its own. Some of the more particular examples of collusion attacks are as follows:
   - Collusive slandering attack: This is also called a collusive badmouthing attack, where certain malicious entities can work together to give negative recommendations about an honest entity and cause serious damage to its reputation. They can also give positive recommendations about each other to enhance their own reputations.
   - Collusive reducing reputation: The reputation of honest entities can be diminished by coordinated malicious nodes through badmouthing only some of the entities they deal with. This is how they produce contradictory views regarding victims' transactional behavior and the reputation of honest recommenders who give opinions about the victims. However, there is no major impact on their own recommendation reputations because they give honest recommendations about other entities.
   - Collusive self-promoting attack: This is also called a ballot stuffing attack, where malicious behavior occurs in the cloud environment by all entities from a malicious group; however, they give positive recommendations for one another. There is another variation of this attack, in which malicious behavior is shown by just one member of the collusive group, while positive reviews are given by others. In the more complicated form of attack, malicious behavior is shown by a single entity for some time to avoid being detected, whereas positive reviews are given by other entities in the group. When an attack of this kind is carried out, it is often referred to as ballot stuffing. In this situation, recommendations are given for fake transactions. For instance, collusion can be established between a seller and a group of buyers in an online auction system to dishonestly give high ratings that are inconsistent with actual transactions. This will cause the seller's reputation to increase, which increases the number of orders the seller receives from other buyers, and they can sell at a greater price than justified.

2) IDENTITY MANAGEMENT RELATED ATTACKS

Reputation is associated with an identity related to an entity; hence, there is a strong relationship between the former and the identity policy employed by a cloud community. There may also be an association between this identity and a real-world identity, or it could be developed without this kind of association. The term pseudonym is used in the latter scenario, which may be a user-defined identifier, a public key, an IP address, or a mix of them that is created, for instance, through concatenation and/or a hash function. On the basis of the identity policy adopted, a single, multiple, or limited number of identities can be obtained by one identity. Some costs may be incurred for creating an identity, such as resolving a resource-consuming problem or paying a registration fee. The identity management system that a cloud system adopts is also linked to the extent of anonymity supported, and hence determines the extent of privacy that an entity can acquire, which is a feature required by most cloud systems. The anonymity level backed by a cloud system depends on the way the following issues are managed: determining the entity that holds/requests/acquires some part of the trust information; linking a specific transaction with a particular entity; and linking a given pseudonym with an actual identity.

It is evident that when more information is related to the identity of an entity (either a pseudonym or a real-world identity), there is a lower level of anonymity and privacy, and a greater level of accountability and reliability of the reputation system that can be attained. Therefore, reputation is a trade-off with the degree of privacy in relation to the extent of accountability that can be attained through the identity policies adopted. Attacks belonging to this category manipulate the kind of identity management adopted and the extent of anonymity backed by a system, and can be categorized into registration policy-related and authentication policy-related attacks.

1) Registration policy-related attacks: Every entity taking part in a reputation system should be registered with the system with some kind of identity in accordance with the identity scheme, which, as explained previously, should describe four features: first, the traceability (vs. anonymity) of an entity, and whether there is a link between the identity and the entity's real-world identity or not (the latter case is referred to as pseudonym); second, the technique used for creating an identity, and whether an entity can create the identity on its own or it

has to be allocated, for example by employing a public key infrastructure (PKI) [50]; third, cost relationship, and whether identity creation requires some kind of cost or is free [51]; and fourth, the uniqueness of the entity's identity, and whether there is a single unique identity or multiple identities for an entity, that may be linked or not linked to one another to represent the same entity.

When pseudonymity is backed by a reputation system and there is no cost related to the creation of new unlinked identities, attacks of the following kinds may take place:

- Sybil attack: Sybil attacks are carried out when multiple identities are created by a single malicious entity, which is then used together to destroy the system [52]. In this kind of attack, a malicious entity can use its various identities to enter the system by acting as a different entity each time. They then offer a lot of incorrect reputation information. It is analytically explained in [53] that a single entity or a group of entities is targeted by Sybil-like attacks in a reputation system. In the former scenario, a malicious unit that has a group of identities can use them to disseminate negative reviews regarding a single user (i.e., self-collusion or badmouthing), or commit fraud against a single user by utilizing a few of its pseudonyms to carry out ballot stuffing (i.e., self-collusion for ballot stuffing). This can be done by distributing the identities into three categories: the service providers, the recommenders that provide false positive reviews for the service providers, and those that enhance the reputation of recommenders with respect to their reliability. The service provider is chosen by the victim based on its reputation, which is deceptive, while the attacker may no longer use its pseudonym. When entities are divided into groups (such as groups of mutually trust entities [53] or neighborhoods of entities [54]) and group reputation is considered for estimating the entity's reputation, then the group reputation can also be damaged by the malicious entity through the Sybil attack. For instance, the attacker can join a group and then exhibit malicious behavior to decrease the group's reputation (insider attack), or become part of distinct groups, generate a good reputation as a recommender, and then propagate negative reviews regarding the target group (outsider attack) to decrease their reputation [55], [56]. As such, the adversary is capable of boosting or ruining the reputation of those entities. An adversary is capable of exploiting multiple fake identities, with the aim of deceiving the TMS and giving misleading feedback for a slandering or a self-promoting attack. Several theories have been proposed to address Sybil attacks, some focusing on enforcing membership policies like [29], and others on building different algorithms in the trust system like [52] and [57], but there are still some challenges.
- Whitewashing/Pseudospoofing: A malicious entity may give up its own identity and enter the system using a new identity to avoid getting a bad reputation [58]. An entity may do so when the reputation of the new entity is greater than its own. This kind of entity is known as a whitewasher or a pseudospoofer when it alters its identity from time to time so that it cannot be recognized. Pseudospoofers act in a different way from what happens in the Sybil attack, as they cannot be easily synchronized and can carry out collusion attacks because their different identities (generated maliciously) are not able to act simultaneously. Therefore, they can exhibit individual attack behavior as explained previously, but they cannot carry out collusion attacks, despite modifying their pseudonym from time to time.

2) Authentication policy-related attacks: When there is no authentication of entities and messages, further attacks can be carried out. Authentication is the process through which the digital identity of the one sending the communication is verified. Different kinds of attacks can be carried out when it is not possible to ensure that the users of a reputation system are actually who they present themselves to be, and that the user carrying out system operations is actually the one authorized to do so. These include:
   - Impersonation: In this kind of attack, a malicious entity presents itself as another entity by stealing the pseudonym of the victim, for instance. In this way, the attacker can exhibit dishonest behavior on behalf of the impersonated entity (therefore having a negative impact on their reputation), or propagate unfair recommendations about others by using the stolen pseudonym (therefore having a negative impact on the reputation of the impersonated entity).
   - Man-in-the-middle attacks: Entities in cloud systems need to depend on intermediate entities to put forward their queries or responses. This also happens in cloud reputation systems, where it is possible for intermediate entities to manipulate the feedback in two ways: not communicating trust information correctly (for example, by omitting or changing recommendations), or privacy infringements, for example, by using reputation information passing through them to understand the recommender's habits. This kind of misbehavior is linked to the inherent tradeoff between trust and privacy.
   - Repudiation: An entity may deny that it has sent, requested, or acquired a recommendation. When

it cannot be confirmed that an entity is guilty for carrying out such actions, malicious entities do not fear being identified or punished and may give unfair recommendations, deny sending a recommendation, give many fake recommendations that create congestion and decrease performance in the reputation system (DoS attack), or unfairly accuse another entity of exhibiting improper behavior (false accusation) while providing recommendations. For instance, when the exchange of recommendations requires the payment of fees by an entity when receiving a recommendation, the receiving entity may falsely deny either asking for or receiving the recommendation, and hence refuse payment. Here, the recommender is not given any reward for making recommendations. In addition, there is a false decrease in its recommendation reputation.

III. OVERVIEW OF TRUST MANAGEMENT

To begin with, trust management must be established for purposes of overcoming the challenges associated with the centralization of security systems, including centralization of trust relationship control, policy language heterogeneity, and inflexibility that makes it impossible to uphold complex trust relationships especially when dealing with large-scale networks. Policy languages set roles of authorization and security policies implementation in trust management. The roles of authorization are authenticated following sets of policies of security that are, in turn, authenticated by some particular credentials. Various previous attempts to implement trust management include KeyNote and PolicyMaker [59], [60]. The techniques are dependent on policy roles for them to execute automated authorization, hence referred to as policy-based trust management. Later, many researchers were inspired by the trust management, and they specified the same concept in a wide array of environments, including e-commerce, Web services, wireless sensor networks, grid computing systems, as well as cloud computing that is most recent [57].

In some cases, the security threat to the TMS comes from the service users themselves, but the quality of different types of feedback can explain much about the experience of the user, as it can be either malicious or not malicious [4], [13]. Attackers may interfere with cloud services by providing misleading feedback (collusion attacks), or they may also create multiple accounts (Sybil attacks) [3], [17]. Such malicious behaviors may lead to a plethora of challenges to detecting these attacks, among which are:

(i) Consumers' dynamism, a situation in which the new users of the cloud services join just in time as the old ones leave the cloud environment, making it almost impossible to detect malicious activities like collusion of feedback;
(ii) Identity Multiplicity, a situation in which in a single user possesses multiple accounts related to one cloud service under different identities, making Sybil attack detection difficult;
(iii) Poor judgment of a user's intentions as to whether malicious or not; and
(iv) Difficulty predicting when to initiate responses to malicious behaviors from attackers (i.e., occasional behaviors vs. strategic behaviors).

The unpredictability of consumers as well as the dynamic nature of the services offered in cloud computing makes it difficult to guarantee the continuous availability of TMS. Thus, it is not appropriate to make use of approaches that are based on consumers' capabilities and interests by measuring the similarity and availability of cloud computing operations [4], [13]. The TMS ought to have a high level of adaptability and scalability in order to provide sufficient and effective services in cloud environments.

Trust is defined from a wide range of perspectives from different literal works. However, this paper adopts the definition by the authors in reference [56] for trust as the degree to which the provider of a cloud service recommendation to depend on the consumer of a cloud service, provisioning the cloud service but expecting particular qualities promised by the provider of the cloud service [2]. For effective establishment as well as evaluation of the trusted relationship, there ought to exist a trust management technique depending on service consumers and service providers perspectives [2], [61]. This paper has classified trust as SPP (Service Providers Perspective) as well as SCP (Service Consumers Perspective). The crucial force behind trust management systems within SPP is the provider of the service. Conversely, the fundamental force behind trust management systems within SCP is the service requester.

A. CLASSIFICATION OF TRUST MANAGEMENT SYSTEMS (TMS)

There exist several works that report different techniques of trust management, grouped in four distinct classes: Reputations, Predictions, Policies, and Recommendations. This paper has explained the trust management from the perspective of service providers (in other words, the perspective of the cloud service providers). However, similar techniques are applicable in the rest of the perspective (in other words, the perspective of the cloud service consumers).

Figure 2 shows the classification of Trust Management Systems in cloud environment as SPP as well as SCP. The main driver of trust management systems in SPP is the provider of the service, where the service providers evaluate the trust value for all service consumers. The unrecognized relation is presented as a dashed line, where this relation happened when the service provider needs to interact with any consumer for the first time. Conversely, the main driver of trust management systems within SCP is the service consumers, where the service consumers evaluate the trust value for all service providers. The unrecognized relation is presented as a dashed line, where this relation happened when

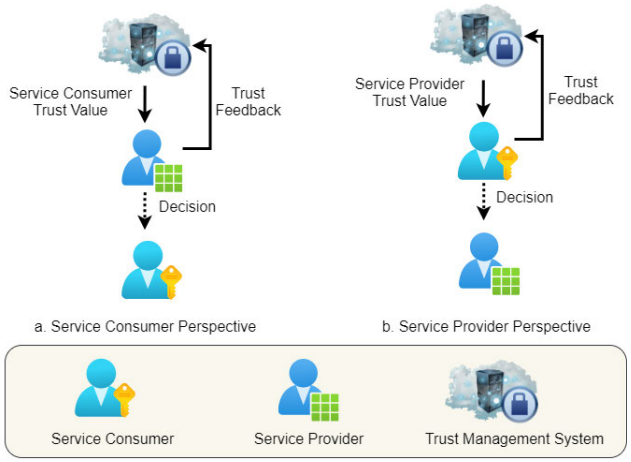

FIGURE 2. Classification of trust management systems.

the consumer needs to interact with any service provider for the first time.

1) POLICY-BASED TRUST

The policy-based trust is among the ancient ways of establishing trust that are highly applied. It has been highly applicable in a wide range of cloud environments [62]–[64], Web applications [65], environments that are service-oriented [66], [67], the grid [68], and the peer-to-peer (P2P) systems [69]. The policy-based trust makes use of some policies, each of which performs different tasks to control the level of authorization and points out a small trust threshold to provide access authorization. The trust credentials or thrust results determine the thresholds and can be obtained using several ways. For example, the auditing and monitoring approach proves violations of Service Level Agreement (SLA) in the services offered in the cloud (in other words, the trustworthiness of a cloud service is determined only upon the satisfaction of SLA) [70]. Entities' credibility approach, on the other hand, points out sets of parameters for measurement of the parties' credibility like quantitative and qualitative attributes such as response time, customer support, security, and availability [71], whereas the feedback credibility approach specifies a set of factors for measuring the feedbacks' credibility. Several factors can be used to measure feedback credibility, including the experience of cloud service consumers (in a nutshell, the quality of feedbacks varies from one individual to the other). A majority of researchers often identify two credibility features, including expertise and trustworthiness [72]–[74].

The literature review shows that policy-based trust can be applicable for all models of cloud service. In 2010, the authors in reference [75] introduced a new language to indicate compliance requirements on the basis of a model-driven method. In 2011, the authors in reference [76] propose a TrustCloud Framework for attaining trust cloud services through SLA detective controls and monitoring mechanisms. In 2014 and 2015, the authors in references [2], [57] presented a credibility framework in which authentic feedbacks are differentiated from deceptive ones.

2) RECOMMENDATION-BASED TRUST

Recommendation-based trust has been used extensively in the field of cloud environment [29], [71], [77], service-oriented environment [78], [79], and the grid [80]. Recommendations exploit the knowledge of participants concerning the trusted parties, more particularly when the involved party knows some information about the trust feedbacks' source. As pointed out in the theory of social psychology, a person's role considerably influences the trust evaluation of another person in the event that a recommendation is given. The commonly known forms of recommendation are the explicit recommendation and the transitive or implicit recommendation. When a consumer of a cloud service recommends a particular type of cloud service in his /her own volition to a well-established relation (such as friends or family), then that is an explicit form of recommendation. Conversely, a transitive form of recommendation occurs in the event that a consumer of a cloud service trusts a particular cloud service due to the fact that at least his/her trusted relations (friend or family) trusts the service.

The study by [81] presented one of the latest attempts of utilizing recommendation-based trust in cloud computing. Trust is acquired in this study from recommendations using various operations, for example consensus (where trust feedbacks are gathered from several cloud service consumers) and discounting (where trust feedbacks are collected depending on the reliability of cloud service consumers). A cloud trust model is introduced in [77] on the basis of transitive trust, in which a series of trusted relationships emerges from a single root of trust. Recommendation-based trust can be applied to all of the three cloud service models in the same way.

3) REPUTATION-BASED TRUST

Despite being related, trust and reputation are distinct from each other. Trust is fundamentally between two entities, whereas reputation refers to the overall opinion of a community regarding that entity. An entity with high reputation is generally trusted by majority of the entities in that community. When organizations need to make a trust judgment on another trustee, they may use the reputation to measure or determine the degree of trust of that entity. Cloud computing, grid, service-oriented, and P2P networks are extensively employed by reputation systems. The users' choice of cloud services will certainly be affected by the reputation of cloud services or cloud service providers, and this is why cloud providers try to create and sustain their reputation. Reputation-based trust inherently has the objective of judging trust in cloud computing. To measure reputation, an overall score that represents the general opinion is usually obtained. It may also be gauged by determining separate scores on various different areas of performance. Calling on the numerous

cloud users to provide ratings for a cloud service or service provider against various complex and intricate criteria is an impractical task. The reputation of a cloud service provider represents the general perspective of the community regarding that entity. Hence, it is quite helpful for the cloud users (mainly individual users) to select a cloud service provider from the large number of options available. Reputation may play an important part in the beginning when users are seeking a service; however, it is not sufficient later on. This is because as the service is used, the trust of the user on that service fulfilling performance or reliability requirements changes on the basis of that experience.

Reputation-based trust is an essential technique since the feedbacks different consumers of cloud services are capable of influencing a particular cloud service's reputation dramatically either to the positive or negative. The cloud environment [42], [71], [77], as well as the service-oriented environment [78], [82], the grid [83], P2P [74], [84], [85], has extensively made use of reputation-based trust. Reputation, on the other hand, is capable of having a direct or indirect effect on a particular entity's trustworthiness (for instance, cloud service), as discussed by a majority of researchers like [57] and [72]. Contrary to the situation in recommendation-based trust, the consumers of cloud service in reputation-based trust have no knowledge of the trust feedback source. In a nutshell, there exist no trusted relations in the reputation-based trust. A lot of reputation-based systems exist online, among which are the auction systems (such as Amazon and eBay) were used as well as new commodities are sold and bought. Such systems also provide platforms in which the opinions of a cloud service consumer, as well as reviews on specific services or products, are freely expressed.

In the same way, reputation-based trust has been used in various existing studies to manage trust in cloud computing. The study by Habib *et al.* [81] concentrates on combining the reputation of a given cloud service on the basis of feedback through Quality of service (QoS) and other features (such as geographical location, elasticity). This method can be used in various cloud service models. A reputation-based trust model has been presented in [77], the basis of which is IaaS cloud services. In addition, the reputation-based trust management model proposed by Noor *et al.* [2], [56], [57] differentiates authentic feedbacks from those that are deceptive.

4) PREDICTION-BASED TRUST

In the event that there does not exist any prior information concerning the interactions of a cloud service, prediction-based trust becomes very useful then (for example, lack of historical records of previous interactions). Proposals have been made concerning prediction-based trust in both the service-oriented environment [79], [86] and the cloud environment [2], [57], [71]. Essentially, the underlying idea behind this technique is that entities that are similar-minded (for example, consumers of a particular cloud service) have a higher probability of trusting each other. This technique can be applied in the refining of the results of trust and in increasing the credibility of the feedback concerning the trust.

A similar method (i.e. differentiating like-minded cloud service customers) to distinguish reliable feedbacks from the deceptive ones was introduced by Brooks [3] Noor *et al.* [56], [57]. Prediction-based trust was employed by Habib *et al.* [81] to improve the quality of feedback. Here, the consensus of feedbacks (i.e. where the feedbacks on a cloud service are identical to a trustord is trust) is used to achieve trustworthiness of cloud service customers. Using prediction-based trust, the trust results can be refined and the reliability of trust feedbacks can be enhanced.

IV. QUALITATIVE ANALYSIS FOR TRUST MANAGEMENTS

This section explains the trust management generic analytical framework in a cloud environment. In a cloud environment, interaction takes place in three layers. We will discuss a particular bunch of properties and analyze them accordingly in the below sections. Trust is a complete obstruction in light of authorization and the security of what we know as cloud computing [87]. Moreover, overseeing trust feedbacks in cloud conditions is a troublesome issue because of the varying number of cloud administration consumers and the profoundly influential sort of cloud conditions. The TMS system enhances the security of cloud services with all cloud environment conditions. Specifically, we present this model as a versatile validity model that recognizes the malevolent feedbacks by reflecting the cloud administration consumers' feedbacks on the service provider trust values and applying the different detection methodologies.

The way of communication, interaction, and computing resources approach has substantially changed due to quickly growing Internet-based services. The service issues related to trust management have been the attraction of many researchers. Trust management approaches are very helpful in developing faith between the consumers and providers of cloud service, and it increases the growth of it. There are very abnormal and malicious behaviors that affect the efficiency of it. Therefore, we need to apply several methods to overcome these types of abnormal and malicious behavior.

Although there are a lot of advantages given by distributed computing, the exceptionally unique, circulated, and nature that is non-straightforward of cloud administrations advances a lot of difficulties that should be completely tended entirely to before guaranteed advantages of distributed computing can be figured out. Trust is generally viewed as an essential segment of the accomplishment of Internet-based administrations.

A. TRUST MANAGEMENT LAYERS ANALYSIS

There are three layers of trust management and each layer has different features, and we recognized a set of measurements where we went through many trust management issues. The highly distributed, dynamic, and non-transparent cloud nature evaluates the identification of the features. Now, we will go

thoroughly into these headings and find out all the properties of each layer.

1) RECOMMENDATION LAYER

This layer deals with trust recommendations, which involve consumers and providers of different cloud services. Recommendation Layer comprises of various parties involving providers, and services consumers that are trustable for each other. The feedback shared between these parties is likely to be maintained by Feedback Collector. The storage of feedbacks relies upon systems of trust management in a systematic manner of the cloud environment via trusted cloud SPs. This layer contains the following properties:

1) Entity's and feedback credibility: Information that establishes a trust relationship among cloud service providers or consumers is called credible information, and this quality is known as credibility. Entity's credibility and Feedback credibility are some forms of credibility evaluation [88]. As there is a direct relation between identification and credibility; therefore, service providers and cloud consumers use a proper identification scheme to process parallel data. For example, Sybil attacks can occur if there is no complete identity scheme used. These attacks decrease the accuracy of results.
2) Privacy of cloud service consumers information: The privacy property indicates a certain degree of sensitive information disclosure that the service consumer may face while interacting with the trust management system. There may be various causes related to privacy breaches, which could occur as leaks of sensitive information related to the data of service consumers. In this regard, password, username, address, and date of birth are the prime examples. Moreover, behavioral information such as with whom the consumers of cloud services interacted may also be indicated as examples of privacy data. Moreover, cryptographic encryption techniques might decrease the utilization of data, and the anonymization techniques are inappropriate in cloud computing environments due to their highly distributed and dynamic nature, where these technologies will remove consumers' identification information [57].
3) Integration of trust techniques with the trust management system: As far as integration is concerned, it reflects on the ability to fully integrate various perspectives of trust management. To integrate various perspectives of trust management fully, cloud service providers might send their feedback in terms of different perspectives via trust management techniques. In short, combining various trust management techniques like reputation, policy, prediction, and recommendation techniques can quickly increase the efficiency and accuracy of the result derived by different trust management.

2) EVALUATION LAYER

The center of any trust management system lies in this layer. This layer controls a large number of queries of trust evaluation from various parties with the help of a module called the Results Divider and Trust Judgments [85]. It mainly involves how to check the results of the trust database and helps to perform the key evaluation with the help of various trust management techniques. Evaluation Layer forms a connection to deliver test results through results distributor and trust evaluation. The procedure is conducted to prevent redundancy problems in the process of trust evaluation. This layer contains the following properties:

1) Trust management perspectives: In cloud environment, trust management perspectives generically emphasize the views of service providers. Besides, others are most likely to focus on the views of service consumers [89]. Thus, it is vital to assess the perspective supported by a trust evaluation function. The comprehensive trust management system can only be developed by supporting more perspectives trust management system.
2) Trust evaluation techniques: To control trust feedbacks in a cloud environment, this property refers to the level to which a technique can be utilized by the trust management system to evaluate and manage trust feedbacks. There should be a clear differentiation between the ones that choose many trust controlling techniques and the ones that stick to others' trust management styles [90]. There is a clear difference between the functions of trust evaluation which will implement a specific technique for trust management. The more trust management techniques better will be the efficiency of test results.
3) Adaptability of trust management systems: Adaptability is mainly concerned with how to adapt to a change of interested parties (cloud service consumers or providers). For this purpose, various trust evaluation inquires may be followed to customize the criterion of interested parties. In this regard, updating feedback and size of the interaction may be used to ensure the notion of adaptability with interested parties.
4) Trust management system scalability: The system of trust management must be scalable to grow in many aspects (such as the volume of available trust findings, the amount of trust evaluation inquiries that can be managed in a specific time period, and the amount of trust relations that can be facilitated) because the nature of the cloud environment is highly dynamic and diversified. Many problems evolved in a centralized architecture of trust management systems, which are scalability, availability, and security.
5) Attacks detection: This unique property sheds light on the degree of robustness related to the trust evaluation function to prevent malicious attacks. As discussed above, there may be two security scales, namely the evaluation function security scale, and the

communication security level. When it comes to the evaluation communication security scale, it indicates potential security threats against the trust evaluation function such as slandering and self-promoting, whitewashing. Moreover, the communication security level indicates a Man-in-the-middle (MITM), DoS, and distributed denial-of-service (DDoS) attacks.

6) Applicability of trust management systems: The property emphasizes the degree that to what extent the trust evaluation function might be adopted to support trust management systems which are deployed for cloud services. It is pertinent to differentiate the kinds of cloud services where the trust evaluation function is suitable. When the trust evaluation function supports many different types of cloud services, it becomes more comprehensive.

3) RESULT LAYER

Cloud service consumers and providers are also involved in this layer like the Recommendation Layer, which involves the issues of trust evaluation inquiries of other parties. Inquiries related to trust evaluation are supposed to be transmitted to the trust evaluation function via trust result distribution and module of trust. Cloud service consumers and providers have access to final results, and they are maintained in a TMS database. This layer contains the following properties:

1) Response time of trust inquiries: It refers to the time in which the trust management system does require managing trust evaluation inquiries so that feedbacks and results may be accessed mainly when it comes to a significant number of supported trust relationships. For example, the trust management system will handle a low number of inquiries when the trust management system requires a lengthy response time.
2) Redundancy: This property indicates redundancy support, which the trust management system does maintain to assess and manage the service providers' feedbacks. There may be two redundancy approaches namely the evaluation redundancy (which refers to the redundant procedures of duplication that is carried out by the trust evaluation function) that takes place when there is sequential issuance of multiple trust evaluation inquiries, and the trust data redundancy (which is the duplication of the trust data which consists of feedbacks and trust outcomes) that is employed to prevent issues of scalability and supervision. In short, redundancy brings about resource waste. As a result, it affects the performance of the trust management system negatively.
3) Accuracy of trust results: When it comes to accuracy, it highlights the degree of correctness of distributed trust results. These results may be assessed by different characteristics. The characteristics may include the unique identification of feedbacks and using the proper evaluation function security scale. However, poor identification of cloud feedbacks results in inaccurate results. Moreover, the lack of a complete evaluation security function is likely to make the trust management system more penetrable than earlier. In this case, the results of a distributed trust system may also get manipulated by the threats and attempts of attackers.
4) Security of trust management system: This property demonstrates the link between trust evaluation and provides protection to distributors from hostile attacks and actions. In this regard, ''the access control level'' assesses if the trust management system uses access control techniques for the trust results distribution. On the other hand, the security commination level is quite the same as to trust evaluation layer. In short, if results distributors and trust evaluation systems have higher security, then it also makes the trust management system more reliable and protected.

V. RESEARCH PROTOTYPES

An outline of a group of representative research prototypes on trust management is explained in this section. An analysis and comparison of these research prototypes is then carried out by employing assessment components.

A. OVERVIEW OF MAJOR RESEARCH PROTOTYPES

Various representative trust management research prototypes on cloud computing are briefly explained here.

Trust Enhanced Cryptographic Role-based Access Control: A trust model is presented by Lan *et al.* in [6] to describe and enhance the security provided for stored data in cloud storage systems that employ cryptographic RBAC systems. This facilitates reputation and recommendation-based trust management of the cloud services. The emphasis of the model is on the viewpoints of service providers. In addition, the model put forward has a decentralized configuration, in which each service requester gives his/her personal view regarding the reputation of a service customer. This trust model offers a mechanism to the owners and roles to measure the trustworthiness of individual roles and users respectively in the RBAC system. Role inheritance and hierarchy are considered by the recommended trust models in assessing the trustworthiness of roles.

TrustRBAC: A unique role-based access control model that was founded on the basis of trust management was presented by Chaitali and Bhilare [27] for single and multi-domain cloud settings. This model backs recommendation and reputation-based trust management of the cloud services. The direct trust and recommendation trust is determined by the model using security policies for the two domains. The focus of the model is on the service customers' point of view. There is a decentralized configuration of the proposed model, in which every service requester presents their own views regarding the reputation of a service provider. The owners can use this to determine the degree of trustworthiness of the roles and the roles can determine whether a particular user is trustworthy or not. Nonetheless, there are a few security

challenges of these models; for instance, they are susceptible to collusion attacks from time to time.

Trust and Reputation-Based RBAC Model: A unique trust and reputation-based RBAC model was presented by Mahdi *et al.* in [29] that is not only able to adequately bear the security threats of trust-based RBAC models, but can also be scaled because of their satisfactory execution time. The emphasis of the methods is on the viewpoint of service providers. The model put forward is decentralized in nature, where the service providers give their own opinions regarding the reputation of a service customer. Reputation and recommendation-based trust management of cloud services are supported by this model.

CloudArmor: A CloudArmor was presented by Noor *et al.* in [56] that facilitates reputation-based trust management of cloud services. The emphasis of this model is on the viewpoints of cloud service customers as well as providers, which backs reputation as well as prediction-based trust management of the cloud services. A plan operation of CloudArmor is described that presents a series of functionalities for offering trust as a service (TaaS), comprising of a distinct protocol for proving the credibility of trust feedbacks and the confidentiality of reservation users. The model also defines an adaptive and robust credibility model for finding out the extent to which trust feedbacks are capable of securing cloud services from troll users and comparing the trustworthiness of cloud services and an availability model through which the accessibility of the decentralized function of the trust organization service can be regulated. To verify the potential and advantages of this approach, a prototype and experimental study is carried out by employing a collection of real-world trust on the cloud. The applicability of the technique and its ability to identify malicious activities is shown by the experimental findings.

Sla-based trust model: A trust model is presented by Alhamad *et al.* in [62] for cloud computing on the basis of SLA information that facilitates policy-based trust management of the cloud services. In this model, the emphasis is on the views of cloud service customers. This study explains the prerequisites and the advantages of employing SLA for trust modeling within cloud environments. In addition, it offers a high level architecture that encompasses the main capabilities required and offers a protocol for the trust framework. The SLA is basically a legal format that explains how the service delivery will be carried out and offers a framework for service fees. This framework is followed by the service providers to make their use of infrastructure optimal so that the decided terms of services can be fulfilled. The SLA is used by service customers to obtain the quality of service they require and to sustain acceptable business models so that they can continue to provide services in the long run.

Trusted Cloud Computing Platform: A trusted cloud-computing platform (TCCP) is introduced by Santos *et al.* in [63] that facilitates policy-based trust management of cloud services and presents a closed box execution setting for the IaaS services. Confidential execution of guest virtual machines is also ensured through TCCP. In addition, it allows clients to attest to the IaaS provider and to ensure the security of the service before introducing their virtual machines (VMs) into the cloud. The focus of the model is on the perceptions of cloud service customers. TCCP has the following design objectives: 1) to ensure that the VM execution remains within the secure perimeter; 2) to prevent a sysadmin with root license from accessing the memory of a VM hosted within a physical node. The existing methods are used by TCCP to develop trusted cloud computing platforms which concentrates on resolving privacy issues regarding the customers' data and regarding the computation assigned to the cloud. The TCCP prevents the sysadmin from accessing or changing the content of operational VMs.

Accountability as a service for the cloud: Yao *et al.* introduces a unique design in [64] for achieving robust accountability in the Service Oriented Architecture employed in the Cloud that facilitates policy-based trust management of the cloud services. This accountability ensures that the faults are rightly and irrefutably assigned to their causes. Hence, compliance can be imposed by the Accountability Service on the service providers who are involved in business transactions in the Cloud. The emphasis of this model is on the viewpoints of cloud service customers.

TrustCloud: The TrustCloud framework for achieving accountability and trust in cloud computing was put forward by Ko *et al.* [76]. The viewpoints of cloud service customers are emphasized in this model with the aim of imposing cloud accountability and auditability so that policy-based trust management of the cloud services can be accomplished. A centralized framework is employed in this framework, along with monitoring approaches and detective controls so as to attain trusted cloud services. TrustCloud specifically includes five layers for attaining accountability in cloud settings, which are workflow, data, system, policies and laws and regulations. These layers ensure the cloud accountability life cycle that comprises of seven phases, which are policy planning, logging, sense and trace, reporting and replaying, safe-keeping of logs, auditing and optimizing and rectifying.

Introducing the trusted virtual environment module: A novel technique for incorporating trust in a cloud computing setting was presented by Krautheim *et al.* in [77], known as the Trusted Virtual Environment Module (TVEM). The perceptions of cloud service consumers as well providers are emphasized in this model, which facilitates the recommendation and reputation-based trust management of cloud services. The TVEM can be used to solve the main security issues of cloud computing as it allows parties to develop trust relationships. Here, a virtual environment is generated and operated by an information owner over a platform provided by another service provider. The TVEM is a software application that offers improved features for cloud virtual environments over prevailing Trusted Platform Module virtualization methods, consisting of an enhanced application program interface, flexibility of cryptographic algorithm and modular architecture that can be modified. A distinct Trusted

TABLE 1. Comparison of security and accuracy.

Prototypes			[6]	[27]	[29]	[56]	[62]	[63]	[64]	[76]	[77]	[81]	[90]	[91]	[92]	[93]	[94]
Recommendation Layer	Entity's and feedback credibility	Feedback credibility	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓
		Entity's credibility	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
	Privacy of cloud service consumers information	Service consumers privacy	✓	✓	✓	✗	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓
		Service providers privacy	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Integration of trust techniques with the trust management system	Strong use of feedbacks combination	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓
Evaluation Layer	Trust management perspectives	Service consumer perspective	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
		Service provider perspective	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓
	Trust evaluation techniques	Policy-based trust	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓
		Recommendation-based trust	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓
		Reputation-based trust	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✓	✓
		Prediction-based trust	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
	Adaptability of trust management systems	Full	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
		Partial	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗
	Trust management system scalability	Centralized	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Decentralized	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Attacks detection	Assessment Function level	✓	✓	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓
		Communication level	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
	Applicability of trust management systems	IaaS	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
		PaaS	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓
		SaaS	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓
Result Layer	Response time of trust inquiries	Strong emphasis of assessment time	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗
	Redundancy	Assessment Redundancy	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
		Trust Data Redundancy	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Accuracy of trust results	Full	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗
		Partial	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓
	Security of trust management system	Access control level	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Communication level	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗

Environment Key is denoted by the author that integrates trust from the information owner and the service owners to develop a dual root of trust for the TVEM which is different for every virtual environment and not the same as the platform's trust.

Towards a trust management system: A multi-dimensional Trust Management (TM) system model for a cloud computing setting was put forward by Habib *et al.* in [81]. The focus of this model is on the viewpoints of cloud service customers, which facilitates the recommendation, reputation and prediction-based trust management of the cloud services. There is a unique feature in the system for the customers, enabling them to choose from different sources and roots of trust information (such as property certificates through remote attestation, user statements, conformance to audit standards through Cloud Controls Matrix) based on which the trust scores are calculated. There is a decentralized configuration of the suggested model, where the perspective of every service customer regarding a service provider's reputation is noted.

Trust Management System for Grid and Cloud Resources: A trust model was introduced by Manuel *et al.* in [90] to assess the grid and cloud resources through a resource broker. The emphasis of the model is on the viewpoints of cloud service customers that facilitates the reputation and policy-based trust management of cloud services. A suitable grid/cloud resource is selected by the resource broker in heterogeneous environment on the basis of the user requirements. Metrics that were appropriate for grid as well as cloud resources were considered in this model. The trust value of the resources is assessed by trust enhanced resource broker on the basis of both the identity and the behavioral trust.

Security-Aware Cloud Architecture: A security-aware cloud architecture was presented by Hwang *et al.* in [91], [92] that makes use of Virtual Private Network (VPN) and Secure Socket Layer (SSL) to ensure that communication is secure. The focus of the research is on distinct trust management viewpoints, for example that of the cloud service provider and the customers, and this facilitates the policy-based trust management of the cloud services. From the point of view of the service provider, the architecture that has been presented employs the trust negotiation and the data coloring (integration) method on the basis of the fuzzy logic method and the Public-Key Infrastructure (PKI) for verification of the cloud service customer. With respect to the viewpoint of the service customer, the Distributed-Hash Table (DHT)-based trust-overlay networks in various data centers are employed by the proposed model to attain a reputation-based trust management approach. Despite the claim that the architecture is reputation-based, in reality, it is founded on pre-established policies that examine the authenticity of cloud services. This means that the security aware cloud system is actually a policy-based trust management system as the reputation depends on the perspectives of other trusted participants (such as cloud service customers' feedbacks) regarding a particular cloud service.

Certificateless Hybrid Signcryption: A unique certificateless hybrid signcryption (CL-HSC) model without pairing was presented by Wei *et al.* in [93], where just the partial private key for users is generated by the private key generator (PKG). It possibly gains security within the Elliptic Curve Computational Diffie-Hellman (EC-CDH) assumption in the random oracle model. The emphasis of the model is on the service customers' opinions regarding the security of cloud resources. A key derivation technique was presented by the authors in which only the master key needs to be maintained by the data owner to eliminate intricate key management. When our proposed CL-HSC system is integrated with the key derivation approach, an efficient and secure data-sharing mechanism for cloud storage is presented, which is able to prevent collusion attacks, replay attacks and spoofing attacks and can attain user revocation with ease.

Decentralized Trust Management System: A distinct prototype of the decentralized trust management system (DTMS) was presented by Xiao *et al.* in [94] on the basis of the blockchain technologies. The focus of the model is on the viewpoints of cloud service customers as well as providers. In contrast to the traditional and centralized trust management system, a decentralized consensus-based trust assessment model and blockchain-based trust storage system is utilized by DTMS, which offers a transparent assessment process and irrevocable storage of trust credits. In addition, blockchain efficiency is enhanced through the model by using just the trusted nodes in the verification and consensus procedure. Furthermore, a trusted execution environment (TEE) is creatively implemented by the design system to provide protection to the trust assessment process along with an incentive model that is used to bring about increased participation and reprimand malicious actions.

B. COMPARISON OF SECURITY AND ACCURACY

Any type of trust management service is vulnerable to a variety of attacks [95]. These attacks have the potential to either enhance or destroy the reputation of a specific entity [36], [96]. In order to build an accurate and secure trust model system, we focus on implementing various metrics to prevent these attacks, which enables us to create a stable, reliable, and accurate trust model framework. Table 1 shows the comparison between 15 related works.

VI. CONCLUSION

To ensure the functionality of cloud services, it is important to have robust and reliable reputation systems. Because the majority of trust systems and studies in the field of decentralized reputation systems do not examine realistic adversary models that may comprise complex and coordinated attacks, a detailed analysis of threats faced by reputation systems is offered by presenting a classification of reputation attacks. We explained the major categories and subcategories into which the attacks could be divided. In this study, we have presented the taxonomy for trust criteria and reputation attacks in cloud computing. Also, some of the fundamental concepts

regarding trust management of services within cloud environments have been presented, along with the latest technologies. The main characteristics of the cloud services and their models were specifically reviewed. The trust management viewpoints were then distinguished and the trust management methods were categorized into four groups. A generic model is presented that comprehensively views the issues pertinent to trust management during interactions occurring in a cloud setting. A comparison of 15 representative trust management research samples in cloud computing and the appropriate research domains was also carried out by employing this analytical model. There are three layers in the model, and a series of dimensions are further determined for every layer (which are the assessment criteria), which serve as the criteria to evaluate these research prototypes.

FUTURE WORK

Several studies have concentrated on the topic of cloud service trust; however, there are many issues to be tackled. We will incorporate additional criteria in our work to improve the trust model's security. In particular, we will look for other forms of reputation attacks that could jeopardize the cloud computing system's security and recommend measures to overcome them.

REFERENCES

[1] J. Liang, M. Zhang, and V. C. M. Leung, "A reliable trust computing mechanism based on multisource feedback and fog computing in social sensor cloud," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5481–5490, Jun. 2020.
[2] T. H. Noor, Q. Z. Sheng, and A. Bouguettaya, *Trust Management in Cloud Services*. Berlin, Germany: Springer, 2014.
[3] T. T. Brooks, Ed., *Cyber-Assurance for the Internet of Things*. Hoboken, NJ, USA: Wiley, 2017.
[4] S. Bhatt, F. Patwa, and R. Sandhu, "An access control framework for cloud-enabled wearable Internet of Things," in *Proc. IEEE 3rd Int. Conf. Collaboration Internet Comput. (CIC)*, Oct. 2017, pp. 328–338.
[5] M. Firdhous, O. Ghazali, and S. Hassan, "Trust management in cloud computing: A critical review," 2012, *arXiv:1211.3979*.
[6] L. Zhou, V. Varadharajan, and M. Hitchens, "Trust enhanced cryptographic role-based access control for secure cloud data storage," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2381–2395, Nov. 2015.
[7] T. Bhattasali, R. Chaki, N. Chaki, and K. Saeed, "An adaptation of context and trust aware workflow oriented access control for remote healthcare," *Int. J. Softw. Eng. Knowl. Eng.*, vol. 28, no. 6, pp. 781–810, Jun. 2018.
[8] D. Marudhadevi, V. N. Dhatchayani, and V. S. S. Sriram, "A trust evaluation model for cloud computing using service level agreement," *Comput. J.*, vol. 58, no. 10, pp. 2225–2232, Oct. 2015.
[9] W. T. Tsai, P. Zhong, X. Bai, and J. Elston, "Role-based trust model for community of interest," in *Proc. IEEE Int. Conf. Service-Oriented Comput. Appl. (SOCA)*, Dec. 2009, pp. 1–8.
[10] M. Varsha and P. Patil, "A survey on authentication and access control for cloud computing using RBDAC mechanism," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 12, pp. 12125–12129, 2015.
[11] P. Zhang, Y. Kong, and M. Zhou, "A domain partition-based trust model for unreliable clouds," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2167–2178, Sep. 2018.
[12] N. Iltaf, A. Ghafoor, and M. Hussain, "Modeling interaction using trust and recommendation in ubiquitous computing environment," *EURASIP J. Wireless Commun. Netw.*, vol. 2012, no. 1, pp. 1–13, Dec. 2012.
[13] Z. Tan, Z. Tang, R. Li, A. Sallam, and L. Yang, "Research on trust-based access control model in cloud computing," in *Proc. 6th IEEE Joint Int. Inf. Technol. Artif. Intell. Conf.*, vol. 2, Aug. 2011, pp. 339–344.
[14] A. Barsoum and A. Hasan, "Enabling dynamic data and indirect mutual trust for cloud computing storage systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 12, pp. 2375–2385, Dec. 2013.
[15] W. W. Smari, P. Clemente, and J.-F. Lalande, "An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system," *Future Gener. Comput. Syst.*, vol. 31, pp. 147–168, Feb. 2014.
[16] M. E. Whitman and H. J. Mattord, *Implementing Information Security*. Boston, MA, USA: CENGAGE Learning, 2012, pp. 433–469.
[17] X. Li and J. Du, "Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing," *IET Inf. Secur.*, vol. 7, no. 1, pp. 39–50, 2013.
[18] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proc. IEEE*, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.
[19] W. Chang, F. Xu, and J. Dou, "A trust and unauthorized operation based RBAC (TUORBAC) model," in *Proc. Int. Conf. Control Eng. Commun. Technol.*, Dec. 2012, pp. 811–814.
[20] S. T. Alshammari, A. Albeshri, and K. Alsubhi, "Integrating a high-reliability multicriteria trust evaluation model with task role-based access control for cloud services," *Symmetry*, vol. 13, no. 3, p. 492, Mar. 2021.
[21] S. T. Alshammari, A. Albeshri, and K. Alsubhi, "Building a trust model system to avoid cloud services reputation attacks," *Egyptian Informat. J.*, 2021.
[22] L. Zhao, S. Liu, J. Li, and H. Xu, "A dynamic access control model based on trust," in *Proc. 2nd Conf. Environ. Sci. Inf. Appl. Technol.*, vol. 1, Jul. 2010, pp. 548–551.
[23] L. Zhou, V. Varadharajan, and M. Hitchens, "Integrating trust with cryptographic role-based access control for secure cloud data storage," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 560–569.
[24] G. Lin, D. Wang, Y. Bie, and M. Lei, "MTBAC: A mutual trust based access control model in cloud computing," *China Commun.*, vol. 11, no. 4, pp. 154–162, Apr. 2014.
[25] C. Zhu, H. Nicanfar, V. C. M. Leung, and L. T. Yang, "An authenticated trust and reputation calculation and management system for cloud and sensor networks integration," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 118–131, Jan. 2015.
[26] X. Li, H. Ma, F. Zhou, and X. Gui, "Service operator-aware trust scheme for resource matchmaking across multiple clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1419–1429, May 2015.
[27] C. Uikey and D. S. Bhilare, "TrustRBAC: Trust role based access control model in multi-domain cloud environments," in *Proc. Int. Conf. Inf., Commun., Instrum. Control (ICICIC)*, Aug. 2017, pp. 1–7.
[28] S. Chakraborty and I. Ray, "TrustBAC: Integrating trust relationships into the RBAC model for access control in open systems," in *Proc. 11th ACM Symp. Access Control Models Technol.*, 2006, pp. 49–58.
[29] M. Ghafoorian, D. Abbasinezhad-Mood, and H. Shakeri, "A thorough trust and reputation based RBAC model for secure data storage in the cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 4, pp. 778–788, Apr. 2019.
[30] L. Huang, Z. Xiong, and G. Wang, "A trust-role access control model facing cloud computing," in *Proc. 35th Chin. Control Conf. (CCC)*, Jul. 2016, pp. 5239–5242.
[31] K. Papadakis-Vlachopapadopoulos, R. S. González, I. Dimolitsas, D. Dechouniotis, A. J. Ferrer, and S. Papavassiliou, "Collaborative SLA and reputation-based trust management in cloud federations," *Future Gener. Comput. Syst.*, vol. 100, pp. 498–512, Nov. 2019.
[32] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, and P. D. Drobintsev, "Trust management in a blockchain based fog computing platform with trustless smart oracles," *Future Gener. Comput. Syst.*, vol. 101, pp. 747–759, Dec. 2019.
[33] C. A. Kerrache, F. Ahmad, Z. Ahmad, N. Lagraa, F. Kurugollu, and N. Benamar, "Towards an efficient vehicular clouds using mobile brokers," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, Apr. 2019, pp. 1–5.
[34] R. Hussain, D. Kim, J. Son, J. Lee, C. A. Kerrache, A. Benslimane, and H. Oh, "Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2441–2448, Aug. 2018.
[35] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.
[36] H. Yu, Z. Shen, C. Leung, C. Miao, and V. R. Lesser, "A survey of multi-agent trust management systems," *IEEE Access*, vol. 1, pp. 35–50, 2013.
[37] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust management of services in cloud environments: Obstacles and solutions," *ACM Comput. Surv.*, vol. 46, no. 1, pp. 1–30, 2013.

[38] D. Fraga, Z. Bankovic, and J. M. Moya, "A taxonomy of trust and reputation system attacks," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 41–50.

[39] P. L. Sun and C. Y. Ku, "Review of threats on trust and reputation models," *Ind. Manage. Data Syst.*, to be published.

[40] A. Josang and R. Ismail, "The beta reputation system," in *Proc. 15th Bled Electron. Commerce Conf.*, vol. 5, 2002, pp. 2502–2511.

[41] P. Van Gorp and M. Comuzzi, "MyPHRMachines: Lifelong personal health records in the cloud," in *Proc. 25th IEEE Int. Symp. Comput.-Based Med. Syst. (CBMS)*, Jun. 2012, pp. 1–6.

[42] A. P. Nasution, V. Suryani, and A. A. Wardana, "IoT object security towards on-off attack using trustworthiness management," in *Proc. 8th Int. Conf. Inf. Commun. Technol. (ICoICT)*, Jun. 2020, pp. 1–6.

[43] W. Fang, N. Cui, W. Chen, W. Zhang, and Y. Chen, "A trust-based security system for data collection in smart city," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4131–4140, Jun. 2021.

[44] S. Iqbal, R. M. Noor, and A. W. Malik, "A review of blockchain empowered vehicular network: Performance evaluation of trusted task offloading scheme," in *Proc. IEEE 11th IEEE Symp. Comput. Appl. Ind. Electron. (ISCAIE)*, Apr. 2021, pp. 367–371.

[45] D. E. Kouicem, Y. Imine, A. Bouabdallah, and H. Lakhlef, "A decentralized blockchain-based trust management protocol for the Internet of Things," *IEEE Trans. Dependable Secure Comput.*, early access, Jun. 18, 2020, doi: 10.1109/TDSC.2020.3003232.

[46] A. Fernandes, E. Kotsovinos, S. Östring, and B. Dragovic, "Pinocchio: Incentives for honest participation in distributed trust management," in *Proc. Int. Conf. Trust Manage.* Berlin, Germany: Springer, 2004, pp. 63–77.

[47] C. Dellarocas, "Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems," in *Proc. ICIS*, 2000, p. 52. [Online]. Available: https://aisel.aisnet.org/icis2000/52

[48] E. Koutrouli and A. Tsalgatidou, "Taxonomy of attacks and defense mechanisms in P2P reputation systems—Lessons for reputation system designers," *Comput. Sci. Rev.*, vol. 6, nos. 2–3, pp. 47–70, 2012.

[49] A. Ugur, "Manipulator: A novel collusion attack on trust management systems in social IoT," in *Proc. Comput. Sci. On-Line Conf.*, Cham, Switzerland: Springer, 2021, pp. 578–592.

[50] *PKI Page*. Accessed: Jan. 2012. [Online]. Available: http://www.pki-page.info/

[51] M. Kinateder and K. Rothermel, "Architecture and algorithms for a distributed reputation system," in *Proc. Int. Conf. Trust Manage.* Berlin, Germany: Springer, 2003, pp. 1–16.

[52] B. B. Sundaram, T. Kedir, M. K. Mishra, S. H. Yesuf, S. M. Tiwari, and P. Karthika, "Security analysis for Sybil attack in sensor network using compare and match-position verification method," in *Mobile Computing and Sustainable Informatics*. Singapore: Springer, 2022, pp. 55–64.

[53] A. S. S. Thuluva, M. S. Somanathan, R. Somula, S. Sennan, and D. Burgos, "Secure and efficient transmission of data based on Caesar cipher algorithm for sybil attack in IoT," *EURASIP J. Adv. Signal Process.*, vol. 2021, no. 1, pp. 1–23, Dec. 2021.

[54] R. Gupta and A. K. Somani, "Reputation management framework and its use as currency in large-scale peer-to-peer networks," in *Proc. 4th Int. Conf. Peer–Peer Comput.*, 2004, pp. 124–132.

[55] J. Sabater and C. Sierra, "Reputation and social network analysis in multiagent systems," in *Proc. 1st Int. Conf. Auton. Agents Multiagent Syst.*, vol. 1, 2002, pp. 475–482.

[56] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: Supporting reputation-based trust management for cloud services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 367–380, Feb. 2016.

[57] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation attacks detection for effective trust assessment among cloud services," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 469–476.

[58] K. Liu, Z. Zhou, Q. Chen, and X. Yang, "Towards an attribute-based authorization model with task-role-based access control for WfMS," in *Proc. IEEE 16th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2015, pp. 361–371.

[59] M. Blaze, J. Feigenbaum, and A. D. Keromytis, "KeyNote: Trust management for public-key infrastructures," in *Proc. Int. Workshop Secur. Protocols*. Berlin, Germany: Springer, 1998, pp. 59–63.

[60] M. Blaze, J. Feigenbaum, and M. Strauss, "Compliance checking in the policymaker trust management system," in *Proc. Int. Conf. Financial Cryptogr.*, 1998, pp. 254–274.

[61] Y. A. Younis, K. Kifayat, and M. Merabti, "An access control model for cloud computing," *J. Inf. Secur. Appl.*, vol. 19, no. 1, pp. 45–60, 2014.

[62] M. Alhamad, T. Dillon, and E. Chang, "SLA-based trust model for cloud computing," in *Proc. 13th Int. Conf. Network-Based Inf. Syst.*, Sep. 2010, pp. 321–324.

[63] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," *HotCloud*, vol. 9, no. 9, p. 3, 2009.

[64] J. Yao, S. Chen, C. Wang, D. Levy, and J. Zic, "Accountability as a service for the cloud," in *Proc. IEEE Int. Conf. Services Comput.*, Jul. 2010, pp. 81–88.

[65] S. D. C. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Psaila, and P. Samarati, "Integrating trust management and access control in data-intensive web applications," *ACM Trans. Web*, vol. 6, no. 2, pp. 1–43, May 2012.

[66] H. Skogsrud, H. R. Motahari-Nezhad, B. Benatallah, and F. Casati, "Modeling trust negotiation for web services," *Computer*, vol. 42, no. 2, pp. 54–61, Feb. 2009.

[67] H. Skogsrud, B. Benatallah, F. Casati, and F. Toumani, "Managing impacts of security protocol changes in service-oriented applications," in *Proc. 29th Int. Conf. Softw. Eng. (ICSE)*, May 2007, pp. 468–477.

[68] S. Song, K. Hwang, and Y.-K. Kwok, "Trusted grid computing with security binding and trust integration," *J. Grid Comput.*, vol. 3, nos. 1–2, pp. 53–73, Jun. 2005.

[69] S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok, "Trusted P2P transactions with fuzzy reputation aggregation," *IEEE Internet Comput.*, vol. 9, no. 6, pp. 24–34, Nov. 2005.

[70] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt, "Certified reputation: How an agent can trust a stranger," in *Proc. 5th Int. Joint Conf. Auton. Agents Multiagent Syst.*, 2006, pp. 1217–1224.

[71] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, Mar. 2007.

[72] J. Al-Sharawneh and M. A. Williams, "Credibility-based social network recommendation: Follow the leader," in *Proc. 21st Australas. Conf. Inf. Syst. (ACIS)*, 2010, pp. 1–11.

[73] Z. Malik and A. Bouguettaya, "Rater credibility assessment in web services interactions," *World Wide Web*, vol. 12, no. 1, pp. 3–25, Mar. 2009.

[74] M. Srivatsa, L. Xiong, and L. Liu, "TrustGuard: Countering vulnerabilities in reputation management for decentralized overlay networks," in *Proc. 14th Int. Conf. World Wide Web*, 2005, pp. 422–431.

[75] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, "Compliant cloud computing (C3): Architecture and language support for user-driven compliance management in clouds," in *Proc. IEEE 3rd Int. Conf. Cloud Comput.*, Jul. 2010, pp. 244–251.

[76] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "TrustCloud: A framework for accountability and trust in cloud computing," in *Proc. IEEE World Congr. Services*, Jul. 2011, pp. 584–588.

[77] F. J. Krautheim, D. S. Phatak, and A. T. Sherman, "Introducing the trusted virtual environment module: A new mechanism for rooting trust in cloud computing," in *Proc. Int. Conf. Trust Trustworthy Comput.* Berlin, Germany: Springer, 2010, pp. 211–227.

[78] S. Park, L. Liu, C. Pu, M. Srivatsa, and J. Zhang, "Resilient trust management for web service integration," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jul. 2005, p. 506.

[79] F. Skopik, D. Schall, and S. Dustdar, "Start trusting strangers? Bootstrapping and prediction of trust," in *Proc. Int. Conf. Web Inf. Syst. Eng.* Berlin, Germany: Springer, 2009, pp. 275–289.

[80] P. Domingues, B. Sousa, and L. Moura Silva, "Sabotage-tolerance and trust management in desktop grid computing," *Future Gener. Comput. Syst.*, vol. 23, no. 7, pp. 904–912, Aug. 2007.

[81] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Nov. 2011, pp. 933–939.

[82] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K. Nahrstedt, "A trust management framework for service-oriented environments," in *Proc. 18th Int. Conf. World Wide Web (WWW)*, 2009, pp. 891–900.

[83] C. Lin, V. Varadharajan, Y. Wang, and V. Pruthi, "Enhancing grid security with trust management," in *Proc. IEEE Int. Conf. Services Comput. (SCC)*, Sep. 2004, pp. 303–310.

[84] R. Aringhieri, E. Damiani, S. De Capitani Di Vimercati, S. Paraboschi, and P. Samarati, "Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems," *J. Amer. Soc. Inf. Sci. Technol.*, vol. 57, no. 4, pp. 528–537, 2006.

[85] R. Aringhieri, E. Damiani, S. D. C. di Vimercati, and P. Samarati, "Assessing efficiency of trust management in peer-to-peer systems," in *Proc. 14th IEEE Int. Workshops Enabling Technol., Infrastruct. Collaborative Enterprise (WETICE)*, Jun. 2005, pp. 368–373.
[86] F. Skopik, D. Schall, and S. Dustdar, "Trustworthy interaction balancing in mixed service-oriented systems," in *Proc. ACM Symp. Appl. Comput. (SAC)*, 2010, pp. 799–806.
[87] A. Khaksari and M. Keyvanpour, "TP-TA: A comparative analytical framework for trust prediction models in online social networks based on trust aspects," *Artif. Intell. Rev.*, vol. 52, no. 3, pp. 1929–1960, Oct. 2019.
[88] Y. Ruan, A. Durresi, and L. Alfantoukh, "Trust management framework for Internet of Things," in *Proc. IEEE 30th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2016, pp. 1013–1019.
[89] J. Wang, S. Jiang, and A. Fapojuwo, "A protocol layer trust-based intrusion detection scheme for wireless sensor networks," *Sensors*, vol. 17, no. 6, p. 1227, May 2017.
[90] P. D. Manuel, S. T. Selvi, and M. I. Abd-El Barr, "Trust management system for grid and cloud resources," in *Proc. 1st Int. Conf. Adv. Comput.*, Dec. 2009, pp. 176–181.
[91] K. Hwang, S. Kulkareni, and Y. Hu, "Cloud security with virtualized defense and reputation-based trust mangement," in *Proc. 8th IEEE Int. Conf. Dependable, Autonomic Secure Comput.*, Dec. 2009, pp. 717–722.
[92] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep. 2010.
[93] W. Luo and W. Ma, "Secure and efficient data sharing scheme based on certificateless hybrid signcryption for cloud storage," *Electronics*, vol. 8, no. 5, p. 590, May 2019.
[94] X. Chen, J. Ding, and Z. Lu, "A decentralized trust management system for intelligent transportation environments," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 13, 2020, doi: 10.1109/TITS.2020.3013279.
[95] C. A. Kerrache, C. T. Calafate, J. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.
[96] S. T. Alshammari and K. Alsubhi, "Building a reputation attack detector for effective trust evaluation in a cloud services environment," *Appl. Sci.*, vol. 11, no. 18, p. 8496, Sep. 2021.

SALAH T. ALSHAMMARI received the B.Sc. degree in computer science from Al Jouf University, Al Jouf, Saudi Arabia, in 2010, and the M.Sc. degree in computer science from Al-Imam Mohammad Ibn Saud Islamic University, Alriyadh, Saudi Arabia, in 2016. He is currently pursuing the Ph.D. degree with the Department of Computer Science, College of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. His main research interests include information security, cybersecurity, data security in cloud computing, data analytics, trust in cloud computing, and software testing.

KHALID ALSUBHI (Senior Member, IEEE) received the B.Sc. degree in computer science from King Abdulaziz University (KAU), in 2003, and the M.Math. and Ph.D. degrees in computer science from the University of Waterloo, Waterloo, Canada, in 2009 and 2016, respectively. He is currently an Associate Professor of computer science with KAU. His research interests include security and management of networks, systems, and services in wired and wireless networks. In the application areas, he is currently interested in software-defined networks, network function virtualization, cloud computing, future internet architecture, the Internet of Things, big data, and security and privacy issues in the healthcare sector. He is an ACM Member.

HANI MOAITEQ ABDULLAH ALJAHDALI was born in Jeddah, Saudi Arabia, in 1983. He received the B.Sc. degree in computer science from King Abdulaziz University, Jeddah, in 2005, and the M.Sc. degree in information technology and the Ph.D. degree in computer science from the University of Glasgow, in 2009 and 2015, respectively. From 2005 to 2007, he worked with Saudi Electricity Company, as a Budget and System Analyst. In 2011, he has appointed as a Lecturer with the Department of Information Systems, King Abdulaziz University. He is currently appointed as an Associate Professor with the Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh. His research interests include information security, human–computer interaction, and machine learning.

AHMED MOHAMMED ALGHAMDI (Member, IEEE) received the B.Sc. degree in computer science and the first M.Sc. degree in business administration from King Abdulaziz University, Jeddah, Saudi Arabia, in 2005 and 2010, respectively, the second master's degree in internet computing and network security from Loughborough University, U.K., in 2013, and the Ph.D. degree in computer science from King Abdulaziz University. He is currently an Assistant Professor with the Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia. He has also over 11 years of working experience before attending the academic carrier. His research interests include high-performance computing, big data, data analytics, BYOD, programming models, digital transformation, and software testing.