IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 10, 2018, accepted February 19, 2018, date of publication March 8, 2018, date of current version April 23, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2810337

Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues

FARHANA JABEEN[1], ZARA HAMID[1], ADNAN AKHUNZADA[1], WADOOD ABDUL[2], AND SANAA GHOUZALI[3]

[1]Department of Computer Science, COMSATS Institute of Information Technology, Islamabad 45550, Pakistan
[2]Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[3]Department of Information Technology, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding author: Farhana Jabeen (farhanakhan@comsats.edu.pk)

This work was supported by a grant from the Research Center of the Female Scientific and Medical Colleges, Deanship of Scientific Research, King Saud University.

ABSTRACT Trust is a salient feature in the context of health care, which is characterized by uncertainty and an element of risk. It is a fundamental requirement for the acceptance and adoption of new services related to health care. Soft trust, based on social control mechanisms, has yielded to evidence-based trust management, where the level of trust is explicitly computed by a trust engine termed the *trust and reputation system* (TRS). In e-health, soft trust can be used for access control, for assessing the quality of data represented in *electronic health records*, to address privacy and security requirements of healthcare systems, and to compute the credibility of an entity in the presence of unknown, possibly harmful entities. Despite the importance of soft trust in healthcare, related literature that explore soft trust issues, associated challenges and requirements are largely missing. To address this deficiency, the main contributions of this paper include: (i) taxonomy related to the soft trust in healthcare systems; (ii) reference model for measuring the performance and features of TRSs; and (iii) future areas of research related to the soft trust in healthcare.

INDEX TERMS E-health, trust, reputation, information systems, trust and reputation systems, healthcare domain.

I. INTRODUCTION

Trust is a salient feature in the context of healthcare, which is characterized by uncertainty and an element of risk [1]. Trust is considered important because it indirectly influences the quality of healthcare based on patient satisfaction, adherence and the continuity of its relationship with healthcare professionals and promotion of an accurate and timely diagnosis. The degree of trust represents the opinion of patients about healthcare professionals [7] and their willingness (based on their evaluation) to recommend a healthcare professional [8]. According to Browne *et al.* [2], to improve healthcare, one strategy is to measure the patient experience with the healthcare service provider. Existing studies indicate that trust is considered an indicator of quality of care and a patient's experience of health services and is correlated with patient satisfaction [3], [4]. Trust is considered important for compliance to medical advice in chronically ill patients [5], [6].

The ubiquity of Web2.0 with the proliferation of blogs and social networks allows a growing number of people to share healthcare experiences online or rate their healthcare providers [9]. Existing literature provides an ample amount of evidence that the patient role has changed from a passive receiver to an active user of online health-related information. According to a survey conducted by Pew Internet & American Life Project in 2009 [10], 44% of users browse the Internet to search for information about health professionals, and 36% to search for healthcare organizations. Another study conducted in the United States has shown that 88% of adults have searched the Internet for information concerning health issues [11]. There are doctor rating/review sites that are consulted by patients before selecting a doctor [12]. The top physician rating websites include RateMDs, HealthGrades, ZocDoc, and Vitals [11], [12]. These physician rating sites collect information about patient experiences and satisfaction with individual *Health Care Providers* (HCPs);

and presents HCPs ratings computed based on collected information [13]. Moreover, they also provide other related information about a physician, such as his or her address and certifications. Similar to other service-oriented businesses, these doctor rating websites allow service consumers to evaluate their experience and satisfaction with healthcare professionals or organizations. Online service consumer ratings and reviews are becoming increasingly important and have a significant impact on service provider selection intentions. Bacon [16] believes that physician rating websites provide essential feedback for doctors, requiring healthcare providers to track and control their online reputations [14], [15]. This in turn emphasizes the need for healthcare organizations to develop health systems to actively market themselves to acquire and retain customers. Tara Lagu [17] suggested that instead of promoting commercial websites to publish online information (ratings and reviews) about doctors and hospitals, hospital health systems should collect information about the quality of service received via patient surveys. Healthcare laws in most countries (such as the UK, Germany) necessitate the collection of ratings and reviews based on patient experience, which can later be posted on doctors' profile pages. In 2007, the UK government indicated its support for healthcare provider ratings by allowing the National Health Service (NHS) to launch the NHS Choices website, allowing patients to evaluate both HCPs and Health care Organizations (HCOs) [18].

TRSs have been developed for diverse environments, including distributed (online services [41] to networks: *Peer-to-Peer* (P2P) networks [49], mobile ad hoc networks [50], *Wireless Sensor Network* (WSN) [51]) and fully centralized environments. In a distributed TRS, the environment is distributed (e.g., in P2P and WSN) in such a way that each entity stores the reputations locally and provides them on demand to other members of the system. In hybrid reputation systems, the users request brokers who are responsible for trading reputation information upon request. The nature of the Internet and that of the healthcare domain lead to new vulnerabilities because the service consumers may provide unreliable or malicious reports, thus unfairly reducing the reputation rating of the service providers [54]. The success of TRS depends on the robustness of the mechanism to accurately evaluate the trustworthiness of an entity in the presence of possible harmful entities [52], [54].

Surveys related to TRSs in domains other than health [49]–[51] have been reported, but no study has specifically explored the use of soft systems in healthcare and its associated challenges and requirements. In this state of affairs, if the stakeholder (e.g., medical practitioners, medical organizations, researchers, policy makers) or TRS solution designer for healthcare were to attempt to seek guidance in the literature then absence of surveys would act as a major drawback in making the right decision. This paper aims to address this deficiency in existing literature. The contributions of this paper are as follows:

I. We have identified the different dimensions and characteristics of trust in the healthcare domain. We have also discussed possible attacks on the TRS.
II. We have identified key requirements for developing TRSs in the healthcare domain and discussed how existing work in this domain and closely related areas have addressed these requirements over the years.
III. A reference model for measuring the performance and features of TRSs is proposed.
IV. Moreover, we have highlighted several future areas of research for TRSs that are currently under-represented in existing literature.

The remainder of the paper is organized as follows: Section 2 discusses the role of trust in the evolving healthcare environment and identifies possible characteristics of trust, Section 3 reviews the existing work on TRSs and identifies the possible attacks on TRSs in the healthcare domain, Section 4 provides the reference model for measuring the performance and security features of TRSs in the healthcare domain and reviews the work related to addressing such requirements, and Section 6 highlights current research trends and areas for future research.

II. TRUST IN HEALTHCARE SYSTEMS

The continuous development of the Internet and the construction of new computing infrastructures are improving opportunities for the provision of e-health [19]. E-health is the use of information and communication technologies to acquire, store, share or transfer healthcare-related information. Moreover, it supports providing healthcare services to users. The main application areas of e-Health include the following: Electronic Health Records (EHRs) [20], [21], ubiquitous & pervasive health [22], telemedicine & telecare services [23], and decision support systems [24]. With the advancement in technology, EHR systems, with the goals of improving patient care and outcomes, enable *HCPs* to monitor health status online and store information derived from medical examination in EHRs, which may include personal information, laboratory results, medical treatments, diagnoses, medications, immunization status, and even some sound and image data. EHR aggregates patient medical information originating from multiple independent HCPs located in the same city, country or across the country border.

In e-health, trust can be broken into two main types: (i) hard and (ii) soft. Soft trust relationships are based on non-cryptographic mechanisms, whereas hard trust relationships are based on cryptographic mechanisms. Soft trust is context-dependent and is derived using individual or social control mechanisms [40]; for example, it can be based on direct experience (direct trust), trustworthy peer experience collected during the period (indirect trust), a combination of both, or third-party certificates, or it may be a subjective degree of belief about others. In the case of soft trust, the level of trust is explicitly computed by a trust engine termed a *Trust and Reputation System* (TRS). The degree of trust changes over time based on the trustee behaviour. The TRS gathers

information from service consumers about the quality of the service received and computes reputations (trust degree) for the service providers [40]. Reputations hold service providers accountable for their actions (based on past interactions) and reveal their behaviour in future interactions [14]. These systems help service consumers to make better decisions related to services/service providers, helping them avoid damage caused by poor quality or even deceptive services [41]. Soft trust based on social control mechanisms has yielded to evidence-based trust management [42].

Hard trust focuses on technical solutions to provide secure interactions between service providers and service consumers [21], [43], [44]. The hard security mechanisms protect users from vulnerabilities and attacks, among others, by only allowing access by authorized users. However, in the healthcare domain, the authorized HCP might sometimes act maliciously by providing false or in accurate information. For example, consider the following scenario. The healthcare provider may act maliciously by specifying that they specialize in the cure of a certain disease, but in reality they do not. Moreover, hard trust mechanisms do not monitor the behaviour of the participating entities (nodes, peers, systems) continuously. The participating entities may pass the hard trust mechanisms and subsequently report inaccurate measurements due to malicious intentions or faulty components.

For trust evaluation, soft trust mechanisms can be used in situations where partial or no hard trust mechanisms exist or vice versa [44]–[48]. In a ubiquitous healthcare system, only partial information may be available, and requests may come from unknown service requesters. Soft trust supports dynamic (on the run time) decision-making in providing services to requestors who are either strangers to the system or do not have access rights to certain services [47], [48]. For example, the resource can be granted if the degree of trust exceeds the threshold. Entities with a poor reputation can slowly (interaction after interaction) be granted more resources after their trustworthiness has increased.

Like trust, privacy also changes dynamically over time. Trust and privacy affect each other, such that a higher value of trust implies less need for privacy. The scope of privacy may vary depending on the e-health application, individuals, society and times [35]. Thus privacy is context dependent concept. The level of trust impacts the amount of information patients are willing to disclose and with whom the information is shared. The revolution of distributed and mobile computing has resulted in overwhelming concerns regarding privacy and security models [21], [36], [37]. Wireless transmission of sensitive patient data present several privacy and security implications [38]. With mobile device location privacy issues arise [37]. In ubiquitous healthcare applications for privacy protection, it is required to consider who controls what information is gathered, where it is stored, who has access to it, how to reduce its dissemination, and how to build trustworthy interoperability between service providers. In healthcare systems, the mechanisms that enforce the efficacy and efficiency of the privacy scheme include the following: (i) social mechanisms such as morals, ethics, and trust; (ii) law enforcement; (iii) technical solutions to provide secure interactions; (iv) regulations for the ruling participating entities; and (iv) a privacy-awareness framework supporting diverse privacy-related requirements of stakeholders. Many stakeholders are involved in e-health applications, among which each has diverse privacy requirements [21]. The trust of the trustor will increase if there is an agile solution that allows diverse and dynamic settings to support stakeholders with varying needs. Security and privacy frameworks should consider soft trust and its attributes [45], [71]–[73], [77].

A. CHARACTERISTICS OF TRUST IN THE HEALTHCARE DOMAIN

The following section describes some characteristics of trust in the health domain and possible attacks on TRS systems.

- **Asymmetry:** If an entity e_1 trusts another entity e_2, this does not mean e_2 will trust e_1. Trust may or may not be unidirectional and asymmetric; that is, if patient p_i trusts health-care professional hp_j, this does not necessarily imply that hp_j trusts p_i. Trust is mutually independent between the two sides. For example, if a patient has a poor experience with a medical practitioner during his/her first interaction, he/she will not take the advised medicines and will not come back for medical tests and treatment continuation. Similarly, the HCP may distrust a patient's historical medical data while making a medical decision. The reason is they are legally accountable for the medical decisions taken by them. Moreover, in ubiquitous healthcare domain relationship between health information systems and their users is asymmetric [53]. Moreover, health information systems based on the P2P infrastructure are symmetric in nature [31].
- **Subjectivity:** Trust is subject to the expectations one person has of another. The opinion that patient p_i holds about health-care professional hp_j depends on two factors: (i) the interpersonal skill of the hp_j, (ii) technical competence, (iii) a commitment to act in his/her interest, and (iv) the amount of extra demand by patient p_i. Let us consider an example scenario. Suppose that a community's common opinion about hp_j is that he/she is a good health-care professional and should be trusted. However, it may still be possible that person p_i may distrust hp_j simply because of the former's more demanding nature. Therefore, p_i trust is subjective to the expectations of p_i from hp_j.
- **Partial Transitivity:** Trust may or may not be transitive. It is possible that unknown entities may be known through a trust path. If patient p_i trusts health-care professional hp_1 and hp_1 trusts health-care professional hp_2, then it is not necessary that p_i would trust hp_2 (and vice versa). In contrast, trust may be derived from parallel transitive chains. For example, assume that a patient needs treatment for her

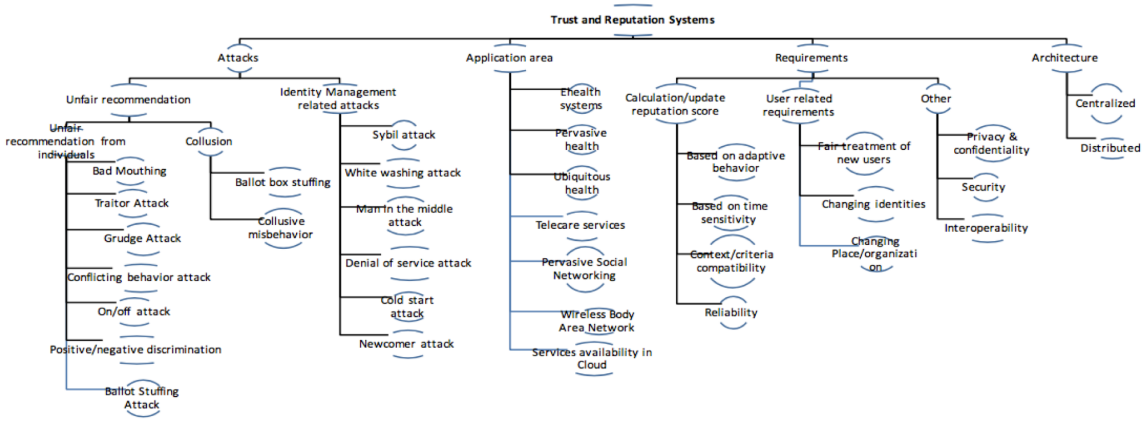

FIGURE 1. Taxonomy of trust and reputation systems in healthcare.

kidney and asks her general practitioner to recommend a good nephrologist hp_j. After obtaining a recommendation for nephrologist hp_1 from her general practitioner, the patient then asks for a second opinion from her friend about hp_j. Upon fusing the feedback from friend and general practionner, the patient will make his/her trust decision.

- **Context Sensitivity:** In e-health, trust establishment must be context-sensitive. Consider an example scenario in which patient p_i establishes a trust opinion about hp_j. The opinion depends on the context in which p_i has formed that opinion about hp_j. For example, patient p_i might trust HCP hp_j for dental surgery. However, p_i may not trust hp_j for gynaecology and ontology diagnosis and treatment.
- **Dynamic:** The trust relationship changes with time. For example, the trust relationship between an HCP and a patient may change in time and space.
- **Reflexive:** Every entity trusts itself, and therefore trust is reflexive. For example, a patient or HCP always has self-trust.

III. TRSs IN THE HEALTHCARE DOMAIN

A. POSSIBLE ATTACKS ON THE TRS

Following are some possible attacks on the TRSs [54].

- **Bad-mouthing Attack:** This attack occurs when a dishonest entity tries to hurt the reputation of one or more entities by assigning unfairly low ratings to them.
- **Collusion Attack:** In this attack, a group of entities work collectively to either boost each other's reputation or conspire against one or more entities in the network.
- **Ballot stuffing Attack**: To falsely raise reputations service providers engage in many fake dealings.
- **Ballot-box Stuffing:** Groups of entities attack competitors by giving out unfair ratings and recommendations.
- **Whitewashing Attack:** Sometime when an entity gets a bad reputation, he/she may leave the system and try to re-register under a completely different identity.
- **Positive and negative discrimination:** Discriminations can be made by service providers or service consumers. The participating entities can give good recommendations to specific entities and bad recommendations to other entities.
- **Denial of Service Attack:** This attack engages resources in meaningless activities and jams traffic to affect the availability of the reputation system.
- **Sybil Attack:** A malicious entity may acquire multiple identities to forge activities to deliberately hurt the reputation of another user or to gain high reputation values with positive feedback.
- **Man in middle Attack:** An authorized service consumer may deploy such an attack to manipulate the ratings given by a loyal service consumer.
- **Traitor Attack:** Dishonest entities establish trust by fair interactions initially and later misuse this trust by behaving maliciously only for specific occasions.
- **Grudge Attack:** A user may take revenge by giving low ratings to another user who gave him/her a low rating.
- **Initialization and cold-start Attack:** Determining a default reputation score for new users is a challenge in reputation systems.
- **Newcomer Attack:** An entity with a bad history or bad reputation score leaves the system and joins again as a new entity.
- **On-off Attack**: Based on the importance of the situation, the malicious entities perform well or poorly.
- **Conflicting behaviour Attack**: Malicious entities behave differently with different nodes.

We devise taxonomy of trust and reputation systems as illustrated in figure 1.

B. TRSs FOR EHR

Deursen *et al.* [55] present a system, Hedaquin, which provides healthcare professionals with an indication of the quality of the health data in a patient's health record. Hedaquin is created upon a Beta reputation system [40], [42]. The main component of Hedaquin is the reputation engine, which calculates reputations by using local, global, rule and

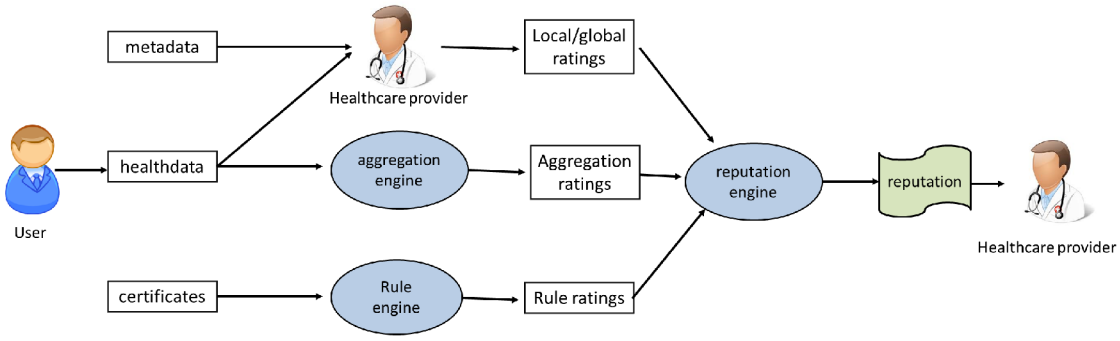

FIGURE 2. Hedaquin architecture [55].

aggregation ratings. A local rating is given to a specific service provider after checking the data quality, while the global rating represents the overall perception (what others think) of the service provider. Moreover, rule rating is collected from a rule engine that assigns a rating to a service provider on the basis of his/her degree, certificates and practices. Aggregation rating is collected from an aggregation engine that performs a comparison of measurements from two data health suppliers for the same person. If the measurements are the same, then suppliers reputation is enhanced; otherwise worsened. The Hedaquin architecture is illustrated in figure 2. To compute a reputation, the system supports the use of some additional information that includes a certainty factor, similarity in scope, order of the ratings and time. It fulfils the system requirement of the fair treatment of new users because of its component known as a rule engine.

Alhaqabani *et al.* [20] propose a model to measure the trustworthiness of medical data in EHR. The proposed model calculates trustworthiness for the HCP who created the data and the HCP who diagnosed the patient and entered the data into the EHR. It follows a time-variant approach and uses Beta and Dirichlet reputation systems [42] to collect reputation scores for the sources of medical data and use them to compute the trustworthiness of medical data via subjective logic. It allows the service consumers to rate the service provider from predefined distinct k levels. There are three main components: Health Authority (HA), Reputation Centre (RC) and Medical Data Reliability Assessment (MDRA) Service. Figure 3 shows the network structure consisting of these components. The Reputation Centre (RC) acts as a Dirichlet reputation system to calculate the reputation score for service providers based on ratings from service consumers. The reputation score represents the subjective opinion of the RC which is shared with healthcare providers on request. The health authority is a legal authority that collects medical data from health service consumers and computes reputations such as RC.

HA gives a rating to each reported case (related to medical misconduct, non-safety, or malpractice cases) according to the severity received from health service consumers and providers. The MDRA service is responsible for assessing

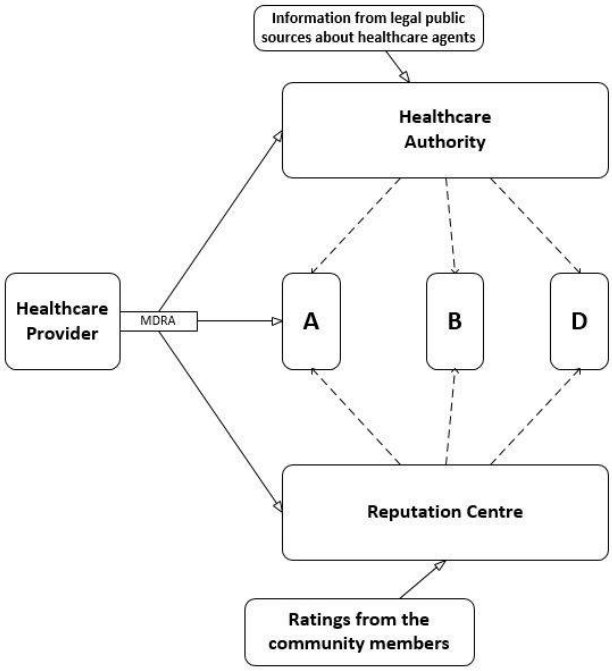

FIGURE 3. Medical data reliability network structure [20].

and communicating the reliability of medical data collected from different HCPs to the EHR system to record its experiences. These recorded experiences are then used by the Medical Data Trustworthiness Assessment (MDTA) service, which computes opinion regarding each service provider using a Beta reputation system.

C. TRSs IN UBIQUITOUS & PERVASIVE HEALTH

The paradigm shifts in healthcare have resulted in changes in security and privacy requirements. Ruotsalainen *et al.* [36] and [53] present Trusted eHealth and eWelfare Space (THEWS) principles to address the challenges associated with personal health records (PHRs) and personal health system s (PHSs) in ubiquitous healthcare. The THEWS principles focus on the rights to be given to the data subject

TABLE 1. Comparison of state-of-the art in the healthcare domain based on different attacks.

	Bad mouthing	Ballot stuffing	Traitor attack	Grudge attack	Sybil attack	Time sensitivity attack	Initialization /cold start problem	Conflicting Behavior Attack	White wash attack
Hedaquin [55]	*	*	—	—	—	*	**	—	—
Alhaqabani et al. [20]	—	—	—	*	—	*	**	—	—
		Partially addressed*	Fully addressed **	Not Specified —					

to control the access and use of personal information. The data subject is given the right to control collection, usage, assessment, and sharing of his/her information by setting own context-aware personal privacy and trust policies.

Moreover, it emphasizes the involved systems to ensure trust verification, data processing transparency and openness of their interests. THEWS principles present a new prospect for management privacy in open dynamic systems. An individual is allowed to confirm network and systems trustworthiness that require or process the personal information of the individual for secondary purposes. Personal privacy policies can be set by individuals. An individual can also set context-aware personal privacy and trust policies to allow secondary use of healthcare information.

Ruotsalainen *et al.* [36] present a privacy-enabled architecture for ubiquitous health based on THEWS principles. Instead of using the traditional security services, the presented architecture makes use of existing work related to soft trust for trust verification, policy management services and context-awareness in the construction of privacy policies. The trust information is computed based on the trust value and the trust feature vector. The trust value is computed based on attributes such as (i) legal requirements and contextual features, (ii) architectural and technological aspects, (iii) the privacy policy, (iv) predictability, (v) transparency and (vi) ability.

The trust feature vector contains the following attributes: (i) degree of international privacy directive compliance, (ii) degree of health-care-specific laws and rule compliance, (iii) degree of its own privacy policy openness compliance, (iv) degree of relationship openness compliance, (v) degree of following its own privacy policy compliance, (vi) system certification compliance, (viii) position on the blacklist, (ix) compliance with respect to the acceptance of external monitoring of events accessing personal health information, and (x) supporting access to audit trials. Table 1 highlights a comparison of existing TRSs in the healthcare domain by addressing the identified attacks in Section 4.

IV. REQUIREMENTS FOR THE TRSs IN THE HEALTHCARE DOMAIN

Designing efficient TRSs in the healthcare domain clearly raises research issues at several levels. The requirements and challenges identified in this section will serve as a reference model for measuring the performance and features of existing TRSs.

A. ADAPTIVE BEHAVIOUR

TRSs rely on feedback provided by others, thus avoiding or reducing the influence of unfair ratings in reputation systems, which constitutes a fundamental problem. Unfair behaviour may be explained by a variety of reasons, including personality/habit, business gains, irresponsibleness, victim exploitation and randomness. The reputation system can only be safeguarded against malicious attempts if there are regulations with credible sanctioning options, or technical mechanisms that can detect and discard malicious activities. Jøsang *et al.* [54] identify some fundamental requirements for robustness that should, in general, be satisfied. They provide a detailed discussion on different attack types that can affect TRSs, including a playbook, unfair ratings, discrimination, collusion, re-entry and sybil attacks. For TRSs, a dishonest service consumer is sometimes difficult to detect because his behaviour changes over time. A malicious service consumer can establish a good reputation by fair interactions initially, only to deploy an attack once the trust is gained. In another case, dishonest service consumer recommendations may be quite random and therefore very difficult to detect, for example, providing negative ratings to all interactions with a healthcare professional of a particular healthcare organization. Therefore, the reputation model should be able to reflect service consumer behavioural patterns by incorporating past behaviour to calculate his/her trustworthiness. This goal can be easily accomplished in centralized TRSs, but in distributed systems, especially in open and dynamic systems (ubiquitous health), there is limited availability of the past behaviour of an entity that has disconnected from its home network and entered a holistic or unfamiliar environment.

Studies that support avoiding or reducing the influence of unfair ratings use external factors in trust evaluations, such as entity creditability and its reputation to determine the trustworthiness of the provided recommendations. Xiong and Liu [56] present an approach that requires the reporting entities to compute the degree of satisfaction based on the quality of the service experienced. The work also provides a mechanism to compute the feedback similarity rate between the requesting entity and the feedback reporting by the witnessed entities over the set of common entities with whom they have directly interacted. Hedaquin [55] gives more weight to the ratings received from users with high trustworthiness as a recommender. How the recommender credibility is calculated is not explained in detail [55]. To ensure that only those service consumers to provide ratings

were those who used the service, Josang *et al.* present a mechanism to confirm proof of the interaction [40]. The proof of interaction (i.e., ticket) allows the determination of whether two parties were actually involved in a transaction for which a rating is provided. Weitzel *et al.* [57] present a mechanism to measure the credibility of network sources based on the number of social interactions (retweet ties) between the two entities, which was constructed according to healthcare information. Gómez and Martínez [58] propose a trust and reputation model that allows a node in WSN to identify the trustworthy node that provides a specific service and then to reach it via the most reputable path. In [59], Boukerche and Ren present a multicast strategy that makes use of the computed trustworthiness score of a node to determine its behaviour and generate corresponding actions. The proposed scheme rewards a node for every successful forwarding event and penalizes a dishonest node for malicious dropping. For multicasting, the trustworthiness value of a node becomes a selective criterion for choosing qualified nodes. Work has been conducted in the distributed domain that handles the adaptive behaviour problem using different strategies. Hoffman *et al.* have surveyed the existing literature related to attacks on TRSs [60].

B. FAIR TREATMENT OF NEW USERS

Determining initial reputation score for new entities is a challenge in reputation systems. If the new entities are assigned a very low default reputation value, they may never be selected and may not get a chance to improve their reputation. For example, in the P2P environment, in which the group of peers works collaboratively in the medical consultation, or research, a peer might be reluctant to obtain services from the peer with a low reputation value. However, assigning a high default reputation score will provide an unfair advantage to new entities who are still unknown to the system.

Initially, when a new entity joins the system, the construction of a trust evaluation based on little or no information can be completed by gathering information from direct and indirect sources. The TRS should define a mechanism that can represent the uncertainty associated with a new entity without penalizing them or providing an unfair advantage. TRS must distinguish between entities with unknown quality and with poor long-term performance. For this purpose, service consumers should be encouraged to provide ratings. Otherwise, the TRSs will face the problem of free riders [61]. Consumers are more willing to provide feedback about a service provider if they are given an incentive.

An open environment with multiple entities that have varying interests and domain environments is, by definition, not trusted. In this environment, it cannot be assumed that there exists some predefined trust between the entity and systems. Moreover, the system features and regulations that are followed are often [53] unknown. In such an environment, with the passage of time, an entity becomes successful in enhancing its reputation score and creating a connection with trustworthy and reliable peers. However, in such systems, the entities are sometimes more conservative about offering or obtaining services from unknown entities. The entities are reluctant to risk initiating a connection or considering the recommendations provided by the entity with the lowest reputation score. However, it is possible that the newcomer provides reasonable and better services in comparison to other peers.

In a distributed environment in which an entity wants to interact with an unfamiliar entity, it can contact its closest trustworthy peers to obtain trust information. In this scenario, if no trustworthy peers have any information, then one solution is to verify the entity's public key using a challenge-response method. A trusted value should be assigned based on the internal information (for example, a trust value based on a trust policy, whether there is a protection method installed, risk analysis, among others). The implementation of such a mechanism would be difficult in an open environment. In the healthcare domain, this task can be accomplished by the NHA with whom each HCP is registered [18]. The NHA can be held responsible for assigning a base rate to a practitioner based on his/her education, experience, complaints and previous reputation history available with any other national or international trusted TRS. Le Hoang Son [62] has reviewed the available studies dealing with the new user cold-start problem in TRSs.

C. CONTEXT/CRITERIA COMPATIBILITY

Context/criteria knowledge is a critical requirement for TRSs, especially when calculating trust. Chen and Kotz [63] describe context as the set of environment friendly circumstances and settings that governs an entity behaviour or in which the event that occurred is of interest to the user. Some of the requirements that should be addressed by a context-aware TRS in the healthcare domain include (i) allowing the service consumer to select the information that characterizes the context, (ii) tagging the trust information according to the context, (iii) performing a context-aware reputation computation by categorizing the context and using a specific reputation computation technique based on the type of context, (iv) adapting the trustworthiness computation and assessment according to the context, (v) performing an implicit context reconfiguration, and (vi) performing autonomously.

In the healthcare domain, there is work that emphasizes the need for context-related information. Bricon-Souf *et al.* review work related to context-aware services in hospitals focused on improving the management of patient health record, communication and information sharing between professionals using context-aware equipment [67]. Sánchez *et al.* [65] present a mechanism for estimating hospital staff activities. The work maps contextual information with user activity (using a hidden Markov model). The contextual information taken into account includes the location, time, role, user identity and availability of information. Behrooz and Devlic [68] present a context-aware privacy policy language to enable mobile users to control access to their context information. The establishment of policies allows the

control of who can access, what kind of information, and in which situation. Seppälä *et al.* [69] consider a situation in which the individual, environment, information technology system, service, and stakeholder are privacy-related context information components in ubiquitous health. Furthermore, the properties of the identified components are defined to create context-aware privacy policies. Fenza *et al.* [70] present a generic context-based architecture supporting the selection of autonomous services by matchmaking the user context and available services in the health-care domain. In this work, context data are defined as comprising static (e.g., user profile, preferences, among others) and dynamic (e.g., blood pressure, temperature, among others) data.

The reputation context could enhance systems by providing improved granularity. It is possible for an entity to have different reputation in different contexts. Consider an example scenario, in which an HCP may provide high quality services on high-in-demand trivial aspects, and low-quality services on crucial aspects that are comparatively low in demand but associated with a large financial gain. For example, a pharmacist may provide a high-quality bandage at a low price to increase his reputation score, but a low quality of surgical instruments or diabetes testing equipment to satisfy his profit requirements. Moreover, the reputation values in various contexts can have an indirect influence on each other's formation, which in turn complicates the development of a global reputation value for an entity. Consider an example scenario, in which an HCP with high reputation values in a specific context (e.g., HCP) is considered a successful and highly reputed member of society even from the perspective of other contexts. The opposite situation, in which an HCP with a low reputation value in one context will not be highly respected in other contexts, is also true. The reputation of an entity in one context cannot always be transferred to every other context. For example, the reputation of a healthcare provider as a surgeon cannot be inferred from his/her reputation as a physician. However, in e-health, some mechanisms are required to determine the similarity between contexts to compute the aggregated value. Hedaquin [55] satisfies the context requirement to some extent by assigning more TRS weight to ratings that are similar in scope. For example, the scope function supplies zero weight if the scopes are dissimilar (e.g., the similarity between blood sugar and height measurements is zero). To assess the trustworthiness of medical data, Alhaqabani *et al.* [20] assess the trustworthiness of the HCP and consider the context in which the medical data were collected. The developed TRS should be able to differentiate between different contexts and calculate reputation scores that are relevant to each context rather than aggregate the ratings for different contexts.

D. PRIVACY AND CONFIDENTIALITY

TRSs should guarantee privacy both to the entity owing the reputation and the entities providing the recommendations. In the healthcare domain, one important requirement for TRS is rating secrecy, that is, the service consumer identity information is kept secret to avoid retaliation and privacy violation. The TRSs should ensure that participating entities do not retrieve identification information about each other. Designing a mechanism for TRSs that achieves both trust and anonymity is challenging. Revenge rating is an issue, especially in TRSs developed for the healthcare domain, where a service provider (e.g., doctor), by acting as a service consumer (e.g., patient), may take revenge by spoiling the reputation of another service provider. For example, a heart physician as a service consumer may give bad ratings to an oncologist as a service provider, who consequently may spoil the reputation of that specific heart physician as a service consumer.

Revenge rating and negative discrimination can be avoided if the TRS allows the service consumers to provide ratings anonymously, i.e., their actions must be disconnected from their real-world identity as well as their other actions that can lead to disclosure of their identity. Anonymous online reviews can be particularly harmful to a physician's reputation because of the Internet's global scope [40]. Hiding the identity of raters opens the TRS to bad-mouthing and negative discrimination attacks. To avoid such attacks, one solution can be to only allow service consumers to have an interaction with the service provider providing the rating. Alhaqbani *et al.* [20] present a pseudo-anonymity technique in which the patient is assigned a unique local ID at each HSP. The patient is held responsible for linking the medical records stored by different HSPs. To allow record aggregation from different HSPs, the patient must link himself to specific HSPs (using the pseudonym provided by the HSP) as long as the HSP is in trust agreement. Pseudonyms are used to preserve patient anonymity and are used as a reference when the HSP wants to exchange data about the patient.

The TRS should support transparency, and service consumers should be accountable for the recommendations (feedback) they provide about other service providers. Any malicious user trying to manipulate trust ratings should be identifiable. The system should know the identity of all service consumers and service providers and keep their identities concealed from each other. In addition, it should keep track of all dealings, ratings and estimated reputation of service consumers and service providers.

Anonymizing user identity alone does not solve the problem. Anonymous ratings provided by a service consumer using single pseudonym can be linked to each other. Data mining techniques along with some real-world information collected through another source of information (the service consumer behaviour at a public forum or the spatio-temporal information associated with each reading in a participatory sensing system) can be used to re-identify that individual. The servers responsible for the management of ratings can do this. In ubiquitous health and m-health applications, the sharing of sensed data tagged with spatio-temporal information could be a threat to user privacy. Consider an example scenario. If the location information is not kept private, it may leak the patient's state of health, for example, a patient visit to a

place where there is a psychiatric clinic or a clinic specialized in sexually transmitted diseases. Therefore, such systems require a mechanism that provides user location along with user identity privacy.

Christin *et al.* [72] present an anonymity scheme based on multiple pseudonyms for the participatory sensing system. To report a sensor reading, the user is required to select a new pseudonym for each time period. This scheme allows the linkage of interactions in a unique period while limiting linking across multiple periods.

Tormo *et al.* [71] present a privacy-enabled *Service-Oriented Architecture* (SOA) for health information integration and exchange. The presented architecture, addresses problems related to exchange information based on trustworthiness in healthcare organizations working in different domains. The model allows the healthcare providers to decide whether attribute providers (who maintain patient information) are sufficiently reliable to obtain user attributes. Moreover, the work presents a trust and reputation model that support the preservation of privacy. The model uses homomorphic encryption technique to aggregate feedbacks from service consumers about the specific provider in a privacy-preserving way. Wang *et al.* [73] presents a reputation framework for the evaluation of sensing reports and participant trustworthiness. The work also addresses the problem of anonymity. The participants are required to use their blinded identity, which acts like a pseudonym and can change randomly with each sensing report. Moreover, anonymous certificates are generated that include the reputations of participants.

E. CHANGING IDENTITY

A user who registers himself/herself with several forged identities at the TRS allows him/her to forge or control a large amount of entities and acts on behalf of them (Sybil attack). If a user has a bad reputation, it would be in his interest to change his identity so that he can start as a new user. If a service consumer is allowed to have multiple identities, it may disrupt the accuracy of the TRS computation by sending false data collusively or by sending multiple reputations for a single task. Having multiple identities also threatens the privacy of the user. A sybil attacker with external knowledge can exploit the received recommendations to infer the private interests of users [74].

To discourage sybil attack, one simple solution can be to ask for some information at the time of registration, such as the device International Mobile Equipment Identity (IMEI) number, and restrict each device to the maximum registration of one account. Other solutions include (i) penalizing the user by imposing a computational cost on identity creation and (ii) averaging all the recommendations received by identities with an IP address in the same zone. Due to the mobility feature in a mobile network, detection and handling of sybil defence is quite different compared with online networks. There is a need for sybil-resilient schemes that prevent adversaries from distorting reputation scores.

F. RELIABILITY

Reliability is concerned with the number and quality of information resources used to calculate reputation scores. Experience, knowledge, and credibility are important elements and must be considered while computing reputation. A greater number of reliable sources used to calculate the trustworthiness of an entity will allow computing the reputation reliably. Incomplete information leads to inaccurate information and, in turn, affects the computation of the reputations. TRSs should support transparency, allowing the entities to be well-aware of how the reputation is computed and verified. The main component of Hedaquin [55] is the reputation engine, which calculates reputation based on local, global, rule and aggregation ratings in the e-health domain. Rule ratings are collected from the rule engine that assign a rating to a service provider based on his/her degree, certificates and practices. Aggregation ratings are collected from an aggregation engine that compares measurements from two data health suppliers about the same person.

In many countries worldwide, the public has limited access to information related to the breach of ethical standards and professional negligence. In Australia, cases of medical negligence are reported to state government bodies such as the *Healthcare Complaints Commission* (HCCC) but not to the public. In the United States, such information about medical practitioners is kept in a national practitioner databank. Any current or prospective employer or registration board may apply for information about a medical practitioner. In the United States, some states have taken initiatives to publish complaint and litigation data about doctors on the web. Alhaqabani *et al.* [20] and Deursen *et al.* [55] assume that there is a health authority that records information about cases of medical negligence reported by different HCPs. For the specific HCP, a reputation score is computed based on the information received from the health authority and the reputation centre (i.e., recent reputation scores and reputation score history). In our opinion, while calculating the reputation of any service provider in the healthcare domain, the health authority should give importance to the severity of the mishandling done by the HCP and a penalty should be imposed accordingly.

Computing the reputation of a service provider based on the number of service consumers to whom they provided services does not provide reliable information. Moreover, to inquire about the trustworthiness score of a service provider, the service consumer must inquire about the reputation of the target entity in a particular context. Considering the recommendation score about the service provider from a highly trustworthy peer who had a direct interaction with the service provider in a context that differs from the target context is not reliable. In contrast, considering the reputation score for the target entity from a less trustworthy peer who had a direct interaction with the target entity in a particular context is comparatively more reliable and influential in making the right decision.

Furthermore, it is possible that the trustworthy peer has rated the target entity in the particular required context (as required by the requesting entity), but the criteria used for evaluation differ or the weight given to each criterion differs from that of the requesting entity criterion requirement. Weitzel *et al.* [57] present an approach to compute reputation based on social interactions that have been constructed according to health information. The authors provide a scheme to determine user reputation in a social network (i.e., twitter) based on retweet ties. To increase usability, the TRS should support the enquiring entity in the search for important aspects of reputation. The TRS should possess a mechanism to measure the reliability of the entity in providing services according to the expected level of trustworthiness.

An entity with a high reputation score as a service provider is not necessarily reliable in the role of recommendation agent. To satisfy reliability concerns, TRSs should be equipped with mechanisms to determine the credibility level of the received ratings. To assess the trustworthiness of medical data, Alhaqabani *et al.* [20] assess the trustworthiness of the HCPs and consider the context in which the medical data are collected. To evaluate the trustworthiness of historical data, Hedaquin [55] builds on the subjective logic and the Beta reputation system. The system allows weighting of ratings with respect to their scope of similarity. To address the reliability requirement, if sufficient ratings related to a certain scope are not available, the ratings for similar scopes are used.

G. DEFAULT REPUTATION SCORES FOR NEW USERS

Determining default reputation score for new users is a challenge in TRSs. TRSs must distinguish between the entity with unknown quality and with poor long-term performance. Hedaquin [55] assigns a default score of 0.5 in the absence of any evidence. This approach does not work well because the system assumes that service consumer rating behaviour is consistent. In contrast, Alhaqbani *et al.* [20] use the average reputation score of the community to which the entity belongs as the default score. This technique improves reliability since the average reputation score reflects the trustworthiness of the whole community at any one time. When a new entity joins the system, little or no information about such an entity can be gathered from direct or indirect sources for trust evaluation. In such situations, trust can be built based on third-party references provided by the entity itself.

Moreover, in such environments it cannot be assumed that there exists predefined trust between the entity and systems. In such situations, due to the lack of security and trust, the entities are sometimes more conservative about offering or taking services from unknown entities or those whom they do not like, leading to the formation of groups by known entities that share services and provide transitive trust among members. Such group coalitions may result in a ballot box stuffing attack, providing false recommendations for outsiders and positive (increased) recommendations for group members. TRSs should be equipped with a mechanism to address the adjustment of newcomers as well as ballot box stuffing problems.

H. TIME SENSITIVITY OF REPUTATION

The goal of a TRS is to predict the trustworthiness of entities in providing the quality of services in future interactions based on information collected from their past behaviour related to service provision. The reputation of an entity calculated by the TRS should be grounded in current reality and should be updateable. If the current behaviour of the concerned entity is not considered or more weight is given to the past behaviour of an entity, then the computed trustworthiness value would not be correct.

The trustworthiness of the recommending entities and their reputation score related to a specific entity should be time-dependent. The importance of the trustworthiness of old ratings of target entities and old trustworthiness on recommending entities (credibility of recommending entities) should decay with time. Older information should have a reduced influence on the calculation of a reputation value. Weights should be assigned to ratings (received from peers or assigned by a trustor based on direct interactions) based on their age. The TRS should support mechanisms to repair any incorrect data that is used to establish the reputation. For this purpose, it must account for the temporal behaviour of the entities.

In an open dynamic environment, the number of participating entities varies over time, new entities join, and the previous ones may leave, subsequently leading to different internal policies related to the provision or acquisition of service. Therefore, trust should be re-evaluated continuously (after a certain duration) and should be based on experiences related to recent interactions. If the TRS updates the reputation score after it had been fixed for a long period of time, then such time lags provide an opportunity to the service provider to supply a large number of low quality services over a short period of time to prevent significant degradation of the reputation score.

Creating old positive behaviour as equivalent to new negative behaviour may result in attacker abuse of the system. If a TRS gives equal weight to a complete rating history (i.e., all interactions experienced) while calculating the overall reputation, then malicious users can take advantage of such systems by performing short-duration malicious attacks because their lengthy previous history (with a high reputation score) can outweigh their current actions. Hedaquin [55] satisfies the time sensitivity requirement and allows the association of a time stamp with ratings to support giving more weight to recent ratings and to more recently created health data. Browne *et al.* [2] use a time-varying mathematical approach (based on Beta and Dirichlet probability density functions) for feedback aggregation and reputation rating expression. Josang and Haller [42] introduce a forgetting feature that allows the system to discard old ratings after a predefined period.

I. INTEROPERABILITY AND PORTABILITY

Currently, most of the developed TRSs are platform-specific [50], [51], [55]. Reputations calculated in relation to an entity are specific to that particular platform or community. Most platforms have their own TRSs that are not compatible with any other platform. The TRSs differ not only in the methods related to the reputation computation but also in the range of supported trust values. According to Emmert *et al.* [75], the questions asked of the service consumer at physician rating web sites to rate physicians differ widely from portal to portal, not only in quantitative but also in qualitative aspects.

Creating one's own standing in the community by gaining a good reputation is not trivial. It requires continuous effort over certain periods of time to demonstrate good behaviour, i.e., to participate in providing quality services and correctly measuring the trustworthiness of other entities. Starting as a new entity in the new system is not easy. Consider the following example scenario, in which medical physician P serves hospital H_1 for several years in a specific city and country. P was actively involved in providing trustworthy services and in providing trustworthy recommendations about the healthcare staff and services. Consequently, P has established a good reputation in the community. However, for some reason, P needs to change his work place and must move to some other new hospital H_2 in another city or country. In such a situation, P will be left with no choice but to build his/her reputation from scratch. This emphasizes the need for the TRS should to support portability and interoperability requirements, so that the activity history of P as well as his/her reputation can be easily transferred. Furthermore, the interoperability between TRSs developed for different domains (such as e-commerce and healthcare) would enable an overall perception about the activities of an online entity (including his/her interests and reputations in different domains).

J. SECURITY

To provide security, there is a need to establish and evaluate trust between devices (especially in the distributed domain) using both hard and soft trust mechanisms. TRSs should be equipped with a mechanism to address the denial-of-reputation situation, in which a malicious entity acquires the identity of a reputable entity with the aim of stealing or damaging the reputation to lock him/her out of the system. Moreover, TRSs should be able to address the threats related to the underlying infrastructure. Such attacks aim to steal the data, make information unavailable or damage the data integrity of the information while in storage or during transit. An efficient security mechanism for the TRSs should be context-aware, adaptive, and must satisfy the security requirements of the stakeholders, with each having different privacy requirements and decision-making powers. The main security problems include confidentiality, availability, and integrity.

Martínez-Pérez *et al.* [37] discuss the privacy and security challenges in mobile health applications and review the existing work to address such challenges. The authors investigate the approaches and measures taken by Europe and its member states to protect healthcare systems. In this respect, this work evaluates the policy context, security challenges, requirements, and the relevant practices implemented for e-health security. Furthermore, [38] reviews the sensor network architecture for pervasive healthcare and discusses the security techniques they employ. The security mechanisms for the TRSs in distributed computing domains can be developed based on such established techniques. In [44], Kumar and Lee review existing approaches to address security requirements in wireless healthcare scenarios. The work does not review the literature related to addressing the security threats confronted by TRSs in the healthcare domain.

In [48], Yuan *et al.* discuss the relationship of trust, reputation and security in ubiquitous healthcare. In [49], Selvaraj and Anand address security issues in TRSs for P2P networks. The work also surveys existing reputation management systems for P2P networks developed for different domains including healthcare.

EHRs contain personal data, and therefore they may be subject to security and privacy attacks. In the distributed EHR system, the participating entities may have different security needs. In [77], Bahtiyar and Ça?layan present a trust assessment model for obtaining e-health service. The presented model allows an entity to evaluate the trustworthiness of one or more properties of the underlying security system.

Table 2 illustrates addressing which TRS requirements can be helpful in mitigating different reputation attacks. Table 3 highlights the support for the requirements identified in Section IV by the current TRSs in the healthcare domain. We will rate these TRSs on 1 of 3 levels: Strong represents an evaluation criterion parameter that is strongly supported by the TRS, Medium represents partial support for the evaluation criterion parameter, and Weak denotes weak support for the criterion parameter. Table 4 summarizes the research focus of the work included in this paper.

V. DISCUSSION & FUTURE RESEARCH SCOPES

A. DISCUSSION

Although a cure-all solution is not yet available, there are studies examining a wide range of specific issues that are relevant to soft trust in healthcare [1], [20], [36], [39], [40], [53], [55]. Based on the study of all related work in the domain of trust in the healthcare domain, we discovered investigations focused on providing patient-centric care and improving the collaboration between multiple stakeholders for achieving reliability [20], [31], [55].

There are information systems that offer limited accessibility to resources [29], [30], and those that support collaboration among multiple stakeholders [31]. Moreover, there are studies in the healthcare domain that focus on establishing trust relationships via cryptographic techniques (i.e., Hard Trust) [21], [31], [43], [44] and that emphasize the benefits of trust, which can be established using non-cryptographic techniques [36], [44], [45]. Moreover, some studies have

TABLE 2. TRS requirements for mitigating different attacks.

Attacks	Calculation/update of reputation				User related requirements		Other		
	Adaptive behaviour	Time sensitivity	Context/criteria compatibility	Reliability	Fair treatment of new users	Changing identities	Privacy & confidentiality	Security	Interoperability
Bad mouthing attack	x	x		x		x			
Grudge attack	x	x		x			x		
Traitor attack	x	x		x			x		
Conflicting behaviour	x	x		x					
On/off attack	x	x	x	x					
Pos / neg discrimination			x	x					
Ballot box stuffing	x	x		x					
Collusive misbehaviour	x	x		x					
Sybil attack						x		x	x
Whitewashing attack						x		x	x
Man in the middle attack								x	
Denial of service attack								x	
Cold start attack					x				x
Newcomer attack					x				x

TABLE 3. Comparison of state-of-the-art TRSs in the healthcare domain based on different TRS requirements.

	Adaptive	Reliability	Fair treatment of new user	Context/criteria compatible	Time sensitivity	Robustness	Privacy	Security	Interoperability and Portability	Changing Identity
Hedaquin [55]	**	***	*	***	***	*	—	—	—	—
Alhaqabani et al. [20]	—	***	***	*	***	*	***	—	—	—
		Weak *	Low **	Medium ***	Not Specified —					

emphasized the ability of the framework supporting the hybrid trust model (using both soft and hard trust) to improve the security of the distributed systems [46], [82]. However, the incorporation of soft trust or hybrid trust in systems developed for the healthcare domain has not been widely addressed by the research community and requires attention. Some investigations address the requirement for the computation of HCP reputations, but either their solution is not complete or is, in some cases, too basic [11]–[18], [76]. To date, direct evidence at physician rating sites regarding the following is lacking: (i) techniques and trust models that have been incorporated to compute the reputation of HCPs, (ii) discussion regarding the requirements of the TRS that were and were not met in the healthcare domain, (iii) the robustness against attacks expected on the TRSs in healthcare, and (iv) the incorporated privacy and security techniques and trust model [11]–[18]. Moreover, TRSs in the healthcare domain have been developed that emphasize the quality of the data in patient health records [2], [55]. One limitation of these TRSs is that they have not been tested in real-world scenarios within a specific legal framework.

None of the work related to TRSs in the healthcare domain presents a complete solution to address most of the requirements identified in Section 4, although some have, to some extent, addressed identified requirements as shown in Table 1 and Table 2. Moreover, there are studies that either stress the need for a TRS in the healthcare domain or in e-Health application areas [36], [40], [45], [47], [48], but they do not suggest any practical solutions to the associated requirements.

There is a dearth of empirical research in medical care settings. A published assessment of the P2P domain related to TRSs focuses mostly on file sharing [49], and thus, the TRS focusing on collaborative diagnosis/treatment in the P2P domain can be developed based on such established techniques. The current situation stresses the need for the attention of the research community on the development of TRS solutions for e-health applications considering the identified requirements.

B. FUTURE DIRECTIONS

For the healthcare to be the trusted industry, there is a need to understand the stakeholder expectations from it. In addition, there is also need to understand which of such expectations is addressed in a good manner and which expectations needs to be addressed. Most of the current trust models in the health sector encode trust as a numerical value (termed as ratings) which might not be valuable for service consumers. In real

TABLE 4. Overview of different TRS schemes in healthcare.

Research	Research Focus	Application Area	Computing Environment
[1]	Provides a systematic review of the literature related to measuring trust in health system	Health, Healthcare	Centralized/Distributed
[20][55]	Proposes a TRS to measure the trustworthiness of medical data as entered into the patient's EHR	Healthcare	Distributed
[3] -[8]	Emphasises on the importance of trust as an indicator of quality of care and patient's experience of health services	Health, Healthcare	Centralized/Distributed
[9]-[18][76][61][75]	Focuses on (i) impact of physician rating sites in health systems and (ii) their fundamental characteristics	Healthcare	Centralized/Distributed
[19][22][23] - [31]	Discusses challenges facing E-Health in different application areas such as WSN and P2P.	E-Health, Healthcare	Centralized/Distributed
[21]	Provides a survey of work using hard trust techniques to provide privacy and security	EHR systems	Centralized/Distributed
[32]	Emphasizes on the importance of trust between patients and physicians in the E-health era	E-health	--
[33]	Discusses EHR systems, their data standards, interoperability standards, data models, and associated challenges	E-health	Distributed
[34]	Focuses on how to measure interpersonal strength	General	--
[35] [20][40][71]-[73] [36][37][53][78][77][43][44][45] [71]	Addresses privacy requirement in healthcare systems Focus on addressing different privacy requirements in reputation systems [36][53] Presents a privacy architecture for ubiquitous health based on soft trust [37] Discusses privacy and security vulnerabilities due to mobile computing in mobile health applications [78][77] privacy-preserving identity management for distributed e-health [43][44] Privacy protection in pervasive systems (challenges and state-of-the-art) [45] Privacy protection using soft trust in ubiquitous computing [71] Proposes a privacy-enabled Service Oriented Architecture (SOA) for health information integration and exchange	Healthcare Healthcare/distributed systems Healthcare Healthcare Healthcare Distributed systems Ubiquitous Healthcare	Centralized, Distributed WSN, Distributed distributed
[37][38][39][40][44][46][47][49][82]	[38],[44] Discusses security concerns and reviews existing approaches to address security requirements in wireless healthcare scenarios [46][47][82]Hybrid trust model (soft and hard trust) for enhancing security in distributed systems [37][38][39][40][44] Focuses on security issues in healthcare applications. Reviews work related to addressing security challenges [49] Focuses on work related to addressing security issues of reputation management systems for peer-to-peer networks	Healthcare Healthcare Healthcare/E-health	Distributed Distributed Distributed
[39]	Computing quality of the data (collected using participatory sensing) via TRS	Healthcare and other applications	Distributed
[39][40][48][20][53][55][56-59][71-73][78][77][79-82][86-89]	Literature addressing requirements of TRS in healthcare	Healthcare	Distributed
[49] - [51] [52]	Survey of trust management Schemes for online service [41][52], peer-to-peer [49], mobile ad-hoc networks [50], and wireless sensor networks [51]	Smart Environments, online TRSs	Centralized, Distributed
[42][60][62]	Discusses requirements for Robust TRSs	Smart environments, Healthcare	Centralized
[52]	Discusses possible attacks on TRSs	General online TRSs	Centralized
[40][55][56][57][58] [59]	Propose schemes to address adaptive behaviour problem	Healthcare, E-health	Centralized, Distributed
[61]	Proposes mechanism to handle free rider problem	Peer-to-peer TRSs (general online service domain)	Peer-to-peer networks
[62]	Review of techniques related to cold-start problems in recommender systems	TRSs in different application areas	Centralized, Distributed
[63], [65]-[70][20][55]	Emphasizes on the need for context-related information	Health care, E-health	Mobile computing
[70]	Proposes a hybrid context-based architecture supporting the selection of autonomous services in healthcare	Health	Body Sensor Networks
[55][20][57]	Focus on addressing reliability requirement by TRSs in healthcare domain	Healthcare, E-health	Centralized, Distributed
[20][55]	Focus on addressing default reputation score for new user problems	Healthcare, E-health	Centralized, Distributed
[20][55][42]	Focus on addressing time-sensitive requirements of TRSs in the healthcare domain	Healthcare, E-health	Centralized, Distributed
[72][73]	Proposed an anonymity scheme for TRSs in participatory sensing applications	Healthcare	Distributed
[20]	Presented a pseudo anonymity technique for TRSs in the EHR system	Healthcare	Distributed
[79]	Impact of cloud computing on health-care	Healthcare	Cloud
[80][81]	Reputation Model for Healthcare Services Availability in Cloud Computing	Healthcare	Cloud
[82][83][84]	Trust Management in Body Area Networks	Healthcare	Distributed
[85]	Social Media and health care	Healthcare	Centralized, Distributed
[86][87][88][89]	Reputation Schemes for Pervasive Social Networks	Healthcare and other applications	Distributed

life, the service consumer's preferences related to selection of service provider may vary based on the information related to quality measures. Considering service consumer's opinions about influential attributes (quality measures) related to the health-care providers and organizations helps to gauge the statistical significance of each attribute to overall trust degree [90]. Moreover, for health service providers to guard their reputations, they must know which trust attributes they need to address. This could enhance monitoring and evaluation endeavors, which may in turn result in improved health care. For example, in case of healthcare professional the quality measures, such as *ability, integrity*, and *benevolence*, are common in literature related to trust. *Ability* refers to skills, competencies, and characteristics, which enable a trustee to provide influence in a specific context. In this case, if a trustee is a healthcare professional, then the ability refers to the skills, competencies, and characteristics required for appropriate diagnosis and correct treatment in the specific medical domain. *Benevolence* refers to the intention of the trustee to do the right thing instead of maximizing profits. For healthcare professionals, benevolence is closely associated with synonyms such as loyalty, openness, caring, non-exploitation, trust, easy to reach, supporting the privacy of the patient and responsive. *Integrity* refers to the adherence of the trustee to accepted rules of conduct, standards and the state legal policies, competence in communication and interpersonal skills, ethics such as honesty and keeping promises. There exists work that discusses the importance of identifying influential attributes towards overall patient satisfaction [91]–[93]. Müller *et al.* [92] in their work reviewed the literature and identified several trust in physician measures. The authors stresses on the need of good quality measures to assess trust in physician. The collection, representation, maintenance and querying of information based on required quality measures are important aspects to be addressed in order to determine adequate information at the adequate time for the right people. This in turn will allow to address the requirements of context awareness, reliability, and accuracy in an effective and efficient manner.

Moreover, in case of Healthcare Organization (HCO), the trust quality measures can be divided in the following dimensions: *trustee dimension, information content dimension, information and communication technology dimension, institutional dimension*. As discussed above, the trustworthiness characteristics of the trustee, include quality measures: *ability*, *integrity*, and *benevolence*. The *ability* in case of HCO refers to the logistics of delivering effective technological support, effective change processes, diagnoses and treatment quality, service availability and accessibility, and a well-trained workforce (having the required certifications and qualifications). For the HCO, *benevolence* is closely related to service affordability, privacy & security support, patient-centred care, facility infrastructure, support for information technology, and the provision of support systems (training, supervision, quality and safety assurance). *Integrity* refers to the adherence of the trustee to accepted rules of conduct, standards and the state legal policies, competence in communication and interpersonal skills, ethics such as honesty and keeping promises. The *information content* dimension of trust refers to attributes that determine the trustworthiness of the data, such as accuracy, completeness, timeliness, relevance, legibility, accessibility, and usefulness. The major sources of risk are related to the quality of the data held within an EHR. The *information and communication technology* dimension of trust considers quality measures that deal with the secure and effective data exchange, system interoperability & data standards, privacy & security support, and interoperability between heterogeneous devices (including health monitoring devices and access devices). It facilitates capturing, integrating, and analyzing clinical, administrative, and financial data to support patient-centeredness and healthcare efficiency. Furthermore, this trust dimension is about making information systems (the participating entities in a transaction) trust each other in heterogeneous and distributed multisystem environments. The *institutional* dimension considers third-party memberships and other attributes that shape the health organization environment, including accreditation, professional standard review, quality assurance, authentication approvals, policies, legal requirements and authorities, among others.

This emphasizes on the need to conduct further investigations to develop mechanisms for the identification of trust quality measures for the different stakeholders involved in the health care, about which the customers are concerned. The trust value can be computed using machine learning techniques [94], probabilistic and fuzzy logic techniques [95].

The other major areas where reputation systems in healthcare are used and where further investigations can be done are as follows:

- *Scalable TRSs for Ubiquitous Health Systems*

Considering the need of the day, emphasis should be placed on pervasive and ubiquitous health scenarios in which reputation is inherently distributed and the environment is dynamic [48]. There exist work that addresses some of the requirements of TRSs in ubiquitous and pervasive healthcare [36] [53]. The published studies [20], [55], [71] do provide support regarding the interoperability of different TRSs. Moreover, additional research is needed to create TRS interoperability & portability in ubiquitous health. The reliability of the TRS will be important to consider when fusing feedback from multiple TRSs supporting the use of different reputation scoring functions, or when importing scores from one application area into other.

Moreover, there is a need to build scalable systems supporting combining cryptography-based security regimes with security and privacy decisions based on soft trust. Some studies have emphasized this need [36], [44], [47], [53] and some used it in their proposed solution [82], but there is a dearth of work related to addressing the associated challenges of implementing such systems. Due to the geographical distribution of service providers and service consumers, acquiring trust necessitates not only an understanding of different

national legal frameworks but also an understanding of ways to acclimate such differences. In an open environment consisting of multiple entities having varying roles and interests, the privacy and security requirements vary. To support ubiquitous health in a true manner, there is a need to conduct further investigations on developing legislation that addresses the requirements of privacy and security in the healthcare domain.

There remain many unresolved research issues in the design and development of a new trust and reputation model for open, dynamic, distributed and heterogeneous healthcare systems. For example, determining the appropriate time window for reputation calculation in a specific context, the evaluation of ratings in multiple contexts, a mechanism for evaluating the trustworthiness of medical data, a context-based reputation access meeting specific criteria. Some work emphasizes the importance of incorporating context information in trust decisions related to health [67]–[70]. There is a need to focus on the practical implementation of TRSs that address all context-specific challenges. Moreover, there is a need to define ontologies for the health domain considering the different e-health applications and the involved stakeholders.

• *Reputation Schemes for Pervasive Social Networking*

Social networking has been an essential part of todays world. Several healthcare social network platforms have been established [85]. Some platforms are established with the aim to help physicians diagnose and treat their existing patients. Other platforms are formed to help patients with troubling medical conditions, to get support from the network's members [85]. Advances in mobile technology coupled with the rapid advancement in the social networking lead to the concept of Pervasive Social Networking (PSN) [86]. PSN can be achieved by allowing the mobile devices to communicate with each other for instant social activities at any time and in any places [87]–[89]. PSN demands high level of privacy. Moreover, in a social network, various content information flows. The problem is how to identify the accuracy of public messages. There exist work addressing such issue by keeping track of users' reputations [87]–[89]. Moreover, additional research is needed to address privacy and security requirements of PSN.

• *TRSs for Healthcare Services Availability in Cloud Computing*

The advancement in information technology allows the patients to express their voices in a powerful way. Patients (service consumers) play an increasingly important decision making role in the healthcare market. The advancement in technology allows the patient to play active role in taking care of their health by performing the activities like: (i) reading reviews/reputations about healthcare professionals and organizations; (ii) sharing their EHR stored at different health service providers with their doctors; (iii) participating in healthcare social network platforms; (iv) using sensors, smart phones to track their vital signs, diet and exercise. Such active involvement of the users in turn require easily accessible, highly-interactive, scalable, and efficient healthcare provider systems. To address the growing needs of healthcare consumer, cloud computing is playing an important role. There exist work that studies the impact, incentives and hindrances to adopt cloud computing in health care [79]. Aslam *et al.* [80] presents cloud reputation evaluation model to evaluate the telemedicine based cloud computing services by considering the quality of services provided. In [81] a multi-faceted reputation evaluation method is presented that allows selection of cloud services considering various quality of service metrics. Additional research is needed to address privacy and security requirements of cloud as well as selection of cloud service provider.

• *TRSs for Wireless Body Area Network (WBAN)*

WBAN requires trust management to be taken place in a real time setting so that trustworthiness can be ensured to all stakeholders involved. The trustworthiness requirement among users is significant in order to improve the privacy and security of data communication. There exists work [73], [82], [83], that addresses the privacy and security requirements in WBAN, using a reputation-based scheme. In [83], a trust based scheme is presented for reliable and trustworthy collection of patient's physiological data. Additional research is needed to address trustworthy collection of patient's physiological data, privacy and security requirements of WBAN [84].

VI. CONCLUSION

Healthcare reputation management allows real-time insights about what the people are saying about healthcare organization locations, facilities, services, quality, technology and health-care providers etc. This paper provides insight into the various challenges, design considerations, key requirements related to developing Trust and Reputation System (TRS) in the domain of healthcare, and discussed how existing work have addressed these requirements over the years. A reference model for measuring the performance and features of TRSs is proposed. Existing TRSs in healthcare are compared using the proposed reference model. Moreover, we have highlighted several future areas of research for TRSs that are currently under-represented in existing literature.

There is a need to develop reputation-based trust mechanisms beyond doctor-patient relationships to address issues related to the main application areas of e-Health, including EHR systems, ubiquitous & pervasive health, pervasive social networking, WBAN, telemedicine & telecare services and decision support systems. There is evidence that soft trust supports dynamic decision-making and can be used in situations where partial or no hard trust mechanisms exist, or vice versa. Therefore, the use of soft trust in healthcare systems could improve patient-centred healthcare.

REFERENCES

[1] S. Ozawa and P. Sripad, "How do you measure trust in the health system? A systematic review of the literature," *Social Sci. Med.*, vol. 91, pp. 10–14, Aug. 2013, doi: 10.1016/j.socscimed.2013.05.005.

[2] K. Browne, D. Roseman, D. Shaller, and S. Edgman-Levitan, "Analysis & commentary measuring patient experience as a strategy for improving primary care," *Health Affairs*, vol. 29, no. 5, pp. 921–925. 2010, doi: 10.1377/hlthaff.2010.0238.

[3] J. Veloski, J. R. Boex, M. J. Grasberger, A. Evans, and D. B. Wolfson, "Systematic review of the literature on assessment, feedback and physicians' clinical performance: BEME guide No. 7," *Med. Teacher*, vol. 28, no. 2, pp. 117–128, Mar. 2006, doi: 10.1080/01421590600622665.

[4] D. J. Scotti and R. N. Stinerock, "Cognitive predictors of satisfaction with hospital inpatient service encounters among the elderly," *J. Hospital Marketing, PR*, vol. 14, no. 2, pp. 3–22, 2003.

[5] D. Mechanic and S. Meyer, "Concepts of trust among patients with serious illness," *Social Sci. Med.*, vol. 51, no. 2, pp. 657–668, 2000.

[6] L. Gilson, "Trust and the development of health care as a social institution," *Social Sci. Med.*, vol. 56, no. 7, pp. 1453–1468, 2003.

[7] N. L. Keating, D. C. Green, A. C. Kao, J. A. Gazmararian, V. Y. Wu, and P. D. Cleary, "How are patients' specific ambulatory care experiences related to trust, satisfaction, and considering changing physicians?" *J. Gen. Internet Med.*, vol. 17, no. 1, pp. 29–40, 2002.

[8] S. Joffe, M. Manocchia, J. C. Weeks, and P. D. Cleary, "What do patients value in their hospital care? An empirical perspective on autonomy centred bioethics," *J. Med. Ethics*, vol. 29, no. 2, pp. 103–108, 2003.

[9] L. M. Verhoef, T. H. Van de Belt, L. J. L. P. G. Engelen, L. Schoonhoven, and R. B. Kool, "Social media and rating sites as tools to understanding quality of care: A scoping review," *J. Med. Internet Res.*, vol. 16, no. 2, p. e56, 2014, doi: 10.2196/jmir.3024.

[10] California Healthcare Foundation. *80% of Internet Users Look for Health Information Online*. Accessed: Jan. 2018. [Online]. Available: http://www.pewinternet.org/files/old-media/Files/Reports/2011/PIP_Health_Topics.pdf

[11] B. Kadry, L. F. Chu, B. Kadry, D. Gammas, and A. Macario, "Analysis of 4999 online physician ratings indicates that most patients give physicians a favorable rating," *J. Med. Internet Res.*, vol. 13, no. 4, p. e95, 2011.

[12] S. Reimann and D. Strech, "The representation of patient experience and satisfaction in physician rating sites. A criteria-based analysis of English- and German-language sites," *BMC Health Services Res.*, vol. 10, no. 1, p. 332, 2010. [Online]. Available: http://liveclinic.com/blog/healthcare/the-top-10-doctor-review-sites/, doi: 10.1186/1472-6963-10-332.

[13] T. Lagu, N. S. Hannon, M. B. Rothberg, and P. K. Lindenauer, "Patients' evaluations of health care providers in the era of social networking: An analysis of physician-rating Websites," *J. Gen. Internet Med.*, vol. 25, no. 9, pp. 942–946, 2010, doi: 10.1007/s11606-010-1383-0.

[14] *How Hospitals Hope to Boost Ratings on Yelp, HealthGrades, ZocDoc and Vitals*, Washington Post (WP Company LLC), Washington, DC, USA, Jun. 2015. [Online]. Available: https://www.washingtonpost.com/national/health-science/sites-like-yelp-can-be-tough-but-hospitals-embrace-online-reviews/2015/06/03/a07a68b6-fe63-11e4-805c-c3f407e5a9e9_story.html?utm_term=.bd17eb728a34

[15] M. Emmert, N. Meszmer, and U. Sander, "Do health care providers use online patient ratings to improve the quality of care? Results from an online-based cross-sectional study," *J. Med. Internet Res.*, vol. 18, no. 9, p. e254, Sep. 2016, doi: 10.2196/jmir.5889.

[16] N. Bacon, "Will doctor rating sites improve standards of care? Yes," *Brit. Med. J.*, vol. 338, no. 1, pp. 688–689, 2009.

[17] Health News. (Feb. 23, 2017). *Doctor-Rating Websites Lack Helpful Information*. [Online]. Available: http://www.reuters.com/article/us-health-consumers-doctor-rating-idUSKBN1622NF

[18] *Authorities and Trusts–The NHS in England—NHS Choices*. Accessed: Apr. 10, 2017. [Online]. Available: http://www.nhs.uk/NHSEngland/thenhs/about/Pages/authoritiesandtrusts.aspx

[19] J. P. Harrison and A. Lee, "The role of e-Health in the changing health care environment," *Nurs Econ.*, vol. 24, no. 6, pp. 283–288, 2006.

[20] B. Alhaqbani, A. Jøsang, and C. Fidge, "A medical data reliability assessment model," *J. Theor. Appl. Electron. Commerce Res.*, vol. 4, no. 2, pp. 64–78, 2009.

[21] J. L. Fernández-Alemán, I. C. Señor, P. A. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1532046412001864

[22] I. Brown and A. A. Adams, "The ethical challenges of ubiquitous healthcare," *Int. Rev. Inf. Ethics*, vol. 8, pp. 53–60, Dec. 2007.

[23] F. Sarhan, "Telemedicine in healthcare 1: Exploring its uses, benefits and disadvantages," *Nursing Times*, vol. 105, no. 42, pp. 10–13, 2009.

[24] G. N. Forrest, T. C. Van Schooneveld, R. Kullar, L. T. Schulz, P. Duong, and M. Postelnick, "Use of electronic health records and clinical decision support systems for antimicrobial stewardship," *Clin. Infectious Diseases*, vol. 59, no. 3, pp. S122–S133, Oct. 2014, doi: 10.1093/cid/ciu565.

[25] D. Uniyal and V. Raychoudhury. (Nov. 2014). "Pervasive healthcare-a comprehensive survey of tools and techniques." [Online]. Available: https://arxiv.org/abs/1411.1821

[26] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2688–2710, Oct. 2010.

[27] V. R. S. Dhulipala, P. Devadas, and P. H. S. T. Murthy, "Mobile phone sensing mechanism for stress relaxation using sensor networks: A survey," *Wireless Pers. Commun.*, vol. 86, no. 2, pp. 1013–1022, 2016.

[28] J. K. Y. Ng, "Ubiquitous healthcare: Healthcare systems and applications enabled by mobile and wireless technologies," *J. Converg.*, vol. 3, no. 2, pp. 31–36, 2012.

[29] S. McKnight, "Telehealth: Applications for complex care," *Online J. Nursing Informat.*, vol. 16, no. 3, pp. 1–6, Oct. 2012. [Online]. Available: http://ojni.org/issues/?p=2034

[30] ALLYHEALTH. (Mar. 9, 2014). *Telecare Will Change Our Health System Forever*. [Online]. Available: http://www.allyhealth.net/telecare-will-change-our-health-system-forever/

[31] F. G. Andriopoulou, K. Birkos, and D. Lymberopoulos, "P2Care: A dynamic peer-to-peer network for collaboration in personalized healthcare service delivery," *Comput. Ind.*, vol. 69, pp. 45–60, May 2015. [Online]. Available: http://dx.doi.org/10.1016/j.compind.2014.09.007

[32] Y. Li, L. James, and J. McKibben, "Trust between physicians and patients in the e-health era," *Technol. Soc.*, vol. 46, pp. 28–34, Aug. 2016. [Online]. Available: http://doi.org/10.1016/j.techsoc.2016.02.004

[33] R. Kukafka *et al.*, "Redesigning electronic health record systems to support public health," *J. Biomed. Inform.*, vol. 40, no. 4, pp. 398–409, Aug. 2007. [Online]. Available: http://doi.org/10.1016/j.jbi.2007.07.001

[34] J. B. Rotter, "A new scale for the measurement of interpersonal trust," *J. Pers.*, vol. 35, no. 4, pp. 651–665, 1967.

[35] C. T. Di Iorio and F. Carinci, "Privacy and health care information systems: Where is the balance?" in *eHealth: Legal, Ethical and Governance Challenges*, C. George, D. Whitehouse, and P. Duquenoy, Eds. Berlin, Germany: Springer, 2013.

[36] S. P. Ruotsalainen, B. Blobel, A. Seppälä, and P. Nykänen, "Trust information-based privacy architecture for ubiquitous health," *JMIR Mhealth Uhealth*, vol. 1, no. 2, p. 23, 2013.

[37] B. Martínez-Pérez, I. de la Torre-Díez, M. López-Coronado, "Privacy and security in mobile health apps: A review and recommendations," *J. Med. Syst.*, vol. 39, p. 181, Jan. 2015, doi: 10.1007/s10916-014-0181-3.

[38] I. Krontiris, "Sensor networks security for pervasive healthcare," in *Wireless Technologies: Concepts, Methodologies, Tools and Applications*. Hershey, PA, USA: IGI Global, 2012, pp. 967–983, doi: 10.4018/978-1-61350-101-6.

[39] K. L. Huang, S. S. Kanhere, and W. Hu, "Are you contributing trustworthy data?: The case for a reputation system in participatory sensing," in *Proc. 13th ACM Int. Conf. Modeling, Anal., Simulation Wireless Mobile Syst. (MSWiM)*, 2010, pp. 14–22.

[40] A. Jøsang, "Online reputation systems for the health sector," *Electron. J. Health Inform.*, vol. 3, no. 1, pp. 1–5. 2008. [Online]. Available: http://www.ejhi.net/

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

[42] A. Josang and J. Haller, "Dirichlet reputation systems," in *Proc. 2nd Int. Conf. Availability, Rel. Security*, Washington, DC, USA, Apr. 2007, pp. 112–119.

[43] C. Bettini and D. Riboni, "Privacy protection in pervasive systems: State of the art and technical challenges," *Pervasive Mobile Comput.*, vol. 17, pp. 159–174, Feb. 2015. [Online]. Available: http://dx.doi.org/10.1016/j.pmcj.2014.09.010

[44] P. Kumar and H. J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012, doi: 10.3390/s120100055.

[45] J. Goecks and E. Mynatt, "Enabling Privacy management in ubiquitous computing environments through trust and reputation systems," in *Proc. ACM Conf. Comput. Supported Cooper. Work (CSCW)*, New Orleans, LA, USA, Nov. 2002, pp. 1–4.
[46] C. Lin and V. Varadharajan, "A hybrid trust model for enhancing security in distributed systems," in *Proc. 2nd Int. Conf. Availability, Rel. Security (ARES)*, 2007, pp. 35–42.
[47] A. Joshi, T. Finin, L. Kagal, J. Parker, and A. Patwardhan, "Security policies and trust in ubiquitous computing," *Phil. Trans. Roy. Soc. A*, vol. 366, pp. 3769–3780, Oct. 2008.
[48] W. Yuan, D. Guan, S. Lee, and H. Lee, "Using reputation system in ubiquitous healthcare," in *Proc. 9th Int. Conf. E-Health Netw., Appl. Services*, Taipei, Taiwan, 2007, pp. 182–186.
[49] C. Selvaraj and S. Anand, "A survey on security issues of reputation management systems for peer-to-peer networks," *Comput. Sci. Rev.*, vol. 6, no. 4, pp. 145–160, Jul. 2012. [Online]. Available: http://dx.doi.org/10.1016/j.cosrev.2012.04.001
[50] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.
[51] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 602–617, May 2014.
[52] S. Vavilis, M. Petković, and N. Zannone, "A reference model for reputation systems," *Decision Support Syst.*, vol. 61, pp. 147–154, May 2014. [Online]. Available: http://dx.doi.org/10.1016/j.dss.2014.02.002
[53] P. S. Ruotsalainen, B. G. Blobel, A. V. Seppälä, H. O. Sorvari, and P. A. Nykänen, "A conceptual framework and principles for trusted pervasive health," *J. Med. Internet Res.*, vol. 14, no. 2, p. e52, 2012. [Online]. Available: http://www.jmir.org/2012/2/e52/, doi: 10.2196/jmir.1972.
[54] A. Jøsang, ""Robustness of trust and reputation systems: Does it matter?" in *Trust Management*(IFIP Advances in Information and Communication Technology). Berlin, Germany: Springer, 2012, pp. 253–262. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-29852-3_21
[55] T. V. Deursen, P. Koster, and M. Petkovi, "Hedaquin: A reputation-based health data quality indicator," *Electron. Notes Theor. Comput. Sci.*, vol. 197, no. 2, pp. 159–167, Feb. 2008.
[56] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843–857, Jul. 2004, doi: 10.1109/TKDE.2004.1318566.
[57] L. Weitzel, J. P. M. de Oliveira, and P. Quaresma, "Measuring the reputation in user-generated-content systems based on health information," *Proc. Comput. Sci.*, vol. 29, pp. 364–378, Jun. 2014, doi: 10.1016/j.procs.2014.05.033.
[58] F. G. Mármol and G. M. Pérez, "Providing trust in wireless sensor networks using a bio-inspired technique," *Telecommun. Syst.*, vol. 46, no. 2, pp. 163–180, 2011.
[59] A. Boukerche and Y. Ren, "A secure mobile healthcare system using trust-based multicast scheme," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 387–399, May 2009.
[60] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Comput. Surveys*, vol. 42, no. 1, Dec. 2009, Art. no. 1.
[61] C. M. Burkle and M. T. Keegan, "Popularity of Internet physician rating sites and their apparent influence on patients' choices of physicians," *BMC Health Ser. Res.*, vol. 15, p. 416, Apr. 2015.
[62] L. H. Son, "Dealing with the new user cold-start problem in recommender systems: A comparative review," *Inf. Syst.*, vol. 58, pp. 87–104, Jun. 2016. [Online]. Available: http://dx.doi.org/10.1016/j.is.2014.10.001
[63] G. Chen and D. Kotz, "A survey of context-aware mobile computing research," Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2000-381, Nov. 2000.
[64] A. Soylu, P. de Causmaecker, and P. Desmet, "Context and adaptivity in pervasive computing environments: Links with software engineering and ontological engineering," *J. Softw.*, vol. 4, no. 9, pp. 992–1013, Nov. 2009.
[65] D. Sánchez, M. Tentori, and J. Favela, "Activity recognition for the smart hospital," *IEEE Intell. Syst.*, vol. 23, no. 2, pp. 50–57, Mar./Apr. 2008.
[66] Q. Liu, H. Ma, E. Chen, and H. Xiong, "A survey of context-aware mobile recommendations," *Int. J. Inf. Technol. Decision Making*, vol. 12, no. 1, pp. 139–172, 2013.
[67] N. Bricon-Souf and C. R. Newman, "Context awareness in health care: A review," *Int. J. Med. Inform.*, vol. 76, no. 1, pp. 2–12, 2007.
[68] A. Behrooz and A. Devlic, "A context-aware privacy policy language for controlling access to context information of mobile users," in *Security and Privacy in Mobile Information and Communication Systems. MobiSec* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 94, R. Prasad, K. Farkas, A. U. Schmidt, A. Lioy, G. Russello, and F. L. Luccio, Eds. Berlin, Germany: Springer, 2012.
[69] A. Seppälä, P. Nykänen, and P. Ruotsalainen, "Privacy-related context information for ubiquitous health," *JMIR mHealth uHealth.*, vol. 2, no. 1, p. e12, 2014, doi: 10.2196/mhealth.3123.
[70] G. Fenza, D. Furno, and V. Loia, "Hybrid approach for context-aware service discovery in healthcare domain," *J. Comput. Syst. Sci.*, vol. 78, pp. 1232–1247, Jul. 2012.
[71] G. Tormo, F. Marmol, J. Girao, and G. Perez, "Identity management–In privacy we trust: Bridging the trust gap in ehealth environments," *IEEE Security Privacy*, vol. 11, no. 6, pp. 34–41, Jun. 2013, doi: 10.1109/MSP.2013.80.
[72] D. Christin, C. Roßkopf, M. Hollick, L. A. Martucci, and S. S. Kanhere, "IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications," *Pervas. Mobile Comput.*, vol. 9, no. 3, pp. 353–371, Jun. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.pmcj.2013.01.003
[73] X. O. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "ARTSense: Anonymous reputation and trust in participatory sensing," in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013, pp. 2517–2525.
[74] F. G. Mármol and G. M. Pérez, "Security threats scenarios in trust and reputation models for distributed systems," *Comput. Secur.*, vol. 28, no. 7, pp. 545–556, Oct. 2009. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2009.05.005
[75] M. Emmert, M. Maryschok, S. Eisenreich, and O. Schöffski, "[Websites to assess quality of care–appropriate to identify good physicians?]" *Gesundheitswesen*, vol. 71, no. 4, pp. e18–e27, 2009, doi: 10.1055/s-0028-1103288.
[76] M. Emmert, U. Sander, and F. Pisch, "Eight questions about physician-rating websites: A systematic review," *J. Med. Internet Res.*, vol. 15, no. 2, p. e24. 2013, doi: 10.2196/jmir.2360.
[77] S. Bahtiyar and M. U. Çaglayan, "Trust assessment of security for e-health systems," *Electron. Commerce Res. Appl.*, vol. 13, no. 3, pp. 164–177, May/Jun. 2014. [Online]. Available: http://doi.org/10.1016/j.elerap.2013.10.003
[78] R. Au and P. Croll, "Consumer-centric and privacy-preserving identity management for distributed e-health systems," in *Proc. HICSS*, 2008, pp. 234–243.
[79] *Impact of Cloud Computing on Health-Care, Cloud Standard Customer Council*. [Online]. Available: http://www.cloud-council.org/deliverables/CSCC-Impact-of-Cloud-Computing-on-Healthcare.pdf
[80] W. Aslam, F. Javeed, and M. I. Lali, "A quantitative reputation model for healthcare services availability in cloud computing," *J. Med. Imag. Health Inform.*, vol. 7, no. 6, pp. 1380–1384, 2017, doi: 10.1166/jmihi.2017.2147.
[81] M. Wang, G. Wang, J. Tian, H. Zhang, and Y. Zhang, "An Accurate and multi-faceted reputation scheme for cloud computing," *Procedia Comput. Sci.*, vol. 34, pp. 466–473, Jan. 2014. [Online]. Available: https://doi.org/10.1016/j.procs.2014.07.021
[82] M. I. Shanmugapriya and K. Karthikeyan, "Reputation based incentive scheme for secured data privacy in wireless body area network communication," *Adv. Comput. Sci. Technol.*, vol. 10, no. 7 pp. 2095–2117, 2017.
[83] W. Li and X. Zhu, "Recommendation-based trust management in body area networks for mobile healthcare," in *Proc. IEEE 11th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Philadelphia, PA, USA, Oct. 2014, pp. 515–516, doi: 10.1109/MASS.2014.85.
[84] S. Yu, M. Li, and L. Shi, "Trust establishment in wireless body area networks," in *Wireless Technologies: Concepts, Methodologies, Tools and Applications/Information Resources Management Association*, vol. 1. Hershey, PA, USA: IGI-Global, 2012, doi: 10.4018/978-1-61350-101-6.ch406.
[85] C. L. Ventola, "Social media and health care professionals: Benefits, risks, and best practices," *Pharmacy Therapeutics*, vol. 39, no. 7, pp. 491–520, 2014.
[86] Y. Chen, Z. Yan, and V. Niemi, "Implementation of a reputation system for pervasive social networking," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Changsha, China, Nov. 2011, pp. 857–862, doi: 10.1109/TrustCom.2011.115.

[87] Z. Yan, Y. Chen, and Y. Shen, "PerContRep: A practical reputation system for pervasive content services," *J. Supercomput.*, vol. 70, no. 3, pp. 1051–1074, 2014.
[88] Z. Yan, Y. Chen, and Y. Shen, "A practical reputation system for pervasive social chatting," *J. Comput. Syst. Sci.*, vol. 79, no. 5, pp. 556–572, 2013. [Online]. Available: https://doi.org/10.1016/j.jcss.2012.11.003
[89] L. Garms, K. Martin, and S.-L. Ng, "Reputation schemes for pervasive social networks with anonymity," in *Proc. 15th Int. Conf. Privacy, Secur. Trust (PST)*, 2017, pp. 1–10.
[90] W. Maharani, W. Maharani, and S. Saadah, "Feature extraction and opinion classification using class sequential rule on customer product review," in *Proc. IEEE Inf. Commun. Technol. (ICoICT)*, May 2016, pp. 1–5.
[91] N. Brennan, R. Barnes, M. Calnan, O. Corrigan, P. Dieppe, and V. Entwistle, "Trust in the health-care provider–patient relationship: A systematic mapping review of the evidence base," *Int. J. Quality Health Care*, vol. 25, no. 6, pp. 682–688, Dec. 2013. [Online]. Available: https://doi.org/10.1093/intqhc/mzt063
[92] E. Müller, J. M. Zill, J. Dirmaier, M. Härter, and I. Scholl, "Assessment of trust in physician: A systematic review of measures," *PLoS ONE*, vol. 9, no. 9, p. e106844, 2014. [Online]. Available: https://doi.org/10.1371/journal.pone.0106844
[93] T. N. Anand and V. R. Kutty, "Development and testing of a scale to measure trust in the public healthcare system," *Indian J. Med. Ethics*, vol. 12, no. 3, pp. 149–157, 2015. [Online]. Available: https://doi.org/10.20529/IJME.2015.044
[94] X. Liu, A. Datta, and E.-P. Lim, *Computational Trust Models and Machine Learning*, 1st ed. London, U.K.: Chapman & Hall, 2014.
[95] G. Acampora, A. Castiglione, and A. Vitiello, "A fuzzy logic based reputation system for E-markets," in *Proc. IEEE Int. Conf. Fuzzy Syst.*, Jul. 2014, pp. 865–872.

FARHANA JABEEN received the Ph.D. degree from the School of Computer Science, Manchester University, U.K., in 2011. She is currently an Assistant Professor with the COMSATS Institute of Information Technology, Islamabad, Pakistan. Her research interests are focused on information security and privacy protection, trust model and management and reputation system, co-channel interference, algorithmic solutions to problems in wireless distributed networks including: query processing, spatial analysis, and localization and routing.

ZARA HAMID received the B.S. degree in software engineering from Hamdard University, Pakistan, in 2004, the M.S. degree in software engineering and the Ph.D. degree from the National University of Sciences and Technology, Pakistan, in 2007. She is currently an Assistant Professor with the Department of Computer Science, COMSATS Institute of Information Technology. Her research interests include design and performance evaluation of communication protocols and QoS provisioning in wireless ad hoc and sensor networks and security and privacy issues in these networks.

ADNAN AKHUNZADA is currently an Assistant Professor and an In-charge BS Software Engineering and Telecommunication Networks Programme with the COMSATS Institute of Information Technology, Islamabad, Pakistan. He is also leading a research team with COMSATS involved in O2 project in collaboration with CERN Switzerland. He got a great experience of teaching international modules of the University of Bradford, U.K. He has published several high impact tier 1 research journal publications, the IEEE TRANSACTIONS, the IEEE *Communication Magazine* papers, other reputable magazine papers, book chapter, and national and international conference proceedings. His current research interests include secure design and modeling of software defined networks and future internet, large scale distributed systems (i.e., cloud, fog, edge), light weight cryptography, man-at-the-end attacks, human attacker attribution and profiling, and remote data auditing.

WADOOD ABDUL received the Ph.D. degree in signal and image processing from the University of Poitiers, France, in 2011.He is currently an Assistant Professor with the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University. His research interests are focused on color image watermarking, multimedia security, steganography, fingerprinting, and biometric template protection.

SANAA GHOUZALI received the master's and Ph.D. degrees in computer science and telecommunications from University Mohamed V-Agdal, Rabat, Morocco, in 2004 and 2009, respectively. In 2005 she has received a Fulbright grant to undertake dissertation research on a joint-supervision program at the Visual and Communication Laboratory, Cornell University, Ithaca, NY, USA. From 2009 to 2011, she was an Assistant Professor with the National school of Applied Sciences, Abdelmalek Essaadi University. In 2012, she joined with the College of Computer and Information Sciences, King Saud University, as an Assistant Professor. Her research interests include statistical pattern detection and recognition, biometrics, and biometric security and protection.