# Social Authentication Applications, Attacks, Defense Strategies and Future Research Directions: A Systematic Review

Noura Alomar, Mansour Alsaleh, Abdulrahman Alarifi

***Abstract*—The ever-increasing volumes of social knowledge shared in OSNs, the establishment of trustworthy social relationships over these platforms, and the emergence of technologies that allow friendship networks to be inferred from data exchanged in communication networks have motivated researchers to build socially-aware authentication schemes. We conduct the first study that surveys the literature related to social authentication. In this study, we not only created a taxonomy for classifying all social authentication schemes deployed in online or physical social contexts and extensively analyzed their authentication features, but also built a novel framework for evaluating the effectiveness of all social authentication schemes, identified all the practical and theoretical attacks that may be mounted against such schemes, addressed possible defense strategies, and identified challenges, open questions, and future research opportunities. To measure their accuracy, strengths, weaknesses, and limitations, as well as to identify the potential of knowledge-based and trust-based social authentication schemes, a comprehensive comparative assessment of the security, usability, and deployability was conducted. We hope, by providing a solid foundation for gaining sufficient understanding of the manners in which users' social interactions have been utilized in user authentication schemes and their corresponding security implications, we will guide future research in this domain.**

***Index Terms*—Multi-Factor Authentication, Social Authentication, Social Factors, Social Media, Systematic Literature Review.**

## I. Introduction

THE growing demand that traditional authentication schemes be replaced, coupled with the uniqueness of the social knowledge surrounding every individual, have motivated researchers to exploit human-to-human relationships for authentication purposes. User authentication methods for granting or denying access to restricted content that are based on capturing individuals social contexts and exploiting users relationships with others have gained significant attention in the authentication research community. Thus, various socially aware schemes have been proposed as either primary or secondary authentication mechanisms. The abundance of social data in online social networking sites and the availability of mechanisms for analyzing the social connections between the users of these sites have facilitated the adoption of social authentication techniques on top of these online platforms. For instance, the large number of daily active users (DAUs) on Facebook (e.g., an average of 968 million DAUs in the second quarter of 2015 [1]), in addition to the huge number of photos that are posted on a daily basis (e.g., Facebook reported that its users uploaded more than 250 billion photos with an average of 350 million daily photo uploads in 2013 [2]) have contributed to making Facebook an attractive platform for deploying social authentication. Thus, the expansion of information sharing on Online Social Networks (OSNs), the availability of many different types of social information about the individuals on these platforms, and the ability to visualize the highly sophisticated nature of human social structures formed in these online virtual worlds appear to provide the required foundation for building secure and effective social authentication schemes [3], [4], [5]. Furthermore, the emergence of communication technologies that enable individuals to be continuously connected to their social communities and the growing availability of techniques that streamline the process of deriving the social interactions of large user populations from online or offline contexts could also lead existing social authentication schemes to a fundamentally promising direction.

In real life, people are naturally skilled at identifying their friends, acquaintances, family members, and enemies, for example, by recognizing their voices or associating them with past experiences [6]. However, in online communities, the visibility of individuals' social interactions is lower. Users' interactions on these virtual platforms may not necessarily resemble their real-world social interactions, as most OSNs allow the creation of multiple anonymous identities [7]. The complexity of verifying the accuracy of social knowledge and the difficulties involved in extracting and identifying the characteristics of trust relationships that could be utilized for identity verification highlight further the importance of measuring the robustness of social authentication mechanisms. One of the most important properties that differentiate these mechanisms from traditional authentication methods is that users' security levels are strongly affected by the security of the people they know [8]. Thus, users' inappropriate behaviors in social contexts and their misuse of social information could cause significant increases in the number of compromised users in social graphs. Further, the involvement of human factors in social authentication schemes may also contribute to an increase in the number of security vulnerabilities that can be exploited [9], [10]. For instance, a number of social engineering tricks could be employed for leaking users' sensitive social knowledge [11]. Therefore, a clear prerequisite

N. Alomar is with the College of Computer and Information Sciences, King Saud University, Riyadh, KSA, e-mail: nnalomar@ksu.edu.sa

M. Alsaleh and A. Alarifi are with King Abdulaziz City for Science and Technology, Riyadh, KSA, emails:{maalsaleh, aarifi}@kacst.edu.sa

of the success of these schemes is to explore their security implications, usability issues, and deployability in different contexts.

Prior research studies on social authentication have either focused on implementing new socially aware techniques [12], [13], [14], [15], investigating the security flaws of existing schemes [16], [17], [8], or proposing solutions to improve the security of existing methods [16]. Some proposed methods deploy social authentication as a second factor authentication technique, in combination with passwords, tokens, or biometrics [18], [19]. In spite of the variety of social authentication schemes that have been introduced in different contexts and the differences in the security features that they provide, there exists no survey that reviews and compares the state-of-the-art social authentication mechanisms. In this paper, we report the first research effort to survey the literature related to authenticating individuals based on their social characteristics and to identify the gaps that need to be filled. We analyze the various social authentication mechanisms that were previously implemented, define the underlying threat model and operational assumptions, and propose a categorization of the possible paths that can be followed to attack or manipulate these mechanisms. This paper also discusses possible defense and mitigation strategies. Our overarching goal is to identify the gaps that should be examined, highlight the limitations of existing social authentication approaches, and identify the means that can be utilized for designing effective, usable, reliable, and secure social authentication systems. Consequently, we expect this paper to become the gateway for making further key advances in this promising area of research.

**Contributions.** The primary research contributions of this paper are as follows.

1) **Systematic Review and Taxonomy of the Social Authentication Literature.** After proposing a precise definition of social authentication, we follow a structured methodology for comprehensively surveying all the research efforts related to social authentication, including publications and patents. This is the first study that surveys all the user authentication systems that have utilized any form of social knowledge or individuals' trustworthy interactions for authentication purposes, whether or not explicitly stated by their designers. We also propose a taxonomy for classifying all the research lines related to social authentication, covering social authentication schemes deployed in networked environments, physical contexts, and online social networks.
2) **Security Analysis of Social Authentication Mechanisms.** According to our detailed investigation of the authentication features offered by socially aware systems employed in OSNs or offline contexts, for each social authentication mechanism included in our study, we identify the threat model and the attack surface associated with its deployment and explore the corresponding possible defense strategies.
3) **Establishment of a Framework for Analyzing and Evaluating Social Authentication Schemes.** After categorizing the existing social authentication schemes into knowledge-based and trust-based schemes, we define a novel evaluation framework that is specifically designed to analyze and understand the social properties of all knowledge-based and trust-based schemes, as well as to assess the usability, security, and deployability properties associated with the application of each social authentication mechanism. Using the developed framework as a basis, we comparatively analyze and evaluate the authentication features of all the reviewed schemes by investigating the characteristics of the trust relationships and social knowledge that they exploited for identity verification purposes and correlating them with their performance properties.
4) **Identification of Challenges, Open Issues, and Future Research Opportunities.** According to the observed strengths, weaknesses, and limitations of the surveyed social authentication schemes, we discuss the challenges associated with the involvement of social features in identity verification processes, envision future research opportunities, and concomitantly provide guidelines and recommendations with detailed discussions.

**Organization.** We first define social authentication and survey all the social authentication techniques in Section II. The threat model and attack surface of the surveyed social authentication mechanisms and the possible defense strategies are identified and analyzed in Sections IV and V, respectively. We also comparatively and comprehensively analyze the social authentication properties and evaluate the usability, security and deployability of the reviewed schemes in Sections III and VI, respectively. Open questions, challenges, and future research directions are highlighted in Section VII. Survey studies related to user authentication are then reviewed in Section VIII. Section IX concludes the paper.

## II. Social Authentication Definition and Techniques

To specify the scope of our review and because of the lack of a precise definition of social authentication, we propose a definition that is based on a set of conditions that must be met in a social authentication scheme. We also propose a taxonomy that characterizes the various social authentication schemes based on the types of the social elements that are leveraged in each scheme, i.e., social knowledge or trust relationships, and the means that are used to capture trustworthy interactions, i.e., through the direct involvement of human subjects or the implicit identification of trustworthy relationships. The following sections present the proposed definition and then review the schemes that have been developed or proposed and categorize them based on the taxonomy shown in Fig. 1 (see Appendix A for details about the research methodology followed to review the social authentication literature).

### *A. Social Authentication: A Definition*

As we focus on reviewing the user authentication schemes that leverage information extracted from users' social contexts or intermediate humans in their identity verification processes, all human-computer authentication techniques that rely on eliciting unique characteristics from individuals' social interactions with others are considered social authentication schemes. That is, a user authentication scheme that uses any form of social knowledge, utilizes users' trust relationships, monitors users' social contexts, or records users' friend associations for granting or denying access to any resource is considered a social authentication scheme, regardless of the context of its deployment. Any scheme that involves the intermediation of vouchers or trustees in the user authentication process is also considered a socially aware scheme. Additionally, an authentication scheme that evaluates users' authenticity based on the trustworthiness level of their social interactions, for example, befriending users on Facebook or retweeting posts on Twitter, or the correctness of social information inferred from users' online or offline social experiences, is included in this review. We consider even the schemes that indirectly infer trustworthy relationships, for example, through the existence of mutually trusted friends [20], social authentication schemes if the inferred transitive trust relationships are used for identity verification purposes. Thus, we define social authentication as follows:

> "The direct or indirect utilization of social knowledge or trust relationships in human-computer authentication systems deployed in online or offline contexts."

Research studies that address the utilization of social knowledge or trustworthy interactions for purposes other than authenticating individuals are outside the scope of the present work, for example, studies on improving users experiences by using their social data for building personalized and customized user interfaces, as discussed in [21]. Further, we do not consider user authentication systems that are built on top of existing OSNs to be social authentication schemes if they base their identity verification processes on knowledge items that are not extracted from users' social contexts, such as biometric templates [22]. For example, the knowledge-based user authentication scheme that was built on top of Twitter [23] is excluded, because its challenge questions primarily ask about users' recent lunches without involving any social element. For the same reason, we do not treat the authentication scheme proposed in [24] as a social authentication system, because asking about users' e-mail content may not necessarily imply that the challenge questions, for example, asking about the date on which an email was received, were designed based on users' social interactions. Further, the user authentication systems that utilize access credentials associated with user accounts in OSNs for facilitating access to other federated platforms (e.g., accessing health information management systems, as discussed in [25]) are not considered social authentication systems if they do not leverage social data or trust relationships in their underlying identity verification processes. We also intentionally exclude authentication schemes that involve machine claimers and machine verifiers [26].

### *B. Social Authentication Techniques: A Review*

Previously developed socially aware authentication systems have either leveraged social knowledge to authenticate users or allowed individuals to vouch for each other [19]. The majority of the proposed knowledge-based social authentication schemes are based mainly on photos published by users in online social networking sites [15]. In the case of trust-based authentication mechanisms, a number of researchers have taken advantage of trust relationships between people to build socially aware authentication techniques. There also exist schemes that rely on extracting information from users' social contexts and use this information for validating the identities of the users.

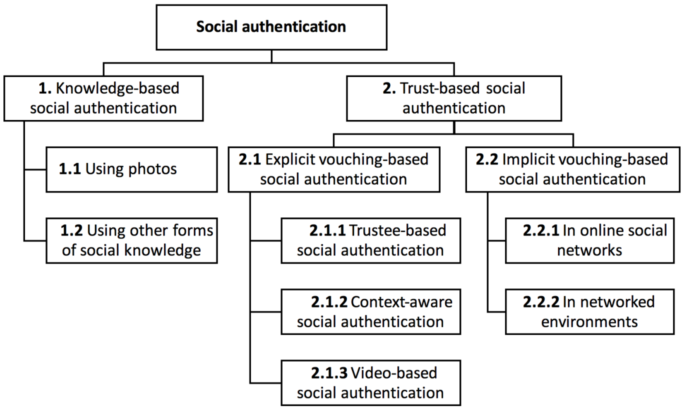
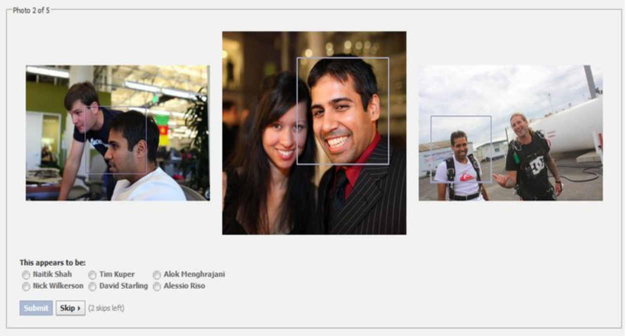

Social authentication
1. Knowledge-based social authentication
1.1 Using photos
1.2 Using other forms of social knowledge
2. Trust-based social authentication
2.1 Explicit vouching-based social authentication
2.1.1 Trustee-based social authentication
2.1.2 Context-aware social authentication
2.1.3 Video-based social authentication
2.2 Implicit vouching-based social authentication
2.2.1 In online social networks
2.2.2 In networked environments

Fig. 1. Taxonomy of social authentication schemes in the literature

*1) **Knowledge-Based Techniques:*** Knowledge-based social authentication mechanisms rely on the design of the security questions that ask the user about his/her social context, such as social relationships, conversations, or shared knowledge [27], [15], [28], [29]. These mechanisms may require the user either to recognize or recall some information about people he/she knows. Ideally, the basic assumption behind using social knowledge for designing challenge questions is that each individual has a unique social context that cannot be completely shared with others [16], [30]. Therefore, it is assumed that attackers face difficulties obtaining sufficient details about users' social contexts. As emphasized in [19], in order for challenge questions to be effective, their answers should be easily memorized, difficult to guess, and unreachable by unauthorized users. To achieve this, a number of research studies have focused mainly on designing authentication schemes that attempt to understand the social context surrounding the users and identify the social knowledge item that can provide their secure authentication. Although the majority of these studies have examined techniques that can be built on top of Facebook's photo-based two factor social authentication system [31], [32], few research attempts have focused on investigating other types of social knowledge that can be uniquely used for authenticating people. This paucity could be linked to the difficulty in analyzing individuals' social contexts, identifying the private social information that users can easily remember, and measuring the accuracy and uniqueness of social data.

Since currently used knowledge-based social authentication schemes, which were developed as variants of some existing two-factor authentication systems [33] (e.g. Facebook's Login Approval and Google 2-step authentication techniques [34],

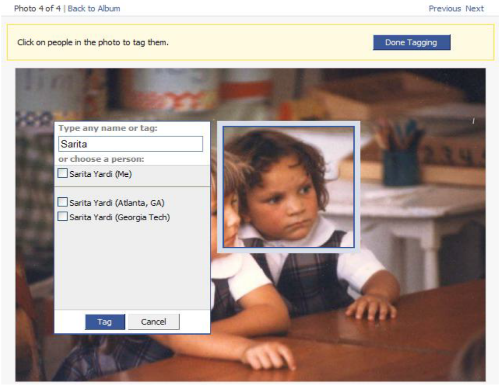


This appears to be:

○ Naitik Shah ○ Tim Kuper ○ Alok Menghrajani
○ Nick Wilkerson ○ David Starling ○ Alessio Riso

(2 skips left)

Fig. 2. Facebook's photo-based authentication scheme [31]



Click on people in the photo to tag them.

Type any name or tag: Sarita

or choose a person:

□ Sarita Yardi (Me)
□ Sarita Yardi (Atlanta, GA)
□ Sarita Yardi (Georgia Tech)

Fig. 3. Photo-tagging in Lineup [27]

[35]), are most frequently deployed on top of online social networking applications, we note that mechanisms that make it difficult for attackers to use publicly accessible social data to compromise users' accounts need to be developed. Further, because social authentication is most frequently deployed as a backup or emergency authentication method, the reliability and security of these schemes are of extreme importance and may be valued higher than their efficiency, since their frequency of use is less than that of their corresponding primary authenticators [19], [36], [18], [37], [12], [31]. Therefore, to avoid compromising users' accounts, backup social authentication methods must be at least as secure and reliable as their corresponding primary authentication methods [38]. In the following sections, we summarize the knowledge-based social authentication schemes that have been developed and discuss their security features.

**1.1 Photo-Based Social Authentication.** Photo-based social authentication schemes or graphical passwords [39], also known as social CAPTCHAs [40], ask the users to identify their friends in a set of images that are published in users' profiles and supplemented with tagging information [15], [41]. The first large-scale deployment of photo-based social authentication was built as an auxiliary authentication mechanism for detecting suspicious Facebook login attempts [15]. As shown in Fig. 2, Facebook's knowledge-based account recovery feature verifies users' identities by presenting photographs of their friends and asking them to name the persons who appear in them [31].

Three years before the release of Facebook's image-based social authentication scheme, Yardi et al. designed a photo-based scheme called Lineup, which leverages data generated from Facebook's social tagging process to authenticate users [27]. In order for a user to be permitted to access a particular Facebook group, based on using users' previously supplied tags, as shown in Fig. 3, Lineup asks the user to identify the names of subjects in a set of images [27], [15]. Lineup was built based on the assumption that a user knows the members of the Facebook group he/she is trying to access and therefore he/she should be able to recognize them and answer the challenge questions [15].

As an attempt to improve the security of photo-based socially aware schemes, Polakis et al. also developed a mechanism that increases the robustness of photo-based security challenges by classifying the photos into either *easy*, *medium*, or *difficult* to recognize [33]. The mechanism presented in [33] relies primarily on changing the quality of the selected images in order to make their automatic recognition by face software solutions difficult, while retaining users' abilities to identify the faces of the subjects who appear in the challenge questions [33]. The approach proposed in [33] follows a photo transformation process that increases the difficulty of challenge questions by modifying some photo properties, for example by rotating some of the included faces or changing the backgrounds of the images. While it might be argued that these modifications may make it difficult for users to identify their friends in the altered photos and thus negatively affect the usability of the corresponding user authentication scheme, the experimental evaluation presented in [33] shows that 99% of users were able to recognize the people they knew and thus answer the security questions.

Another approach for changing the difficulty of challenge questions, which was followed in Lineup [27], is to use the pre-provided photo tagging information to infer additional knowledge from the uploaded photos. In Lineup [27], the decision whether to present a user with a *simple*, *medium*, or *difficult* challenge question is based on the privacy settings that were previously defined [27]. For instance, a *simple* question may ask the user to name one of his/her friends in some photos whereas a *difficult* one may ask about the purpose of a specific Facebook group or event [27]. In [42], [32], the authors proposed another approach for deciding on the degree of difficulty of challenge questions presented to the user, which involves measuring the level of suspicion concerning the users' actions and adjusting the difficulty levels of challenge questions accordingly.

Table I presents additional examples of photo-based challenge questions with varying difficulty levels. Under the assumption that challenge questions become more difficult to guess as their difficulty level increases, the evaluation of the difficulty level of each question in Table I is based on a scale from 1, indicating that a question can be easily solved, to 5, which indicates that the corresponding question is difficult.

**1.2 Other Forms of Social Knowledge.** A few research studies have examined the applicability of using social knowledge other than individuals' published photos for authentication purposes. While the majority of social authentication schemes proposed in the literature were intended to be secondary authentication factors and are most frequently deployed on

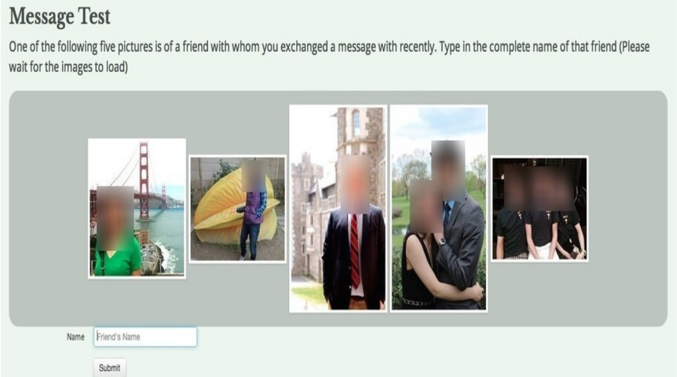
TABLE I
PHOTO-BASED SOCIAL AUTHENTICATION CHALLENGE QUESTIONS WITH VARYING DIFFICULTY

| Challenge Question | Difficulty Level |
|---|---|
| Who is the person? | 1 |
| Who are the person's friends? | 3 |
| When was the photo taken? | 5 |
| Where are the person's friends? | 5 |
| What happened at that time? | 3 |
| Who is the creator of the Facebook group you are trying to access? | 2 |
| Who captured the photo? | 3 |
| How many members have joined the Facebook group you are trying to access? | 2 |

top of online social networking sites, Frankel and Maheswaran proposed a primary social authentication technique that utilizes social knowledge extracted using wireless devices [30]. The fourth factor presented in their paper evaluates the social context surrounding the user and decides not to authenticate him/her if this context unexpectedly changed to include people not known to the user.

For the purpose of identifying other forms of social knowledge that can be leveraged in user authentication schemes, a categorization of social knowledge in online social networks was also proposed in [15]. Jain et al. discussed the manner in which challenge questions used in socially aware authentication systems can be based on information extracted from three main elements that represent social graphs in OSN systems [15]. According to their approach, a challenge question may be related to the properties of a *node*, an *edge*, or a *pseudo-edge* in the social graph associated with a specific user on OSN sites. Questions that are designed based on the attributes of a *node* in a social graph should ask only about data that belong to a specific friend. Therefore, a question that asks the user to name a friend, specify his/her birth date, or indicate his/her level of education is considered a *node* question. For instance, as Facebook's photo-based social authentication scheme asks the users to name their friends in a set of photos, the questions presented by this scheme are *node* questions.

On the other hand, when a user is challenged to provide information about an account that is commonly linked to his/her account and some of the accounts owned by his/her friends, this challenge question can be classified as a *pseudo-edge* question. For example, the social authentication system proposed in [43] challenges users to answer questions related to location information that is common to them and some of their trusted friends. A question about a restaurant, school, university, or any place that was frequently visited by both the user and some of his/her friends can also be categorized as a *pseudo-edge* question. The third type of challenge question that is used in socially aware schemes basically relies on asking a user about his/her interactions with other users in his/her social network. Therefore, questions that ask about a user's connections with others, for example, private messages, retweets, likes, or comments, are considered *edge* questions [15]. Table II presents additional examples of *node*, *edge*, and *pseudo-edge* challenge questions.


Message Test

One of the following five pictures is of a friend with whom you exchanged a message with recently. Type in the complete name of that friend (Please wait for the images to load)

Fig. 4. An Edge Question Generated by a Social Authentication Scheme [15]

TABLE II
EXAMPLES OF NODE, EDGE AND PSEUDO-EDGE QUESTIONS

| Challenge Question | Node | Edge | Pseudo-edge |
|---|---|---|---|
| What is the name of the person presented in <photo>? | ✓ | | |
| What is the birthday of the person presented in <photo>? | ✓ | | |
| What is the level of education of <person>? | ✓ | | |
| With whom did you exchange <message>? | | ✓ | |
| Who published this <photo>? | ✓ | | |
| Who liked this <post>? | | ✓ | |
| Who commented on this <post>? | | ✓ | |
| Select the ones who retweeted this <post>. | | ✓ | |
| Who were with you in <school>? | | | ✓ |
| Select the ones who attended this <seminar>with you. | | | ✓ |
| Where did <person >born? | ✓ | | |
| Select the ones who favorited your last tweet. | | ✓ | |
| Select three users who subscribed in <YouTube channel>. | | ✓ | |
| Who sent this private <message>? | | ✓ | |
| Select four friends who shared <post>. | | ✓ | |
| Choose the person who created <Facebook group>. | ✓ | | |
| Select four of your friends who participated in <Twitter hashtag>. | | ✓ | |

In [15], Jain et al. proposed a social authentication scheme that basically relies on selecting a *node*, an *edge*, or a *pseudo-edge* challenge question from a database that was specifically designed for this purpose (see Fig. 4 for an example of an *edge* question) [15]. For extracting *node*- and *edge*-related information, Jain et al. took advantage of the Facebook Graph API [44] to represent Facebook social graphs and thus enable eliciting the most appropriate knowledge items that can be leveraged to design challenge questions.

*2) **Trust-Based Techniques**:* Techniques that leverage trust as an authentication factor have recently received considerable attention from researchers and mobile application developers. For instance, as an attempt to replace passwords, Google has recently announced the so-called Trust API, which determines the level of authenticity according to trust scores calculated based on several factors related to user activities and usage patterns [45]. In user authentication schemes, the responsibility of authenticating humans can be delegated to an email provider, a phone device, or a trusted person [19]. In this paper, social authentication schemes that involve users' trusted friends for identity verification purposes and require the collection of vouch codes from previously appointed persons are referred to as *trustee-based social authentication techniques*. As some user authentication schemes may also follow specific procedures for evaluating the level of trustworthiness of user interactions inferred from users' physical or online social contexts without requiring explicit intermediation of trustees or vouchers, we categorize these types of authentication factors as *implicit vouching-based social authentication techniques*.

**2.1 Explicit Vouching-Based Techniques.** Social authentication techniques that require users to explicitly initiate a certain form of social interaction with other users in order to obtain their assistance in gaining access to computing systems are considered *explicit vouching-based techniques*. This type of authentication can be accomplished by either requiring the users to collect vouch codes sent to their previously appointed trusted friends or defining other procedures that allow friends to help confirm users' identities, for example, by establishing video or voice chats between the user and some persons he/she knows.

**2.1.1 Trustee-Based Social Authentication.** Trustee-based authentication has most frequently been utilized as a secondary authentication scheme in which users use vouch codes collected from their trustees to recover their locked accounts. It is also sometimes used in combination with other authentication factors, such as biometrics or PINs, to achieve higher security levels [14], [26]. In trustee-based social authentication, also considered explicit vouching-based authentication [26], a user is authenticated with the help of a person whom he/she trusts. Therefore, when *Someone You Know* is introduced as an authentication factor, people can vouch for the authenticity of each other [18], [46], [47]. In general, the vouching process in a social authentication system requires a user to register a number of trusted people as authentication contacts whenever he/she wants to regain access to his/her account. However, trustee-based social authentication systems vary in the way in which they set up, send, and collect trustees verification codes. Furthermore, some techniques give the user the option to choose his/her trustees, whereas other schemes follow specific procedures to implicitly infer users' trust relationships in online communities [18], [14], [48], [49], [50].

As a pre-requisite for trustee-based social authentication, trusted friends should already have been enrolled or registered in the authentication system [51]. Trustee-based social authentication systems should also maintain a list of users who are allowed to authenticate or vouch for each user [26]. Further, users who vouch for the identities of other users should already have been authenticated to use the services offered by the target system. The deployment of vouching systems in enterprise contexts also sometimes requires the registration of the names and contact information of all workers as a prerequisite for the vouching process [12], [18].

The idea behind authenticating individuals with the help of other persons is not new; for example, system administrators sometimes issue temporary passwords to users who have forgotten their passwords [12], [18]. Brainard et al. proposed the first system that introduced human intermediation into user authentication processes [18]. The vouching system they developed helps users to recover their tokens in a two-factor authentication system (see Fig. 5). Basically, their trustee-based authentication system allows people who know their PINs but lost their SecurID tokens to be authenticated with the assistance of other persons who are able to issue temporary passwords using their SecurID hardware authentication tokens [18] (see Fig. 5).

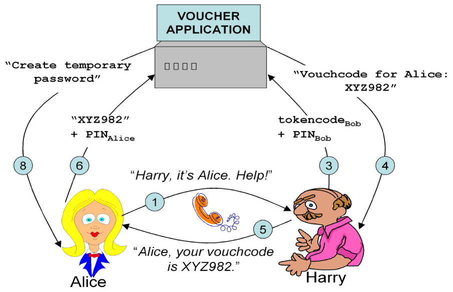
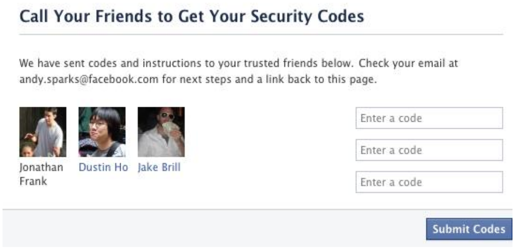

VOUCHER APPLICATION
"Create temporary password"
"Vouchcode for Alice: XYZ982"
"XYZ982" + PIN$_{Alice}$
tokencode$_{Bob}$ + PIN$_{Bob}$
8
6
3
4
"Harry, it's Alice. Help!"
1
5
"Alice, your vouchcode is XYZ982."
Alice
Harry

Fig. 5. A vouching process employed in a social authentication system [18]

Similarly to the system developed in [18], Schechter et al. employed trustee-based authentication as an account recovery scheme [12], [52]. Their scheme was deployed on top of Windows Live ID and depends mainly on using previously supplied names and email addresses of trustees for verifying users identities and issuing account-recovery codes accordingly [12]. Whenever a vouch code is issued for the first time, the scheme notifies all trusted friends of a user that an account recovery process has just been initiated [12]. When an account holder logs in for the first time after issuing a vouch code with the help of any trustee, he/she also receives a notification message saying that his/her account is being recovered. The reason for sending these notification messages is to encourage the remaining trustees to respond to corresponding vouching requests and at same time to give account holders a chance to protect their accounts before allowing attackers to collect the remaining vouching codes and gain unauthorized access to the account being recovered [12].

As a large-scale deployment of vouching-based authentication in online social networks, Facebook released a service that allows users to recover their locked accounts by entering security codes collected from their trusted friends [53]. *Facebook's Trusted Friends* service requires the users to collect vouch codes sent to three persons who were previously selected as trusted friends (see Fig. 6). In the second quarter of 2013, Facebook made some improvements to the *Trusted Friends* feature and renamed it *Trusted Contacts* [37] (see Fig. 7). In particular, the management of trustees has become more flexible and users are now able to choose, edit, and manage their trusted friends by accessing the security settings of their profile pages.

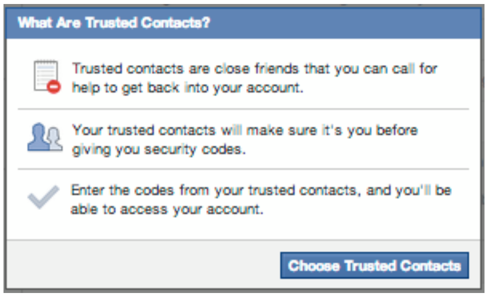
Some researchers have argued that trustee-based social authentication could be a more reliable backup authentication option, as the complexity of analyzing social knowledge is lower than that of analyzing knowledge-based social authentication [18], [12]. Another justification for this argument is the difficulty of identifying whether a correct answer to a



Call Your Friends to Get Your Security Codes

We have sent codes and instructions to your trusted friends below. Check your email at andy.sparks@facebook.com for next steps and a link back to this page.

Fig. 6. Password Recovery in Facebook's Trusted Friends Feature [53]



What Are Trusted Contacts?

Trusted contacts are close friends that you can call for help to get back into your account.

Your trusted contacts will make sure it's you before giving you security codes.

Enter the codes from your trusted contacts, and you'll be able to access your account.

Fig. 7. Password Recovery in Facebook's Trusted Contacts Feature [37]

challenge question presented by a knowledge-based scheme was originally provided by the real owner of a given user account or by a user with a malicious intent [51]. However, we note that passing the responsibility of authentication to humans decreases the automation level of user authentication and introduces further complications related to measuring the level of trustworthiness of social relationships and reflecting them in the corresponding authentication scheme.

**2.1.2 Context-Aware Social Authentication.** Some context-aware approaches have taken advantage of the data that can be extracted from users' social communications and interactions in offline contexts for understanding the inherent trust relationships and using them for authenticating purposes [54], [55]. Because these authentication approaches utilize physical trust relationships without requiring the user to recognize or recall any form of social knowledge, we treat them as trust-based authentication schemes. We also consider them explicit vouching-based schemes, because users are asked to explicitly initiate a form of social interaction to allow the authentication processes to start. While these approaches may be effectively deployed in physical contexts, their deployment for authenticating people in online communities may not always be applicable.

In studies in the psychology literature, it has been proven that people can associate familiar faces with the identities of persons automatically and without requiring attentional or cognitive resources [56]. Building on this fact, the authors of [54] exploited physical trust relationships that are inferred from visual contact between people to build a persistent authentication system. Their proposed authentication approach, when applied in a specific physical context, sends notification messages to all trusted users who exist in the same context once a new person arrives; users then assume the responsibility for checking the authenticity of new comers through visual contact and reporting any suspicious person.

A similar context-aware authentication system utilizing *face-to-face* communications between people was proposed in [55]. The socially aware system presented in [55] determines the level of authentication of each user based on the results reported by two sub systems, i-Contact and k-Contact [55]. The role played by the first sub system is to ask users to confirm the identities of their neighbors who exist in their physical contexts, based on their visual contacts, and pass this contextual information to k-Contact, which determines the authenticity level of the users; for example, a user is given more resource access rights as the number of eyewitness reports collected from other users increases [55], [57]. The main drawback of the context-aware mechanisms proposed in [55], [54] is their reliance on data reported by humans, which may not necessarily and accurately reflect the authenticity of the users. From usability and security perspectives, further experimental results are required for evaluating the applicability of implementing these approaches in different physical contexts.

The degree of authenticity of users can also be more accurately determined by combining data collected from users' online and offline social contexts with other types of data, for example, biometric data [58], [59], [60]. The sophisticated communication, sensing, and networking capabilities of smartphones could also play a significant role in facilitating the continuous inference of social data from physical contexts [61], [62], [63], [64], [65]. Significant improvements in social authentication schemes could also be achieved by leveraging the capabilities of wireless communication technologies, which would allow the extraction of more meaningful information about users' movements and social interactions in their physical contexts, i.e., tracking gestures and motions using wearable sensors [60], [66]. The integration of social data inferred from users' physical environments with knowledge about their activities on social networking sites would therefore help achieve more accurate monitoring of users' behaviors and identification of their unique social features. As mobile computing and communication technologies allow users to be continuously connected with members of their social communities, we also expect combining social data from users' physical and online contexts to facilitate the development of accurate user profiles that could be utilized to improve identify verification processes in existing continuous user authentication schemes [67].

**2.1.3 Video-Based Social Authentication.** In previous research studies, attempts have been made to leverage social relationships for addressing specific problems or vulnerabilities that might be otherwise exploited by malicious individuals [68], [69], [13]. For mitigating the effects of phone thefts, Libonati et al. designed a system based on the fact that individuals can easily recognize and verify the identities of familiar people by looking at their faces [70], [71]. The system utilizes interactive video chatting to prevent attackers from accessing the credentials stored in a stolen or lost phone [68]. The approach presented in [68], called *video notarization*, utilizes users' social networks to verify that a phone device is physically being held by its real owner. As shown in Fig. 8,

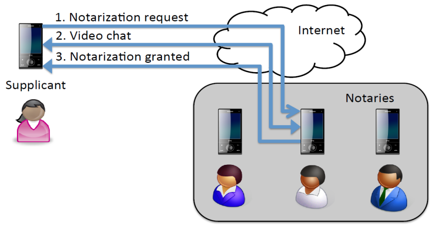


Fig. 8. Video Notarization Process [68]

a user is granted access to his/her device when a person who exists in his/her social network, referred to as *notary*, confirms the identity of the user after recognizing him/her in a video chat.

For the purpose of granting or denying access to secured computing resources, the social authentication system built in the study reported in [6] also relies on establishing video connections between users who would like to access a specific resource and the members of their social circles who have already gained access to the same resource. Thus, by establishing live video data feeds between these different parties, a user can be given the authorization to access the requested resource by any of his/her friends whose identity has already been verified.

**2.2 Implicit Vouching-Based Techniques.** While most currently deployed vouching-based authentication systems require users to explicitly initiate the vouching process and ask for the help of their friends, a few research studies have attempted to leverage social connections extracted from OSNs to implicitly authenticate users [49]. The methods in these studies either utilized implicit vouching to authenticate users on OSNs or leveraged data about users' social relationships extracted from OSNs to enable implicit authentication or authorization in networked environments.

**2.2.1 Implicit Vouching in Online Communities.** Some researchers have directed their efforts toward analyzing the structural properties of social graphs in OSNs for the purpose of uniquely identifying users based on features extracted from their social activities and interactions. Xie et al. proposed a vouching-based authentication system called *Souche*, based on traversing social graphs generated from OSNs, that examines the trust relationships previously established in these communities to determine whether a user who recently joined an online community is legitimate or not [49]. In *Souche*, once a person's identity has been verified in the corresponding social graph, this vouchee can verify the identities of other users and become a voucher [49] (see Fig. 9). The underlying algorithm of *Souche* that was employed for implicitly controlling the vouching process determines whether one user is allowed to vouch for another one by representing the vouching relationships in tree structures and performing global and local quota searches [49]. For example, in Fig. 10, each node has a quota value and the decision whether A is allowed to vouch for the identity of B is based on the value of A's quota as well as on the quotas of all the nodes rooted at F. *Souche* was deployed on Hotmail and its implicit vouching process was based on email communications [49]. However, the underlying vouching process of *Souche* can be replicated for implicitly authenticating people in other OSNs [49].

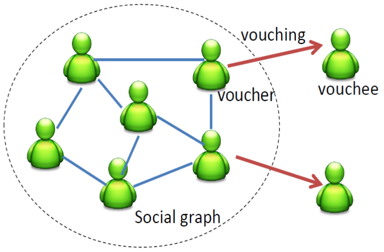


Fig. 9. Vouching in Social Groups [49]

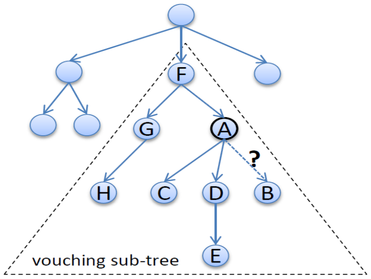


Fig. 10. A Vouching Tree of An Online Social Group [49]

For the purpose of minimizing the number of fake identities that resemble the appearance of real well-known identities in OSNs, Rubinstein et al. proposed another implicit trust-based authentication scheme that determines the trustworthiness of a user account by utilizing a number of metrics to assign a confidence score to each user in an online community based on the quality of his/her social connections [3]. Consequently, as the confidence score of the user increases, he/she is more probably the person he/she is claiming to be. Similarly, for the purpose of developing a socially aware public key infrastructure authentication system, after asking a number of the user's friends to sign a user's digital certificate, the approach proposed in [4] computes a trust score for each user after measuring the quality of trust relationships between the user and each of his/her signers. For approving the identities of users who have recently joined an online social community, it has also been suggested that their trust level should be measured based on properties of their social interactions with trusted users on the same online platform, for example, receiving a private message or a friend request from a trusted user [72].

To defend against identity theft attacks in OSNs [73], Li et al. built a social authentication system that identifies the social power areas of each user and asks him/her to obtain certificates from other users who exist in these areas so that he/she can be authenticated [69]. While this approach does not require that any form of secret information, such as vouch codes, temporary passwords, or tokens, be shared between the authenticator and the authenticatee, the collection of a certificate issued by a person who is commonly trusted by both is a prerequisite of the authentication process.

As other research studies exist in which features extracted from users' behavioral patterns on the Web were successfully leveraged for authentication purposes [74], [75], we note that the availability of data related to users' interactions and browsing behaviors on OSNs can facilitate the design of more effective implicit vouching-based social authentication schemes. For instance, a system that correlates the characteristics of users social interactions on OSNs with their navigation patterns on the Web could facilitate the extraction of unique features about users communications with their friends in online communities. Using existing approaches for identifying the most active and influential members with whom an account owner is most likely to communicate on the corresponding online community (e.g., [76], [77]) could also facilitate the process of accurately identifying trusted users who could serve as vouchers.

A combination of data about users' Web browsing histories and data that can be collected from users' mobile phones, such as calling patterns, sensor data, and e-mails, would also help achieve a more accurate characterization and prediction of users' social interaction patterns and their relationships with others [78], [75]. For instance, researchers demonstrated their ability to construct 95% of friendship graphs using behavioral data collected from mobile phones [78]. More importantly, the use of a combination of social data and behavioral data extracted from different sources, such as Web browsing patterns, mobile data, demographic characteristics, and spatial and temporal communication patterns, is expected to facilitate the construction of better continuous authentication schemes [75]. Fortunately, the availability of multiple interaction analysis tools and approaches that could assist in identifying trustworthy social interactions in online communities, analyzing social graph structures, and gaining better insights about the rates of information diffusion on OSNs is expected to help researchers move forward toward designing systems that continuously verify users' identities using data extracted from their online or offline social contexts.

**2.2.2 Implicit Vouching in Networked Environments.** For the purpose of enabling people to access Wi-Fi networks using their social relationships, referred to as *social Wi-Fi access points*, Durmus et al. proposed a decentralized authentication approach that allows home owners to restrict the access to their Wi-Fi networks by authenticating only trusted friends [79]. Similarly, the authentication approaches patented in [5], [80] examine the nature of social connections that exist between users in OSNs in order to decide whether to authorize a user to access a wireless access point owned by another user and to determine the level of access that should be granted.

Some previously proposed authentication systems that employ social trust were intended primarily to help people regain access to systems deployed in the organizations or enterprises in which they are working [18], [55]. In the study in [81], for instance, social trust relationships in OSNs were leveraged for implicitly deciding whether to enable a person to access a device or a resource owned by another person. In the study in [82], the authors also leveraged the degree of separation between individuals in social networks to allow a user to define people who are allowed to access his/her resources in networked environments; for example, a user can define an access rule that prevents indirect friends from establishing communications with his/her device. While these proposals may be effective for enterprise use, the possibility of exploiting the large volumes of data uploaded to online social networking sites and taking advantage of trust relationships that can be inferred from online communities has gained insufficient attention in the literature related to human authentication [14].

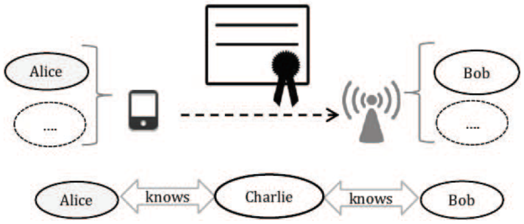


Fig. 11. Identifying Indirect Friend Relationships using FOAF [79]

As emphasized in [83], [79], [84], [85], users' interactions in OSNs can be leveraged for extracting meaningful knowledge about the trustworthiness of social relationships, which can be used for automating human and device authentication processes. To meet the interoperability challenges that may arise in any attempt to infer social relationships from OSNs and integrate authenticated devices into this process, the WebID [86] protocol was utilized to build the socially aware authentication mechanism proposed in [79]. According to [79], a trust relationship between two persons can be inferred either directly or indirectly. As shown in Fig. 11 and using the Friend-of-a-Friend (FOAF) vocabulary [87], a friend relationship between Alice and Bob can be indirectly inferred if there is friend who is trusted by both [79].

In a number of socially aware systems that authenticate people based on their trust relationships, public or private key cryptographic systems were employed for different purposes [69], [68]. While these cryptographic systems were used to protect communications in socially aware systems employed in either enterprises or OSNs, a security issue associated with the use of public or private keys was raised in [14]. The threat scenario described in [14] shows that these keys can be easily copied from one device to another if there is no mechanism in place that restricts access to them when the devices are in the possession of unauthorized persons [14]. Another challenge associated with employing these cryptographic systems in OSNs is related to obtaining the keys of unknown users and ensuring that they are associated with the real owners of the corresponding user accounts in OSNs [69].

The explosive volumes of social data that could be extracted from various users' networking and communication channels could lead social authentication schemes to a fundamentally promising direction. A number of researchers have recently discussed the possibility of extracting social graph structures from data exchanged in communication networks and leveraging the knowledge inferred from the extracted social data for designing socially aware communication techniques [88], [89], [90], [91], [92], [93]. In the study reported in [89], for instance, the authors demonstrated their ability to discover the friends who are most likely to communicate with a given user in instant messaging networks only by analyzing the properties of exchanged packets. A comprehensive discussion on leveraging the characteristics of social ties for the purpose of designing effective routing protocols was also presented in [93], [94]. Thus, combined knowledge about the frequency of communication between users, their geographical locations, and the number of communicated messages over different time periods could indicate the most important social relationships that can be utilized for authentication purposes [89]. The visualization and analysis of social communication patterns between devices in networked environments is therefore expected to help identify the nodes in social graphs that can best be used in implicit vouching processes [90].

As there are millions of users who are connected to cellular networks [88], the analysis of human interactions over these networks could also be a powerful tool for continuously monitoring users' behaviors and eliciting the social features that could help in identity verification. Naboulsi et al. discussed the manner in which the analysis of mobile network datasets can assist in identifying users' friendship networks and understanding the nature of users' social activities and interactions [88]. Large-scale and complex analyses of data exchanged between mobile devices are therefore expected to help reveal high levels of detail about the degrees of trustworthiness of users' social relationships. The correlation of the knowledge inferred from these analyses with demographic elements could also allow social features to be elicited that would help characterize users' permanent and temporary social relationships [88]. Mobile network datasets could also be valuable assets for investigating the dynamic features of users' social interactions, as they could allow the analysis of users' social activities over different time spans. It is also expected that an understanding and comparison of users' communication patterns in cellular networks will help obtain more accurate knowledge about the size and organization of users' social groups. This knowledge could facilitate the processes involved in implicitly distinguishing between users' positive and negative social relationships. This would also facilitate a more accurate characterization of users' stable and dynamic social relationships. The inferred social knowledge could therefore lead to achieving a more accurate identification and characterization of trusted entities that can be leveraged in social authentication schemes.

## III. Social Authentication Properties: Comparative Analysis

To explain the properties and features of each social authentication scheme, we present a comparative analysis of all the social authentication mechanisms that have been developed or proposed. We first compare the knowledge-based social authentication techniques that are discussed in Section II-B1 in terms of a criterion for analyzing their authentication-related features. Then, we present all the trust-based approaches and investigate their authentication effectiveness by comparing their vouching-related characteristics. Most of the patented research studies included in our review (see Section II-B) are not included in this analysis and the comparative evaluation presented in Section VI, as they lack most of the details required for analyzing and evaluating their authentication features, for example, the number of challenge questions, recovery thresholds, and number of answer options.

### *A. Knowledge-Based Techniques*

The five main knowledge-based social authentication techniques proposed in the literature are listed in Table III in chronological order from the oldest proposed scheme to the most recently developed one [27], [30], [31], [33], [15]. As shown in Table III, 80% of these schemes were either deployed on top of Facebook or used datasets containing photos collected from Facebook.

**Analysis Criteria.** For each scheme, we examine the type of social knowledge that is utilized to privately authenticate individuals and associate it with its deployment context. Our evaluation is also aimed at understanding the types of socially aware techniques that have been utilized as primary authentication factors and those that have been used as emergency, backup, or fallback authentication schemes. Further, to assess the usability of each scheme (see Section VI) and since knowledge-based authentication schemes require users to either recognize or recall certain information in order to answer challenge questions, we identify the social knowledge item that needs to be recognized or recalled in each evaluated scheme (see the comparison elements presented in Table III and Table IV).

*1) Type of social knowledge:* We note that the five knowledge-based social authentication techniques differ in the purpose and objectives that motivated the researchers to propose them. While the purpose of Facebook's released knowledge-based social authentication scheme is the verification of users' identities whenever an abnormal or suspicious activity is discovered [31], [15], [33], the remaining schemes were proposed either to improve the security of Facebook's knowledge-based social authentication or to examine the feasibility of utilizing specific social knowledge items for authenticating individuals in online or physical social contexts. For instance, Facebook's photo-based socially aware scheme presents its security questions if it detects two log-in attempts originating from locations at a considerable distance from each other within a short time period [31]. Furthermore, Lineup [27] was intended to ensure that users attempting to gain access to specific Facebook groups are members in these groups by assuming that, if a Facebook user is authorized to access a social group, he/she should know the other members of that group and be able to solve photo-based challenge questions accordingly [27], [15].

A more generalized knowledge-based authentication approach was followed for designing the challenge questions presented by *Soc-Auth* [15]. Similarly to the knowledge-based social authentication approaches presented in [27], [31], [33], *Soc-Auth* [15] presents the user with information relating to persons he/she knows and asks him/her to name the associated human subjects. However, in comparison with Facebook's photo-based social authentication [31], *Soc-Auth* security questions may be based on the attributes related to a person, his/her connections with other friends, or information that is

TABLE III
COMPARATIVE ANALYSIS OF KNOWLEDGE-BASED SOCIAL AUTHENTICATION SCHEMES

| **Social authentication technique** | **Ref.** | **Type of Social knowledge** | **Deployment Context** | **Primary/Secondary Authentication Factor** | **Other Authentication Factors** | **Recognition/ recall based technique** |
|---|---|---|---|---|---|---|
| Lineup | [27] | Photos | Facebook | Primary | None | Recognition of faces and recall of some information relating to photos posted in users' social circles (e.g., place where a photo was taken, time of an event, event description, names of other members who appear in a photo and information relating to objects presented in posted photos). |
| Social authentication devices | [30] | Contextual information gathered from users physical social context | Physical context | Primary | None | None |
| Facebooks photo-based social authentication | [31] | Photos | Facebook | Secondary | Passwords | Recognition of faces. |
| Photo-based SA authentication based on photo-selection and transformation processes | [33] | Photos | Facebook | Secondary | Passwords | Recognition of friends in transformed photos. |
| Soc-Auth: Social Authentication Framework Based on a Categorization of Social Knowledge in OSNs | [15] | Node attributes, edge attributes and pseudo edge attributes | Facebook | Secondary | Passwords | Recognition of friends faces and recall of information relating to node, edge or pseudo-edge attributes. |

known by both a user and one of his/her friends in a given social graph. Therefore, instead of asking the user only to recognize the faces of his/her friends in a set of photos, the *Soc-Auth* approach of authentication leverages other types of social knowledge for privately authenticating the users.

In contrast to the knowledge-based socially aware schemes proposed in [31], [15], [27], [33], which are deployed in online contexts, the socially aware knowledge-based authentication scheme presented in [30] was primarily motivated by the possibility of leveraging social knowledge extracted from users' physical social contexts. Another factor that differentiates Dathan et al.'s scheme from the remaining knowledge-based approaches is that it is capable of automatically identifying suspicious behaviors in physical contexts without requiring the user to explicitly provide some type of knowledge or trigger an event for initiating the authentication process [30]. For instance, in cases where the social authentication devices proposed in [30] are stolen or acquired by unauthorized individuals, if the device starts to record completely different social contexts, this should give clues that could lead to detecting the corresponding thefts.

By considering the prerequisites of deploying each of the five knowledge-based socially aware schemes listed in Table III, it can be seen that the availability of tagged photographs including faces of human subjects is the main requirement for running the photo-based social authentication schemes presented in [27], [31], [15], [33]. For gathering social information from individuals' physical contexts, however, the availability of devices equipped with Bluetooth technology is essential [30]. We note that, as compared to knowledge-based social authentication schemes, social authentication devices do not require users to provide any form of social knowledge to allow their authentication [30].

*2) Properties of challenge questions:* Through a comparison of the properties of the challenge questions asked in the four knowledge-based social authentication systems deployed in online contexts [27], [31], [33], [15], we noticed some similarities and differences in the types of presented questions, their difficulty levels, and the number of options included in the questions, as well as the number of given choices. As shown in Table IV, since the majority of these schemes were designed as improved versions of Facebook's photo-based social authentication scheme, their questions share some common properties. For instance, in the knowledge-based schemes proposed in [31], [33], [15], the number of question instances presented to the user and the number of correct answers that should be provided in order for him/her to be authenticated are seven and five, respectively. Further, for security and usability related reasons, some systems obtain the answers in keyed-in form [27], whereas others either present multiple choice questions only [31], [33] or add another level of security by asking the user to correctly choose a person who appears in a photograph first and then key in his/her name [15].

It is also worth mentioning that some of the numbers presented in Table IV are not explicitly mentioned in the corresponding research studies. Instead, we either assumed that their design decisions were similar to those of Facebook's photo-based scheme [31], in cases where the purpose of the proposed scheme is to improve Facebook's scheme, or inferred these numbers from the sample questions presented in these studies. Furthermore, the schemes listed in Table IV vary in the number of multiple choice answers for each question and the number of difficulty levels guiding the process of choosing the most appropriate question to be presented to the user, which may be based on either his/her privacy settings, number of connections in his/her social graph, or the social power associated with each node in OSNs. Additionally, because Polakis et al.'s

TABLE IV
PROPERTIES OF CHALLENGE QUESTIONS IN PHOTO-BASED SOCIAL AUTHENTICATION SCHEMES

| Social authentication technique | Ref. | # of Questions | Recovery Threshold | # of Photos in a Question | # of Difficulty Levels | # of answer choices | Correct Answer: Chosen | Correct Answer: Typed |
|---|---|---|---|---|---|---|---|---|
| Lineup | [27] | 1 | 1 | 1 | 3 | - | | ✓ |
| Facebooks photo-based social authentication | [31] | 7 | 5 | 3 | 1 | 6 | ✓ | |
| Photo-based SA authentication based on photo-selection and transformation processes | [33] | 7 | 5 | 3 | 3 | 6 | ✓ | |
| Soc-Auth: Social Authentication Framework Based on a Categorization of Social Knowledge in OSNs | [15] | 7 | 5 | 5 | 1 | 5 | ✓ | ✓ |

photo-based socially aware scheme relies mainly on applying photo-transformation processes and classifying the quality of the photos used in challenge questions as *simple*, *medium*, or *difficult*, we assume that their system has three difficulty levels, although it is not clear whether they chose one or some of these classes when implementing their authentication system [33].

Answers to security questions employed in backup or fallback authentication systems should be carefully designed such that they are easily solved by users and difficult for attackers to guess [95], [96]. By linking this fact to the properties of challenge questions presented in social authentication knowledge-based schemes (see Table IV), it can be inferred that, although requiring the user to key in the correct answer and presenting a greater number of possible answers may have positive security implications, these requirements may negatively affect the usability of the corresponding social authentication scheme. Therefore, designers of knowledge-based social authentication techniques should carefully balance their choice of the most appropriate properties that are well-aligned with the purpose of their schemes employment and the context in which their social authentication schemes would be deployed.

In many papers in the literature related to the design and evaluation of personal security questions, the security properties that should be considered have been discussed, guidelines that may contribute to increasing the robustness of these questions have been proposed, or experimental findings related to the memorability and guessability of challenge questions have been presented [96], [95], [97], [98], [99], [100], [101]. However, security questions used in knowledge-based social authentication schemes are built based on knowledge extracted from users' surrounding social contexts as compared to typical personal challenge questions, most of which are based on answers pre-provided by the user. Therefore, the security of knowledge-based social authentication schemes depends on the accuracy, uniqueness, and quality of the social knowledge utilized in the identity verification processes. Thus, issues such as the availability of publicly accessible social data and the disclosure of personally identifiable information in online social networks should also be taken into consideration in the design of security questions for knowledge-based socially aware schemes.

### B. Trust-Based Techniques

The socially aware trust-based techniques included in our evaluation are listed in Table V according to the year in which they were released or published, from the introduction of the first scheme in 2006 to a scheme that was proposed in 2014.

**Analysis Criteria.** For analyzing social authentication schemes that utilize trust relationships for verifying users' identities, we define criteria that focuses on highlighting the vouching-related features of each scheme and identifying its strengths and weaknesses. As shown in Table V, our comparative assessment is aimed at understanding whether trust-based social authentication schemes are deployed mostly in physical or online contexts. We also examine the supplementary authentication factors that are used in combination with each evaluated scheme.

In the case of the schemes that authenticate individuals mainly by following explicit vouching processes, our evaluation pays significant attention to understanding the steps that need to be performed in order for vouch codes to be issued. Because explicit vouching-based socially aware techniques involve users' trusted friends in the authentication processes [15], we also investigate the manner in which these techniques select and communicate with trustees. Our analysis also explores the properties of the issued vouch codes, such as their length, the number of vouch codes that have to be collected in order for a socially aware scheme to verify the identity of a vouchee, and the conditions under which issued code should be invalidated. In particular, we note whether issued vouch codes can be used only once or repeatedly for a specific time period. Although some studies do not explicitly mention all the information required for our evaluation, we were able to infer some of it from the identity verification features of each social authentication scheme described in the corresponding literature. As shown in Table V, nine trust-based social authentication techniques are included in our comparative analysis. Although not all of them were proposed as vouching-based social authentication schemes, we include a few techniques that exploit social trust relationships or the social context surrounding the users in identity verification [79], [55].

According to our observations, trust-based social authentication schemes were originally employed as secondary authentication factors and in physical contexts, for example, in enterprises and organizations. Furthermore, trustee-based schemes vary in the manner in which trustees are chosen. While each technique has its security strengths and weaknesses, some give the users full control over selecting their trustees, whereas

TABLE V
COMPARATIVE ANALYSIS OF TRUST-BASED SOCIAL AUTHENTICATION SCHEMES

| **Social authentication technique** | **Ref.** | **Deployment Context** | **Primary or Secondary Authentication Factor** | **Other Authentication Factors** | **Recovery Threshold** | **Vouch Code Length** | **# of Registered Trustees** | **Contacting Trustees** | **Selecting Trustees** | **One-Time or Temporary Vouch code** |
|---|---|---|---|---|---|---|---|---|---|---|
| Vouching Process Proposed by RSA Laboratories | [18] | Enterprise | Secondary | Hardware Tokens and PINs | 1 | Can be determined by system administrators | Not specified | Explicit ( in person or over phone) | Either automatically or explicitly | Temporary password after invalidating the vouch code |
| Microsoft vouching system | [12] | Windows Live | Secondary | password | 3 | 6 characters | 4 | Explicit (in person or over phone) | Explicitly selected by account owners | None |
| Mobile phone based implicit vouching based authentication | [14] | Physical context | primary | PINs (primary), biometrics (secondary) and private keys | Not specified | Not specified | No specific number | Implicit (automated), trustees are directly communicated using cellphones or Bluetooth | Explicit | Temporary token (valid for 3 days) |
| Trust-based framework for authenticating users in online communities | [69] | Online contexts | primary | None | No vouch code is issued. Certificates issued by common friends are used instead. | No vouch code is issued | No specific number | Requesting certificates from other users in OSNs. | Implicitly inferred based on the certificates collected by the users | Primary |
| Souche | [49] | Online contexts (Hotmail email service) | Secondary | No specific factor is indicated but it can be used with other factors (e.g., CAPTCHA). | No vouch code is issued | No vouch code is issued | No specific number | Trustees are not communicated | Implicitly inferred by traversing social graphs and studying the properties of social connections between users in these graphs. | None |
| Video Notarization | [68] | Physical and online contexts | Secondary | None | No vouch code is issued | No vouch code is issued | No specific number | Via Video chats | Implicitly inferred from users phone address books | None |
| Facebooks trusted contacts social authentication scheme | [37] | Facebook | Secondary | Passwords | 3 | 4 numbers | 3 to 5 | Explicit (in person or over phone) | Explicitly selected by the account owner. | One time |
| i/k-Contact | [55] | Physical context (enterprise use) | primary | Varies depending on the degree of trust of the user | No vouch code is issued | None | The more users, the better authentication level is achieved | Visual contact | None | None |
| EAP-SocTLS: Social Authentication for WiFi Networks | [79] | Physical context | primary | None (works as a substitute to passwords) | No vouch code is issued | No vouch code is issued | No trustees are registered in advance (depends on number of connections in OSNs). | Trustees are not communicated. | Implicitly inferred from social relationships in OSNs | None |

others perform certain processes in order to implicitly infer users' trusted friends. In some schemes, users are advised to explicitly contact their trustees (e.g., in person or over phone) in order to collect vouch codes that vouchers have received from a given social authentication system, whereas other schemes attempt to automate this process by either utilizing cell phone attributes (e.g., Bluetooth and cameras) or automatically inferring trust relationships without asking users to communicate with each other. The evaluated schemes also differ in the processes they follow for generating vouch codes and for verifying trustees' identities before allowing them to vouch for other persons. In the following sections, we analyze the procedures followed in the surveyed trust-based schemes for identifying trusted friends, communicating with them and issuing vouch codes.

*1) Identification and selection of trusted friends:* In some trustee-based social authentication systems, users are required to select a specific number of friends to vouch for their identities whenever they want to regain access to their accounts. For example, in order to be allowed to take advantage of Facebook's Trusted Contacts feature, users should select at least three friends to vouch for their identities [37]. Similarly, the use of the vouching-based social authentication process that was built on top of Windows Live ID required the users to submit the names and email addresses of four trusted friends before they lose access to their accounts [12]. However, in both schemes [37], [12], the number of vouch codes that must be collected from vouchers for account recovery is three.

Device owners who can take advantage of the video notarization system proposed in [68] should also identify their notaries by either using the names saved in their phones address books or manual configuration. *EAP-ScoTLS* [79] implicitly infers users' trust relationships based on the existence of social connections in online social networks. However, it should be noted that an edge linking users in an online social network may not necessarily imply the existence of a trust relationship [32], [51]. Durmus et al. suggested solving this issue by augmenting access control rules for managing the level of authentication based on the types and quality of social connections in social graphs [79]. For instance, the *k-Contact* [55] scheme determines users' authentication levels according to their degree of trust, which is inferred mainly from the number of eye witness reports obtained from people who exist in the same physical context.

Some social authentication attempts have taken advantage of the FOAF ontology to understand the direct and transitive trust relationships between people in online social networks [102], [79]. FOAF is a machine-readable vocabulary that allows the representation of social relationships between people as networks of linked documents on the Web [87]. However, we observed that these schemes rely mainly on understanding who knows whom, although knowing a friend in an online community may not necessarily mean that a trust relationship exists [79]. For example, if a user mentions another user on Twitter, the link established between the two users does not necessarily imply that either of them trusts the other.

Although most currently deployed vouching-based social authentication systems give users the freedom to choose their own trustees, people may experience problems related to remembering whom they previously appointed as trustees when they want to regain access to their accounts [8], [12]. This may be because trustee-based social authentication mechanisms are deployed most frequently as fallback authentication schemes and therefore their frequency of use is low as compared to that of their corresponding primary authentication factors. This usability issue has been considered in Facebook's Trusted Contacts feature; the users are reminded of the identities of trustees who were previously selected when they have provided one correct trustee name [8]. This feature would help address the memorability issues associated with the use of trustee-based social authentication and thus positively affect the user experience. However, from a security perspective, we believe that further constraints should be imposed before a list of the trustees of a particular user account is issued. We also argue that this feature does not equally serve all the users; for example, non-frequent Facebook users would probably be unable to name one previously appointed trustee.

While most of the surveyed trustee-based systems do not impose any constraints related to the selection of trustees, Zhenqiang et al. emphasized the importance of avoiding the selection of the same trustees by different users to prevent attackers from compromising users' accounts [8]. Yesberg et al. also noted the importance of considering issues related to the existence of social relationships between people who vouch for the same user and the maximum number of vouches that each voucher should be allowed to provide over a certain time period [26]. Clearly, restricting the selection of trustees to those who do not share social relationships with each other would significantly minimize the vulnerabilities that could be exploited by attackers to compromise the security and privacy of the users. Thus, the selection of trustees from distinct social groups would minimize the dependencies of the trustees decision as to whether to vouch for a common friend. For this reason, highly dependent social relationships between persons who were appointed as trustees for the same user would make it easier for attackers to break the corresponding authentication scheme, in particular if one trustee has social power that could affect the security behavior of the other appointed trustee.

*2) Communicating with trusted friends:* As in the trustee-based social authentication schemes proposed in [12], [18], users who take advantage of Facebook's Trusted Contacts feature should explicitly contact their trustees and ask for their help [37]. As shown in Fig. 5, in the explicit trust-based scheme proposed in [18], the user is sometimes given the choice to contact the persons previously appointed as trusted friends either by phone or through face-to-face communication. While a number of researchers argue that the communication with trustees should be in person to avoid the risks associated with receiving spoofed emails and SMS text messages [12], [18], personally contacting multiple trustees increases the effort and time required to complete the authentication processes, therefore, leading to a decrease in the efficiency of socially aware systems that condition regaining access to locked accounts on the collection of a certain number of verification codes from trusted friends.

We observe that a number of trust-based social authentication approaches rely on central servers for verifying trustees' identities, storing vouching-related information (e.g., associating users with their trusted friends), or automating the authentication process [18], [14], [13], [7]. In the physical context, as an attempt to take advantage of smartphone capabilities to automate the authentication processes (e.g., [14]), Soleymani et al. proposed a social authentication scheme that automatically issues the vouch codes required for authentication whenever a user starts communicating with his/her trustees either through placing a phone call or by establishing a Bluetooth connection [14]. Zhan et al. also presented a research attempt to automate the vouching process in which a list of trusted friends is maintained in a central repository for each user [13].

Although the social authentication mechanisms proposed in [13], [14] may reduce the burden of contacting each trustee and asking him/her to obtain a vouch code and send it back to the user, these approaches rely primarily on central servers and thus the failure of a server may prevent any user from regaining his/her access credentials. Further, while configuring a central authentication server may ensure consistency in the distribution of vouch codes or communication with trustees, the entire authentication process would clearly stop if a central server became unavailable. Therefore, system designers should take into consideration the single point of failure issues and thus either adopt decentralized approaches or incorporate appropriate backup mechanisms into vouching-based social authentication schemes.

*3) Issuing and collecting vouch codes:* When designing trustee-based authentication systems, developers should make careful decisions related to the process of issuing vouch codes, identifying their expiration periods, and the method that should be employed for encrypting these codes. Further, while trustee-based social authentication systems may either issue a one-time verification code or generate temporary vouch codes [18], [12], these systems should be designed to achieve a balance between the number of codes that should be collected from trustees, the time required to issue these codes for each trustee, and the time period that should elapse before the generated vouch codes are invalidated.
In *Facebook's Trusted Contacts* scheme, users are allowed to appoint three, four, or five users as trusted friends, although the recovery threshold of Facebook's scheme is three. Similarly, the recovery threshold of Microsoft's vouching-based authentication is three, although users are required to register four users as trustees [8], [12]. While a number of constructed trustee-based social authentication systems set the recovery threshold at three [37], [12], the results of the experiments conducted in [8] suggest that users should be asked to collect vouch codes from four trusted friends in order to align the security and the usability considerations of social authentication schemes. Gong et al. performed experiments on datasets collected from three OSNs, Twitter, Flickr, and Google+, to investigate the correlation between the propagation of forest fire attacks on these networks and the number of verification codes that a user should collect in order for his/her identity to be verified [8]. Their results showed that the percentage of compromised nodes in the corresponding social graphs would be reduced significantly by setting the recovery threshold at four instead of three [8].

In other trust-based social authentication systems, in particular those that implicitly infer trust relationships, no specific number of vouchers is indicated. However, in most of them, the more trust relationships, the better the authentication level achieved [55], [69], [68], [14]. For instance, for verifying the identities of unknown users in online contexts, according to the scheme proposed in [69], the more certificates a user collects from users in his/her social power area, the better the chance that he/she will be authenticated.

In the trustee-based schemes employed in enterprise contexts, when a person has initiated the vouching process by asking for a trustee's help, the trusted person is usually supposed to forward the received vouching request to the organization for which both persons work. When the identity of the trusted person has been verified, vouch codes are sometimes generated after cryptographic mechanisms have been applied. The generated vouch codes sometimes can be used only temporarily by users who have lost their primary authentication factors and expire after a specified time period, for example 24 hours [18]. For designing the automated social authentication scheme presented in [14], researchers analyzed phone call histories to determine the minimum phone call duration that should elapse before vouch codes are automatically issued. Bluetooth technology has also been utilized to search for friends' devices that exist in the same physical context to allow users and their trustees to exchange vouch codes [14]. However, the number of trusted friends who should be contacted in advance of using the scheme proposed in [14] and the recovery threshold are unclear.

## IV. Threats and Attacks

The security issues that exist in social authentication schemes are linked to the properties of social knowledge employed in these schemes, the level of privacy each user can assure within his/her social circle, and the degree of trustworthiness of each individual involved in the corresponding authentication processes [33], [8], [12], [36]. It is assumed that these schemes, if deployed as secondary authentication factors, are more difficult to compromise than their corresponding primary authentication factors [36]. Because Facebook's social authentication schemes constitute the most popular techniques that employ social knowledge or trust relationships for verifying users' identities [31], [37], a number of researchers have examined the resilience of these schemes to several security attacks.

While the utilization of social knowledge and the involvement of friends in the human authentication process may increase the convenience of the users and streamline the recovery of lost user accounts, the security of users who use social authentication schemes is correlated with the security of persons who exist in their social groups. For instance, even if a user sets his/her user account in an OSN as private, adversaries may take advantage of less secure accounts that exist in the user's friend list to access social knowledge published within the user's private social circle. This in turn would help attackers understand the social context of the user and thus increase the probability that they can break the corresponding social authentication scheme, for example, guess answers of challenge questions or gain access to accounts owned by trusted friends.

A number of automated attacks against knowledge-based schemes, that rely primarily on advanced algorithms and sophisticated mechanisms for collecting social data from users online or physical social contexts and answering challenge questions accordingly, have been demonstrated in studies in the literature. Fig. 12 shows an example of a process that could be followed by malicious individuals for breaking photo-based social authentication schemes. Several papers have also discussed how, in trustee-based mechanisms, if one user account in an online social community is compromised, harm may be propagated to other users who are socially connected to that account. In the following sections, we discuss various attack classes associated with the deployment of social authentication techniques.

### *A. Statistical Guessing Attacks*

The reliance on shared secrets, such as passwords and the answers to challenge questions, for verifying users identities in human-computer authentication systems, which may be used either as primary or secondary authentication factors, triggers a need for increasing the difficulty of guessing these secrets. In the context of passwords or personal knowledge challenge questions, a number of researchers have addressed the robustness of authentication secrets against statistical guessing attacks [96], [103], [38], [98], [104], [105]. Some studies have either proposed solutions to increase the difficulty of guessing by, for example, preventing users from choosing common passwords [104], or have quantitatively evaluated attackers' ability to guess answers of personal knowledge questions [103]. It has also been proven that publicly accessible information that can be obtained from online social networking sites or inferred from users' demographics, languages, or cultural values are useful for statistical guessing attackers [16], [106], [95], [107].

In online contexts, users' published content and interactions with others may increase the probability of an attacker guessing answers to challenge questions that ask about social knowledge items known to the users. For instance, users' profile photos, comments, and biographies may help close enemies to guess answers to security questions. As users are asked to recognize their friends in Facebook's photo-based social authentication technique [31], attackers may be able to infer these names from the supplied tagging information or correlate the photos properties with users' interactions [16]. The impact of this risk may increase in cases where users' accounts are not protected or when friend requests are accepted by a user without the user knowing their associated real identities. Therefore, it is necessary to reduce the probability that an attacker can guess the answers to challenge questions in knowledge-based social authentication systems.

### *B. Automatic Face Recognition Attacks*

In the case of photo-based social authentication schemes that base the design of challenge questions on the identification of users' faces in selected images, attackers may take advantage of users' publicly available photos to train a variety of face recognition algorithms [16], [108], [15], [109]. Previous studies have demonstrated the effectiveness of applying machine learning techniques to recognize faces in tagged photos [110], [17]. Given that Facebook is the largest photo-sharing online platform and since the friends lists of at least 47% of the Facebook population remain unprotected by default [111], [110], it was proved that 84% of Facebook users are vulnerable to automatic face recognition attacks [17]. In the study reported in [112], by utilizing only Facebook's publicly accessible photos, the authors were efficiently able to break 22% of Facebook's photo-based challenge questions. They also claimed that the success rate of their attack would reach 100% when they gained access to private photos published by their victims [112].

In the case of private Facebook accounts, researchers have also demonstrated their ability to recognize the faces of 38% of the owners of these accounts by using only the photos that they were tagged in by their friends whose user accounts are publicly accessible. Further, the results of Dantone et al.'s study show that the use of information extracted from users' social contexts significantly increased the accuracy of face recognition schemes and helped them achieve a true positive rate of at least 79% [110]. Becker et al. utilized four machine learning schemes to recognize faces in a large dataset of Facebook images and found that a detection accuracy of 65% was achieved using the support vector machine (SVM) approach [108]. The results presented in [17] also show that at least one person can be automatically recognized in 80% of the images used in Facebook's knowledge-based authentication scheme [31].

Polakis et al. performed a large-scale experiment on Facebook and found that 42% of users' social knowledge used to formulate Facebook's photo-based challenge questions is accessible to adversaries [17]. A significant increase in the percentage of users' sensitive information that can be accessed by malicious users may occur when the users befriend each other [17], [73], [113]. Even when a user account is set such that it is protected, the public search listings that are presented whenever the account's username is used to query a search engine could be misused for inferring some properties about users' social graphs (e.g., friend lists) [106], [114], [115].

Jin et al. also showed that using the mutual friends features provided by most OSNs may help an attacker discover at least 60% of his/her victims' social connections [115]. When these connections become accessible to adversaries, more information about the targeted user can be easily extracted from the publicly accessible information published by members within his/her social circle; for example, they can infer the interests of a user using the properties of the nodes to which he/she has connected [116]. For instance, the results presented in [112] show that there is at least one unprotected photo album in over 70% of Facebook user accounts. Therefore, it is not easy to protect users' graph structures in online communities and they can be extracted from their friends' publicly accessible social information as well [117], [114].

### *C. Image-Comparison Attacks*

Image comparison techniques were proved to be more effective than face recognition algorithms for solving photo-based challenge questions [33]. In order for these attacks to be successful, attackers should collect photos that are publicly available in their victims' social networks and apply image comparison techniques to recognize subjects who appear in their collections [33], [15]. Using the collected photos and their supplied tagging information, an adversary could use photo matching algorithms to identify the subjects' faces presented in security questions [33]. Polakis et al. demonstrated

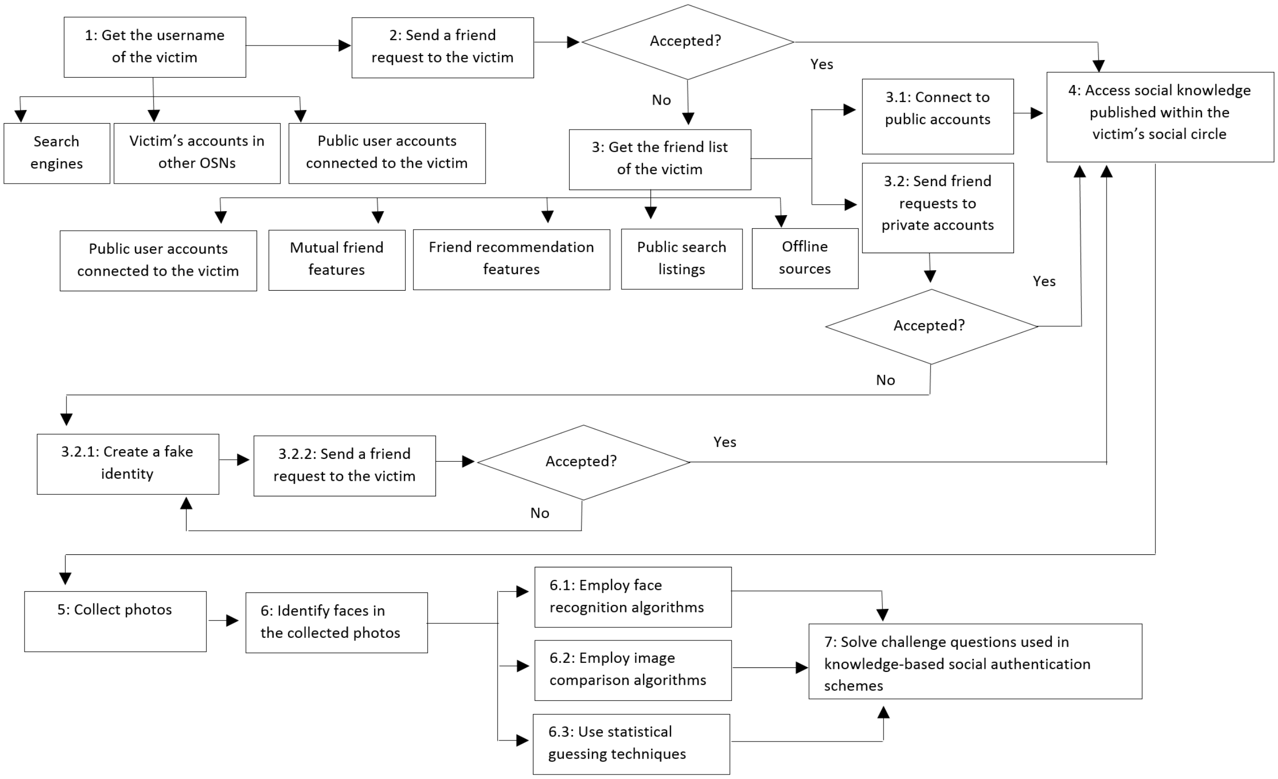

1: Get the username of the victim
2: Send a friend request to the victim
Accepted?
Yes
No
Search engines
Victim's accounts in other OSNs
Public user accounts connected to the victim
3: Get the friend list of the victim
3.1: Connect to public accounts
3.2: Send friend requests to private accounts
4: Access social knowledge published within the victim's social circle
Public user accounts connected to the victim
Mutual friend features
Friend recommendation features
Public search listings
Offline sources
Yes
Accepted?
No
3.2.1: Create a fake identity
3.2.2: Send a friend request to the victim
Accepted?
Yes
No
5: Collect photos
6: Identify faces in the collected photos
6.1: Employ face recognition algorithms
6.2: Employ image comparison algorithms
6.3: Use statistical guessing techniques
7: Solve challenge questions used in knowledge-based social authentication schemes

Fig. 12. Breaking the Security of Knowledge-Based Social Authentication Schemes

the detection accuracy of these algorithms by showing that at least 98% of the photos used in the challenge questions included in their dataset were recognized by their image comparison approach [33]. Polakis et al. also claimed that the efficiency of their approach would increase when the names presented by challenge questions were combined with photos' supplied tagging information to eliminate some of the answers after each successful photo identification [33]. However, the success of image comparison attacks is correlated with the coverage of collected images, as well as with the quality of the supplied tag information. Therefore, the more photos an attacker collects from a victim's social contexts, the better his/her chance that executing a photo matching attack will lead to successfully identifying subjects in corresponding challenge questions [118].

### D. Insider Attacks

As social authentication systems either involve trusted relationships in the authentication process or use users' published social knowledge for formulating challenge questions, the impossibility of controlling information sharing with members who exist within a user's social circle may pose certain security risks [16], [119]. As opposed to external attackers, who may have to invest more time and effort to enter into a victim's social circle and access his/her protected information, insiders who already exist in victims' social graphs have access to most of the resources required to harm them [9], [120], [121]. The problem of sharing information with an unintended audience has been examined in studies in the literature [119], [122], [123], [124], [125]. Johnson et al. investigated the privacy concerns of more than 250 Facebook users and found that at least 94% of the surveyed individuals indicated that they use Facebook's privacy controls to prevent outsiders from obtaining access to the content posted in their social networks [119]. However, 37% stated that the current privacy settings do not allow them to mitigate the threats coming from insiders, such as friends and family members. For example, to break Facebook's photo-based social authentication scheme [31], a friend can access the photos, tagging information, and social interactions of his/her victim and use these resources to identify subjects who appear in the photos presented in challenge questions. Thus, online social networking platforms should add privacy control features that allow users to flexibly restrict insiders from accessing their shared contents.

### E. Forest-Fire Attacks

The forest fire attack was proved to be effective for breaking the security of trustee-based social authentication mechanisms by means of attacking users' trustees [8]. The basic idea behind forest fire attacks is to correlate users' security with the security level of their vouchers [8]. In forest fire attacks, an attacker attempts to compromise his/her victim's trustees, referred to as *seed users*, and collect the vouch codes they receive in order to gain access to his/her victim's account. As demonstrated in [8], the ignition phase of forest fire attacks involves gaining access to the accounts owned by seed users through launching any form of security attack, for example, by means of statistical guessing. After the seed users have been compromised, the propagation phase involves launching an account recovery request using a victim's username. This enables attackers to use verification codes sent to compromised seed users to launch iterative recovery requests and compromise thousands of users. Although knowledge of the victims' previously appointed trustees is a precondition for launching successful forest fire attacks, previous studies have shown that attackers can easily access users' friends lists and guess the names of users' vouchers [8], [18]. For instance, Facebook users need to correctly guess a name of only one trusted friend in order to be presented with the names of other appointed trustees [8].

### F. Identity Impersonation Attacks

To maintain the credibility and trustworthiness of social authentication schemes, it is necessary to ensure that the formulation of the challenge questions and the process of appointing trustees exclude suspicious user accounts. It is also essential to detect fake identities as early as possible and before they develop social connections with their victims' friends [126]. It is also important to verify the authenticity and legitimacy of social interactions and ensure that the properties of real-life social networks are accurately reflected in the corresponding social authentication scheme.

Javed et al. introduced the *Trusted Friend Attack* and demonstrated the manner in which attackers may gain access to users' accounts when their victims accept fake friend requests [36]. Taking advantage of the lack of features to help OSN users verify the identities of other user accounts before accepting incoming friend requests, attackers may clone the identity of other users in order to gain access to their victims' social circles and establish forged trust relationships. These attacks are referred to as *Identity Cloning Attacks*, if the victim has a profile on the same OSN in which his/her identity is maliciously being cloned, and *Fake Profile Attacks*, if the victim has no online presence on the corresponding online platform [73], [127], [128]. Thus, the security of knowledge-based authentication schemes would be clearly affected if the social knowledge published by fake accounts were used to formulate the challenge questions presented by these schemes. For trustee-based authentication schemes, it is also crucial to limit the propagation of identity impersonation attacks in order to eliminate the possibility of a user choosing a forged user account as a trusted friend.

### G. Other Attacks

Some papers discussed the vulnerability of knowledge-based social authentication systems to denial of service attacks, in which an attacker attempts to post photos containing subjects unknown to the user and supply them with wrong tagging information in order to decrease the possibility that the user is able to answer challenge questions [27]. Further, researchers have raised concerns related to the vulnerability of trustee-based systems to denial of service attacks [12].

Social authentication schemes deployed in online contexts, such as in OSNs, are also vulnerable to social engineering attacks as previous studies found that the high levels of social trust that govern users' interactions in online communities could lead the users to disclose private information or befriend malicious individuals [11], [17], [96], [129]. In the case of vouching-based authentication techniques used in organizational contexts, it was argued that intermediating humans in the process of issuing users' verification codes significantly increases the vulnerability of these schemes to social engineering attacks [18], [12]. Social engineering techniques may be used to discover users' trustees or collect vouch codes from trustees via spoofing messages or phone calls [18], [8].

Given that previous studies have proven the feasibility of perpetrating automated identity theft attacks in OSNs, found that the probability of users befriending strangers in these networks is high, and shown a direct correlation between the security of users and the security of their trustees, it is clear that the attack surface of social authentication is large and influenced by many human and technological factors [73], [8], [130].

## V. Defense Strategies

By considering the properties that may strengthen or weaken the security of knowledge-based, as well as trust-based, social authentication schemes (discussed in Section III and Section IV), this section demonstrates the possible strategies that could help defend against attacks that may degrade the security of these schemes.

### A. Knowledge-Based Schemes

In order to increase the robustness of the security questions presented by knowledge-based social authentication schemes, a few solutions have been proposed for minimizing the probability of insiders or outsiders guessing answers. For photo-based schemes, several solutions have been suggested, which include applying certain photo transformation processes to the photos presented by social authentication schemes, excluding social knowledge posted by popular friends or friends whose profile pages are not protected, and giving the user the option to customize his/her challenge questions [16], [33], [96].

While it could be argued that allowing users to formulate their own challenge questions would be an alternative that provides greater security, researchers have found that user-chosen questions provide insufficient security levels and have some usability shortcomings [96], [131], [132], [133]. Renaud et al. also proposed increasing the ambiguity of challenge questions by asking users indirect questions that cannot be directly solved using data published in public sources [107]. For example, one type of question that they proposed [107] presents users with pictures of animals and asks them to associate them with the people they know.

Another means of defending against these types of attacks is to limit the amount of social knowledge exposed to adversaries or individuals who exist within users' social circles. OSNs could add features that measure the strength of social connections or the degree of separation between a user and each of his/her direct or indirect friends and decide on the percentage of a user's profile information that could be presented to each of his/her profile viewers [134], [135]. It was also suggested that the probability of successful guessing attacks can be reduced by minimizing the number of guessing attempts allowed for each user and adding features enabling users to monitor all failed and correct guessing attempts associated with their accounts [43].

Other researchers have proposed formulating challenge questions based on the users private interactions with people they know. For instance, it was suggested that *edge* questions are more secure than *node* questions, because they ask about information that is privately shared between a user and his/her friends [15]. However, it should be noted that many users may not privately communicate with their trusted friends on the platform on which a social authentication scheme would be employed. Thus, although *edge* questions are more difficult to guess than *node* or *pseudo-edge* questions, the deployment of this strategy would not be applicable to all user classes, which in turn may also raise some scalability-related issues.

More advanced strategies include techniques that divide a user's social graph into disjoint clusters and formulate challenges asking about the social knowledge selected from these disconnected sets [16]. While many of the proposed strategies rely mainly on filtering out social knowledge uploaded by public user accounts, popular friends, or users who can be easily recognized, the success of these strategies is proportional to the number of connections of a user and the volume of data posted by his/her friends. Thus, in the case of users who do not frequently interact with others or who are not active in a particular social community, the exclusion of some of their connections may benefit adversaries by limiting the size of the solution space they are attempting to explore.

### B. Trust-Based Schemes

*1) Trustees:* To decrease the level of propagation of forest fire attacks in systems that employ vouching-based authentication, it has been suggested that the selection of a specific person as a trustee by a large number of others should be prevented by, for example, limiting the out-degree centrality of each node in the corresponding trustee networks [8]. However, to the best of our knowledge, there is a lack of experimental evidence that identifies the optimal number of appointments that should be linked to a trustee in order to guarantee the security of individuals in a specific online or offline community. In [8], [51], an approach was proposed that guides the trustee selection process and limits the spread of forest fire attacks by ensuring that the trustees selected by each user belong to disjoint social communities. Thus, a greater security guarantee would be achieved as the number of clusters employed for selecting the trustees of a given user increases. However, there is still insufficient research evidence that identifies the best clustering techniques that could be applied for improving the security and robustness of trustee-based social authentication schemes.

It was also suggested in [8], [51] that the selection of trustees should be restricted, and the authors proposed assigning scores to each node in a user's social network and choosing the nodes with the highest scores as trustees for the corresponding user. This could be implicitly computed based on certain graph properties or explicitly achieved by augmenting the community moderation features that ask users to rate the level of trustworthiness of each node to which they connect. However, we still argue that the indicators that could accurately reflect the level of trust between two given nodes in a social graph of an online community should be identified. For instance, the number of mutual friends shared by two nodes cannot be considered a good indicator of the level of trust between these nodes in an OSN [8], [136]. This is because many users form groups of shared interests and thus their accounts may be tightly linked, although they do not know or trust each other.

Removal of the features that remind users who their trustees are may also prevent attackers from being able to specify the seed users who should be compromised in order to compromise their target victims. Although this option could also be another means of defense against forest fire attacks, it would clearly degrade the reliability of the corresponding social authentication scheme, as it would increase the possibility of the received vouch codes being treated as spam messages [8]. Thus, discouraging trustees from sharing these codes, although they are in fact needed by the corresponding user who may have forgotten the names of his/her previously appointed trustees and hence be unable to contact them and ask for their help [8].

*2) Trustworthiness of social relationships:* Measurements of the degree of trust of each social connection belonging to a node in an online community, for example, by analyzing users' behavior or studying the properties of social graphs [49], may help identify suspicious user accounts and thus prevent other users from selecting the owners of these accounts as trustees. The patented method presented in [50], for instance, defines a black list, a gray list and a white list for each user according to which it examines the trustworthiness of nodes in the user's social network. Thus, before authorizing communications from user A to another user T in an online community, the mechanism examines all the nodes in the path between A and T and ensures that they are not included in T's gray list, which is derived from T's black list, and are already included in T's white list.

The patented approach presented in [137] includes measuring the authenticity of identities by comparing individuals' social graph properties with properties of their social communications and assigning confidence scores to each user account accordingly. The basic assumption behind this approach is that the social interactions of a false user identity are unlikely to resemble those that are associated with the real owner of a given user account. For example, it might be observed that a given user account is sending friend requests to many other suspicious user accounts or commenting on posts written by persons who are unlikely to be known to the real owner of the corresponding user account.

In the study reported in [51], the authors suggested analyzing social knowledge posted by two given user accounts in order to determine the probability that the owners of these accounts know each other in the real world and thus simplify the process of implicitly identifying trustworthy interactions over online social networking platforms. For instance, for the purpose of deciding whether there is a parent-child relationship between two user accounts in a social networking system, Underwood et al. proposed comparing the properties associated with these accounts and the level of interaction between them over the corresponding online social networking platform in order to identify the attributes that they share, for example, common friends, common addresses, or the involvement in common social activities [42]. For instance, it could be determined that user A has frequently shared his/her smartphone or location with another user B or has been tagged in most of the photos posted by user C. In [138], the authors also suggested combining public and private data gathered from a number of online and offline sources for the purpose of predicting the level of trustworthiness between individuals based on many attributes, including their common friends, their commonly visited places, and their shared ownerships.

The authors of [139] also proposed increasing the reliability of a friend request sent from user A to user B in an OSN by searching users who are linked to both user A and user B on the same network, calculating the degree of familiarity of each of these common friend with user B, and modifying the authentication request message to include information about the common friend whose degree of familiarity is the highest. The mechanism proposed in [139] takes a number of properties into consideration for calculating the degree of familiarity between different user accounts, including the rate of data flow between user accounts and the recency of their social relationships over OSNs. In [140], additional metrics were also proposed for measuring the level and quality of social interactions in a given social context, including the rate of private communications between two given individuals and the degree of mutuality of social interactions between those individuals.

*3) Vouch codes:* It has also been suggested that constraints should be imposed on the number of vouch codes that can be generated or requested within a given time period [8]. However, the impact of such constraints on the propagation speed of forest fire attacks has not yet been explored in studies in the literature. In [51], the authors also proposed deciding on the number of vouch codes that should be provided for recovering each user account in an online community according to an analysis of the activities of each account and measurements of its degree of suspicion.

*4) Verification of social interactions:* Verification of users' social interactions and the detection of fake profiles in OSNs would positively influence the security of knowledge-based and trust-based social authentication schemes. Several strategies have been suggested for identifying fake identities in online communities, which focus primarily on analyzing social graph properties, studying user activities, or building models that predict and rank the authenticity of user profiles [128], [126], [141], [142], [143], [144]. In [141], for instance, it was argued that the similarity percentage of the social interactions of two accounts could be leveraged for identifying cloned profiles. For defending against a *Fake Profile Attack*, which does not require the prior presence of the victim on the same platform in which the fake profile is created, Conti et al. proposed investigating the growth rates and structural properties of social graphs for characterizing suspicious user behavior [128]. Thus, according to Conti et al.'s proposed approach for detecting fake profiles [128], fake profiles would behave differently as compared to legitimate ones; for example, social networks associated with fake profiles would have faster evolution rates over time.

As the above approaches [128], [141] require the availability of data about users' social interactions and connections in order to detect fake profiles, Xiao et al. implemented a machine learning model for classifying newly created accounts as fake or not before they form connections and build forged trust relationships with other user accounts [126]. In [144], another approach for detecting fake profiles was proposed that basically ranks user accounts based on their likelihood of being fake or legitimate. The prediction mechanism proposed in [144] leverages simple features extracted from the activities of victim accounts in OSNs for assigning weights to user accounts and determining their level of legitimacy accordingly. Wang et al. approached the problem from a different angle, demonstrating the effectiveness of analyzing properties related to user behavior while browsing the Web (e.g., clickstreams and user sessions) for identifying fake profiles in OSNs [143].

## VI. Usability, Security, and Deployability: Comparative Evaluation

Inspired by the comparative evaluation approaches that have been applied to user authentication schemes [145], [39], in this section we present our evaluation of 14 social authentication schemes (see Tables III and V). Our evaluation framework focuses mainly on the usability, security, and deployability of each social authentication scheme.

**Evaluation Criteria.** We defined 24 metrics for evaluating the usability, security, and deployability of the evaluated socially aware schemes, as well as their authentication features. Although other metrics exist that can be used for evaluating specific social authentication schemes, we chose not to include them and focused on the metrics that could help address the social side of all the included authentication schemes. Table VI lists the elements of our evaluation approach and Table VII summarizes the results of our evaluation. In Table VII, we use (🟩) to indicate that the corresponding evaluation element is completely satisfactory, whereas (♦) is used to denote partial satisfaction and (▲ ) implies that a social authentication scheme does not satisfy the corresponding evaluation element. Further, a cell that contains (●) implies that, to the best of our knowledge, the literature does not include sufficient details for evaluating a social authentication technique against a specific evaluation metric. We also use (⊗) to indicate the inapplicability of a metric for evaluating a social authentication scheme.

### A. Usability

We defined seven metrics based on the properties of the challenge questions presented by each knowledge-based social authentication scheme and the relative effort required to collect vouch codes from trustees in trustee-based social authentication schemes to facilitate our evaluation of the overall usability of the schemes included in our evaluation. We paid significant

TABLE VI
SOCIAL AUTHENTICATION SCHEMES: OUR EVALUATION CRITERIA

| | |
|---|---|
| **Usability metrics** | Memorability (E1) |
| | Learnability (E2) |
| | Ease of use (E3) |
| | User friendliness (E4) |
| | Low physical effort (E5) |
| | Reasonable time to authenticate (E6) |
| | Reasonable time to collect authentication data (E7) |
| **Security metrics** | Resilient to automated attacks (E8) |
| | Resilient to guessing attacks (E9) |
| | Resilient to outsider attacks (E10) |
| | Resilient to insider attacks (E11) |
| | Resilient to social engineering attacks (E12) |
| | No correlation between users' security levels (E13) |
| | Resilient to physical attacks (E14) |
| | Little or no reliance on third parties for completing the authentication process (E15) |
| | Less vulnerable to leaking claimers' sensitive information by verfiers (E16) |
| | Uniqueness of authentication secrets (E17) |
| | Difficulty of obtaining knowledge from users' social contexts (E18) |
| **Deployability metrics** | Cost-effectiveness (E19) |
| | Applicability of deployment in highly secure contexts (E20) |
| | Ease of deployment (E21) |
| | Scalable to large number of users (E22) |
| | Scalable to deal with large volumes of data (E23) |
| | Applicability of the authentication approach (E24) |

attention to the cognitive effort involved in recognizing or recalling the social data required to answer security questions or remembering previously appointed vouchers in each social authentication approach. We also took the convenience, user-friendliness, and user acceptability and familiarity of each scheme into consideration.

While the usability of most of the reviewed social authentication schemes is relatively acceptable, we emphasize the importance of conducting user studies that address the learnability of these schemes, since most of them are supposed to be deployed as secondary authentication factors and therefore the users are not expected to frequently practice using them [19]. Extensive evaluations of many usability-related considerations, for example, how to reduce the time and effort required to collect vouch codes received by trustees, are also lacking. We also argue that designers of knowledge-based social authentication schemes need to research the memorization abilities of their target users and focus on asking the users to recognize social knowledge items that are already known to them rather than on designing recall-based questions [131], [39], [95].

*1) Knowledge-based schemes:* In the case of knowledge-based schemes, asking the user to key in his/her answer instead of choosing it would reduce the probability that a user would remember the answer and key it in correctly. In [15], for example, the users were asked to key in their answers instead of selecting or choosing the correct one (see Fig. 4). The authors of [15] argued that, although keying in an answer in a textbox is less usable than choosing an answer from a list, such as in Facebook's photo-based authentication scheme [31], when the user's answer is keyed in it is more difficult for an attacker to guess the answer.

In [32], it was also suggested that the memorability issues that exist in knowledge-based social authentication schemes be addressed by measuring the levels of interaction between a user and each member in his/her friend list (e.g., through assigning scores to the tie strengths between each of two given user accounts in an OSN) and formulating challenge questions to include social knowledge related to the user's most frequent or important interactions. Further, although an increase in the difficulty level of security questions would make it more difficult for attackers to guess the answers, the usability of the corresponding schemes may be degraded in cases where the user is required to recall the answers instead of recognizing them [95], [38], [96]. Similarly, the usability of a knowledge-based social authentication scheme is correlated with the number of challenge questions it presents and the threshold that a user should reach to achieve recovery.

Thus, the usability of a knowledge-based scheme decreases as the cognitive overhead for the user increases. Consequently, designers of security questions should align the properties of these questions with the purpose of deploying a particular scheme and the context in which the scheme would be deployed. Further, there should be a balance between the properties of the presented questions and the level of importance of the user account that is being protected [19]. These properties include the number of questions and their difficulty level, the number of answer choices, and the threshold required for recovery. The decision whether to present multiple-choice questions or ask the user to key in his/her answer, as well as the choice of the type of social knowledge that a user must recognize or recall, are also of extreme importance for designing usable social authentication schemes.

*2) Trust-based schemes:* For trustee-based social authentication systems, a number of researchers have discussed the usability issues related to remembering the names of persons selected as trustees and determining the optimal number of vouch codes that should be collected in order to achieve a good balance between the usability and the security level that should be achieved by these systems [12], [8]. As opposed to knowledge-based schemes, which frequently do not require the user to contact his/her friends in order for the authentication process to be completed, most of the reviewed vouching-based schemes require users to explicitly contact their trustees in order to collect verification codes. Further, users should also consider the expiration periods of these codes, as well as the delay that may be incurred when at least one of their trustees is unavailable. This in turn increases the effort that must be invested by users, which may negatively affect the user experience. Furthermore, users' cognitive overhead is directly correlated with the number of persons who should vouch for their identities. Therefore, the efficiency of trustee-based systems is directly linked to the recovery threshold required by these systems and the number of trusted friends who must be registered by each user before the social authentication processes can be started. Even in the case of the schemes that implicitly infer users' trustworthy interactions, careful attention should be paid to the efficiency considerations related to the time required to crawl and traverse the nodes in a given social network [49], [79].

### B. Security

Because of the involvement of the human factor in each socially aware technique and since some of them may rely on publicly accessible social data for authenticating users, while not sufficiently accounting for the risks coming from members within users' social circles (e.g., friends or acquaintances) [146], 11 metrics were specifically chosen to measure the security consequences of adopting each scheme. For each one, we evaluated the vulnerability of users to impersonation by members within their social groups. The guessability, uniqueness, and predictability of authentication secrets were also considered. We also determined whether the utilization of a scheme would imply that the security of users would be negatively affected by the security of members who exist in the users' social networks.

The results of our comparative evaluation suggest that none of the social authentication schemes that have been proposed is adequately secure, although the security level of these schemes is supposed to be higher than that of their corresponding primary authentication factors [36]. We also note some common security shortcomings, for example, the vulnerability to insider attacks and social engineering attacks.

*1) Knowledge-based schemes:* Our observations show that a number of the reviewed social authentication techniques employ social knowledge shared within the users' social groups for authenticating them. On the other hand, the results of a number of studies agree that individuals' social interactions are frequently shared with an unintended audience in OSNs and that users frequently fail to control their privacy in these networks [147], [17], [113], [119]. Further, even if account holders set their profile pages to be private, adversaries may have some knowledge about users' social interactions from other members in their social groups, for example, when a user is tagged in photos shared by his/her friends [17], [148]. In most knowledge-based social authentication schemes, the quality of social data used in the underlying authentication processes directly affects the security of users [95]. Furthermore, the number of edges connected to a node in a social graph and the security properties of these connections may negatively or positively impact its security. Thus, untrusted friends may be able to guess or infer the knowledge employed in the corresponding social authentication scheme, for example, by using users' uploaded photos or users' friend lists, which in turn increases the users' vulnerability to insider attacks. Users may also be vulnerable to attacks launched by outsiders who may attempt to establish connections with users' accounts or use social engineering tricks to extract knowledge about users' social interactions from their friends [113], [73].

*2) Trust-based schemes:* In the case of social authentication schemes that delegate part of the authentication responsibilities to trusted friends, it has been found that this delegation may degrade the security of the users since their security would be correlated with the security levels of their trustees [8]. Further, when considering the expiration periods of vouch codes, designers should take into account that higher security levels would obviously be achieved if these codes were invalidated faster. However, they should balance the security gains with the usability of their schemes. The same applies when deciding on the length of the verification codes as well as the number of vouchers who should be registered in advance of use or who should be contacted when a user requires authentication. In the case of authentication systems that employ implicit vouching techniques, careful attention should be paid to measuring the level of trust of users' connections and deciding on the approach that should be followed for identifying the most trustworthy nodes that could be employed in implicit vouching processes [79]. For instance, direct relationships with untrusted friends in OSNs should be implicitly excluded. Further, platform designers should account for the possibility that a user who explicitly contacts his/her trustees may be exposed to phone- or email-based attacks attempting to extract vouch codes from his/her trustees [12]. Further, appropriate mechanisms should be implemented to verify the identities of users appointed as trusted friends before allowing them to vouch for a user.

### C. Deployability

The hardware and software requirements, as well as the cost associated with the deployment of each scheme in online or offline contexts, were evaluated. Further, the scalability, accuracy, and reliability of authentication were also considered in our evaluation. We also determined the applicability of deploying the 14 mechanisms in highly secure environments and whether the features of the proposed authentication approaches would equally serve target users.

*1) Knowledge-based schemes:* While the manner in which social knowledge is employed varies from one scheme to another, most of the reviewed schemes have shortcomings that limit the applicability of their deployment to either a specific context or a specific group of users (see Table VII). Further, to ensure the appropriate function of most of the reviewed social authentication schemes, users should already have formed connections with other users within the same platform, interacted with their friends, or uploaded sufficient social knowledge for the use of the corresponding social authentication scheme.

TABLE VII
COMPARATIVE EVALUATION OF SOCIAL AUTHENTICATION SCHEMES: NON-FUNCTIONAL REQUIREMENTS

| Social authentication technique | Ref. | Usability | | | | | | | Security | | | | | | | | | | | Deployability | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | E1 | E2 | E3 | E4 | E5 | E6 | E7 | E8 | E9 | E10 | E11 | E12 | E13 | E14 | E15 | E16 | E17 | E18 | E19 | E20 | E21 | E22 | E23 | E24 |
| Lineup | [27] | ◆ | 🟩 | 🟩 | 🟩 | ⊗ | 🟩 | 🟩 | 🔺 | 🔺 | 🔺 | 🔺 | 🔺 | 🔺 | ⊗ | 🟩 | ⊗ | 🔺 | 🔺 | 🟩 | 🔺 | 🟩 | 🔺 | 🟩 | ◆ |
| Social authentication devices | [30] | ⊗ | ● | 🟩 | 🟩 | 🟩 | ● | ● | ● | ⊗ | ◆ | 🔺 | ● | 🟩 | ◆ | 🟩 | ⊗ | ◆ | 🔺 | ◆ | 🔺 | ◆ | 🟩 | ● | ◆ |
| Facebooks photo-based social authentication | [31] | 🟩 | 🟩 | 🟩 | 🟩 | ⊗ | 🟩 | 🟩 | 🔺 | 🔺 | ◆ | 🔺 | 🔺 | 🔺 | ⊗ | 🟩 | ⊗ | 🔺 | 🔺 | ● | 🔺 | 🟩 | 🔺 | 🟩 | ◆ |
| Photo-based social authentication based on photo-selection and transformation processes | [33] | 🟩 | 🟩 | 🟩 | 🟩 | ⊗ | 🟩 | 🟩 | 🟩 | ◆ | ◆ | 🔺 | 🔺 | 🔺 | ⊗ | 🟩 | ⊗ | 🔺 | 🔺 | ● | 🔺 | 🟩 | 🔺 | 🟩 | ◆ |
| Soc-Auth: Social Authentication Framework Based on a Categorization of Social Knowledge in OSNs | [15] | 🟩 | 🟩 | 🟩 | 🟩 | ⊗ | 🟩 | 🟩 | 🟩 | ◆ | 🟩 | ◆ | 🔺 | 🔺 | ⊗ | 🟩 | ⊗ | ◆ | 🔺 | ● | 🔺 | 🟩 | ◆ | 🟩 | ◆ |
| Vouching Process Proposed by RSA Laboratories | [18] | ◆ | 🟩 | 🟩 | 🟩 | ◆ | 🟩 | ◆ | 🟩 | ◆ | ◆ | ◆ | 🔺 | 🟩 | ◆ | 🔺 | ◆ | 🟩 | ⊗ | ◆ | ◆ | 🟩 | ◆ | ⊗ | ◆ |
| Microsoft vouching system | [12] | ◆ | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🔺 | ⊗ | ◆ | 🔺 | 🔺 | 🔺 | ◆ | ⊗ | 🔺 | ◆ | 🟩 | ⊗ | 🟩 | ◆ | 🟩 | ◆ | ⊗ | ◆ |
| Mobile phone based implicit vouching based authentication | [14] | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | ◆ | 🟩 | ◆ | ◆ | ◆ | 🔺 | 🟩 | ◆ | 🔺 | 🟩 | 🟩 | ⊗ | 🟩 | 🔺 | 🟩 | ◆ | ⊗ | ◆ |
| Trust-based framework for authenticating users in online communities | [69] | 🟩 | 🟩 | 🟩 | 🟩 | ⊗ | 🟩 | 🟩 | ● | 🟩 | 🟩 | ● | ● | ◆ | ⊗ | 🔺 | 🟩 | ⊗ | ⊗ | 🟩 | ◆ | 🟩 | ◆ | ⊗ | 🟩 |
| Souche | [49] | 🟩 | ● | ● | 🟩 | ⊗ | 🟩 | 🟩 | 🟩 | 🟩 | ◆ | ● | ● | ◆ | ⊗ | 🟩 | 🟩 | ⊗ | ⊗ | 🟩 | ◆ | 🟩 | 🟩 | ⊗ | 🟩 |
| Video Notarization | [68] | 🟩 | 🟩 | 🟩 | ◆ | 🟩 | 🟩 | ◆ | 🟩 | 🟩 | 🔺 | ● | ● | 🟩 | 🟩 | 🔺 | 🟩 | ⊗ | ⊗ | 🟩 | 🔺 | 🟩 | ◆ | ⊗ | 🟩 |
| Facebooks trusted contacts social authentication scheme | [37] | ◆ | 🟩 | 🟩 | 🟩 | ⊗ | 🟩 | 🔺 | ● | ◆ | 🔺 | 🔺 | 🔺 | 🔺 | ⊗ | 🔺 | ⊗ | 🟩 | ◆ | ● | 🔺 | 🟩 | ◆ | ⊗ | ◆ |
| i/k-Contact | [55] | 🟩 | 🟩 | 🟩 | ◆ | 🟩 | 🟩 | 🟩 | ● | 🟩 | ◆ | ● | ● | ● | 🟩 | 🔺 | 🟩 | ⊗ | ⊗ | 🟩 | 🔺 | 🟩 | 🔺 | ⊗ | ◆ |
| EAP-SocTLS: Social Authentication for WiFi Networks | [79] | 🟩 | ● | ● | ● | 🟩 | 🟩 | 🟩 | 🔺 | ⊗ | ● | 🔺 | 🔺 | ◆ | ● | 🟩 | 🟩 | ⊗ | ⊗ | 🟩 | 🔺 | 🟩 | 🟩 | ⊗ | ◆ |

While some individuals may have privacy concerns that could limit their interactions and restrict their information sharing behavior on social networking platforms [149], [150], [151], how to design alternative social authentications that address users' privacy concerns and do not rely solely on users' shared knowledge for authenticating them remains an open question. For instance, Facebook's knowledge-based social authentication depends mainly on photos uploaded by users and their supplied tagging information, although some users may have recently joined the online community and not sufficiently interacted.

Further, some photos may be associated with wrong or inaccurate tags, which may therefore decrease the probability that a user would be able to answer the security questions. Thus, asking the users to manually tag their photos or appoint other users who have already joined the same social community as trustees would obviously limit the scalability of social authentication schemes that follow these approaches [27]. Further, as users' social networks vary in size and since users differ in their social experiences, security questions used in socially aware authentication schemes should be designed such that they are applicable to all users. For instance, in Facebook's photo-based social authentication, a user who has few social connections may find it easier to identify subjects who appear in the corresponding challenge questions as compared to another one who has a very long friend list [112]. Social authentication schemes should also address the dynamicity of individuals' social relationships and interactions.

*2) Trust-based schemes:* In comparison with knowledge-based socially aware schemes, it is clear that the availability of trustees when needed is essential in most trust-based authentication schemes that ask the users to collect vouch codes from their friends. It is also noticeable that registering trustees in advance of using many of the vouching-based authentication schemes shown in Table V is mandatory for a user to recover his/her account. Further, we note that, considering that a person has to explicitly communicate with his/her friends by phone or in person in order to collect verification codes sent to his/her trustees, the involvement of a number of external authenticators may significantly increase the effort, cost, and time required to recover user accounts. The overhead imposed on the user may also increase in cases where the vouch codes generated by the corresponding authentication scheme are valid for only a specific time period. Thus, the unavailability of one trusted friend may prevent a user from accessing his/her account. Further, the delay associated with collecting a vouch code from one friend may require the user to restart the entire recovery process and recollect the vouch codes received by his/her trustees.

Further, although some trust-based schemes may have been proven to be effective in specific cases, the possibility of applying them in other online or offline contexts is still unclear. For instance, *EAP-SocTLS* was proposed specifically for mitigating the consequences of sharing passwords of Wi-Fi access points with others, such as friends or visitors [79]. Furthermore, the video notarization feature developed in [68] may effectively prevent unauthorized persons from accessing credentials stored in stolen phones. However, requiring vouchers to allow a video chat with each supplicant may raise scalability- and efficiency-related issues.

We also note that a number of these schemes, and in particular those that can be deployed in physical contexts, have special hardware or software requirements. For instance, the video notarization scheme proposed in [68] requires the users to use their mobile devices cameras in order to start video chats with persons who are supposed to vouch for their identities. Similarly, the availability of trusted friends in the same physical place whose mobile devices are equipped with Bluetooth technology is essential for the correct functioning of the Bluetooth-based vouching scheme proposed in [14]. Further, for proving that devices are physically possessed by their owners using the scheme proposed in [55], two software programs, i-Contact and k-Contact, must be installed.

## VII. Open Issues, Lessons Learned, and Future Research Directions

According to our comprehensive and systematic investigation of all the literature related to social authentication, we now discuss the challenges and the open problems that need to be solved and suggest key research opportunities that could be explored to fuel further advances in the design and development of more robust, secure, privacy-preserving, and usable social authentication schemes. We believe that addressing the issues discussed in this section is vital for the success of social authentication schemes and will encourage more creative exploitation of social knowledge and trust relationships in these schemes.

### A. Open Issues, Challenges, and Lessons Learned

*1) Maintaining unique social contexts:* The effectiveness of deploying knowledge-based social authentication schemes on online social networks strongly depends on users' connections, interactions, and uploaded data. Therefore, the uniqueness level of a user's social context in online social networks may differ according to the number of connections, the type and volume of uploaded data, and the tie strength of social connections. Thus, the overlap that could occur between the social networks of different users who have common friends on the same OSN may decrease the uniqueness level of the users' social contexts. Even if we assume that these users would behave differently and perform different social interactions on the corresponding online platform, it should be noted that some users may have recently joined the online community or not have performed sufficient social interactions with other users. Therefore, as users' social networks evolve over time and grow as they connect to new friends, one of the challenges to the success of social authentication schemes is to ensure that users maintain high security levels, regardless of the types of social activities and the characteristics of the social connections that they have developed on the corresponding OSN.

*2) Characterization of trustworthy social relationships:* The accurate identification of trusted nodes in social graphs is essential for the success of social authentication schemes. However, as highlighted in previous studies [152], [153], [65], [154], trust has multiple facets and can be defined from different perspectives. Our analysis of the features of all the implicit vouching-based social authentication schemes shows that a unified and formal procedure that could be followed for evaluating the trustworthiness of nodes in social graphs is lacking. Further, as trust relationships are complex in nature, we also note that a mechanism that considers all the characteristics of social relationships, i.e., positive vs. negative, long-term vs. temporary, and direct vs. indirect relationships, before involving them in the corresponding authentication processes is lacking. Further, as there are many properties of trust that could be employed for computing trust levels, such as transitivity and composability [153], it has not yet been determined which of these properties is best to leverage in social authentication schemes. For these reasons, we believe the construction of trust quantification and validation models that could be utilized in trust-based social authentication schemes should be explored.

*3) Applicable social authentication schemes:* The essential role of human relationships in social authentication schemes and the fact that users' actions are unpredictable and highly ambiguous would clearly limit the applicability of a specific technique to all classes of users [55]. For trustee-based schemes, the requirement that users appoint trusted friends who are already registered on the same platform that they are using and the transfer of part of the authentication responsibility to these friends would obviously complicate the social authentication processes and make them inapplicable for users whose trusted friends are not members of the same online social community or are unavailable when needed. In the case of knowledge-based schemes, users may not be able to recall some of their interactions that took place in these communities if these interactions were not important to them or if they have not recently used the corresponding system. For these reasons, we believe that treating all users in the same manner in social authentication schemes is an issue that needs to be resolved in the future.

*4) Quality of social knowledge used in challenge questions:* The reliance on publicly accessible data in most of the reviewed social authentication schemes is a major weakness that downgrades the security of these schemes. This also leads to a high correlation between the reliability of authentication in knowledge-based schemes and the quality of social data, types of user interactions in the target community, and the date on which these interactions took place [19], [17], [95]. Thus, the reliance on a dataset that can be easily tainted or the use of social data that are not up to date in the challenge questions presented by knowledge-based schemes would clearly decrease the reliability of these schemes [19], [17]. For these reasons, the question of how to ensure that social authentication schemes maintain acceptable security and usability levels without being affected by the quality of social knowledge utilized in these schemes remains open.

*5) Exclusion of publicly accessible social knowledge:* We note that most of the social knowledge employed in social authentication schemes is known to other users and that there remains a demand for researching the possible means of capturing users' unique social interactions and exploiting these interactions for authentication purposes. We also note that the exploitation of individuals' social interactions in social authentication schemes remains limited to specific types of social knowledge or trust relationships and that there are many possible areas that need to be explored for increasing the robustness of these schemes.

*6) Reflection of offline social factors in online social authentication schemes:* In order for social authentication schemes and, in particular, those that employ implicit vouching techniques, to function correctly, the identification of trustworthy relationships is essential. However, the factors that lead one person to trust another are not limited only to their interactions in the online community in which a social authentication scheme would be deployed. Instead, users' shared experiences and sophisticated interactions in offline contexts negatively or positively affect the trustworthiness level of their relationships [27]. Further, even if we assume that trust relationships are correctly identified, they are highly dynamic and change over time, while they should be immediately reflected in the corresponding social authentication system. The evaluation of human relationships and the trustworthiness of a person or not are also highly subjective and may be affected by users' cultural backgrounds, beliefs, and prior experiences [27]. For these reasons, as users' real-life social interactions may not resemble their interaction in online communities, the decision whether to take into consideration features extracted from users' offline social contexts or not when verifying users' digital identities is a major challenge. Because of the nature of social interactions on the corresponding online platform (e.g., connecting to business professionals on LinkedIn vs. connecting to friends on Facebook), it is also challenging to identify the specific offline and online social features that would be utilized in the corresponding social authentication scheme and decide how to verify the correctness and consistency of these features.

### B. Future Research Directions

*1) Degrees of importance of social relationships:* As the properties of strong social relationships can be easily remembered as compared to those of weak social ties, it seems that current social authentication schemes do not sufficiently take the importance level of social relationships into consideration or tailor the properties of challenge questions according to the unique social experiences of each user. It should also be noted that the importance degrees of users' social relationships may differ according to factors that cannot be visualized in online communities; for example, a weak social tie between two members on Twitter may not necessarily imply that their friendship is weak, in particular if they do not significantly interact on the corresponding online social communication platform. Therefore, we believe that exploring the usability and security implications of leveraging the properties of social ties in the design of more effective challenge questions would be a promising line of research.

*2) Maintaining privacy and security:* Two of the important directions that should be explored in future work are 1) the utilization of the knowledge generated in individuals' social contexts without compromising their privacy and 2) the decision whether better security implications would be realized by allowing a user to choose his/her trustees or by delegating their implicit selection to service providers. Thus, an attacker attempting to compromise a user account should not be presented with any information relating to the user's social interactions, such as photos in Facebook's challenge questions [31]. In [43], for instance, it was suggested that this problem could be addressed by asking users to clearly specify the social knowledge items that could be used to form challenge questions, for example, by implementing features that allow users to mark their posts as private or public. However, we believe that more intelligent solutions that maintain users' privacy without increasing the vulnerability of social authentication schemes to human errors are required.

*3) Identification of unique social knowledge items:* A knowledge-based social authentication mechanism that relies on asking the user to recall or recognize social knowledge other than the names of his/her friends remains to be designed. For example, security questions in knowledge-based social authentication schemes may rely on collecting answers associated with friends' birth dates, the school where they studied, or other forms of knowledge that strangers would be unable to guess. This could be achieved by asking the user to choose his/her own questions before he/she loses access to his/her account or to provide some information that is known only to persons he/she trusts. Although this approach could work, users might still choose questions that they or their close friends can easily remember [131]. Therefore, there is clearly a need for researching the factors that may contribute to enhancing the security of challenge questions presented in social authentication schemes while maintaining users' ability to easily recognize or recall the requested social knowledge items.

*4) Difficulty levels of challenge questions:* In previous research papers, only three means of altering the difficulty of challenge questions considered in photo-based social authentication schemes were proposed [27], [33], [42], [32]: altering the quality of the photos, asking the user to recognize or recall social knowledge that strangers could not easily guess, and aligning the difficulty levels with the degree of suspicion of users' behaviors. However, as users' social experiences involve other types of social knowledge, such as mutual friends and shared interests, we expect researchers in the future to further explore the properties of users' social networks and leverage the abundance of trust data that can be extracted to design more effective challenge questions.

*5) Properties of social authentication schemes:* It is also necessary to research the optimal numbers of challenge questions, answer choices, trustees, and vouch codes that would help achieve better security and usability levels. While the results presented in [8] show that setting the recovery threshold at four trustees in trustee-based schemes would be beneficial, more research studies on the best means of contacting, selecting, and verifying the identities of trusted friends in explicit vouching-based social authentication schemes are still required. For explicit vouching-based social authentication schemes, there is also a demand for reducing the level of dependency on other users for completing the authentication processes. This might significantly help resolve the issues related to the availability of trustees and the correlation between users' security levels.

More research is also needed to determine the optimal number of challenge questions that a user should answer in order to be successfully authenticated in a knowledge-based scheme. Further, while some questions may be more applicable for a specific group of users than for others and since individuals vary in their memorization abilities, it is also necessary to investigate the relationship between the time required for a user to recall the answers of security questions and the type of social knowledge being queried.

*6) Knowledge-based vs. trust-based social authentication:* Although there are variations in the purposes of each proposed social authentication scheme that we reviewed, as well as in their contexts of deployment, in our opinion future researchers should build on the progress that has been made in studies in the literature by comparing the authentication effectiveness of trust-based schemes versus knowledge-based schemes and deciding which of these would be a more convenient or secure option for a specific context or group of users. For instance, knowledge-based and trust-based schemes could be combined in one hybrid authentication model to achieve better security guarantees.

*7) Properties of social graphs:* To address the trade-off between the security and usability considerations of social authentication schemes deployed in online contexts, we also stress the importance of studying the behavior of users in the online communities in which social authentication schemes would be employed and researching the factors that drive user interactions in these communities. Further, while an understanding of the dynamics of user interactions in OSNs might inspire the design of reliable socially aware authentication techniques, it seems that only a few of the evaluated schemes have utilized the quantitative metrics used to analyze users' behaviors in OSNs. For instance, Kim et al. [16] found that nodes with high centrality values are less vulnerable to impersonation than those with lower values, whereas nodes that have low clustering coefficients are more resilient than those that are tightly connected to each other [155], [156]. Thus, given that explicit vouching requires significant effort from the user and his/her trustees and that explicit vouching-based schemes are vulnerable to forest fire attacks and the trusted friend attack, we believe that it is important to further investigate how the capabilities of node centrality metrics, for example, closeness, betweenness, and eigenvector centrality values, could be leveraged to improve implicit vouching-based socially aware schemes [36], [8].

## VIII. Related Surveys: User Authentication

Despite the growing importance, attractiveness, and popularity of social authentication schemes, no study exists that specifically surveyed the schemes that take social knowledge or trust relationships into account for identity verification purposes or highlighted challenges and recent advances in this promising research area. In this paper, we report the first systematic review that surveyed all the social authentication schemes, introduced a taxonomy for characterizing these schemes, and highlighted the limitations, strengths, and weaknesses of these schemes.

In general, previous surveys have paid significant attention to reviewing user authentication mechanisms that rely mainly on biometrics [157], [158], [159], [160], [161], tokens [159], text-based passwords [145], [162], [163], graphical-based passwords [39], [145], [164], [165], [166], or techniques that combine a number of these authentication factors for validating users' identities. For instance, Bonneau et al. reviewed 35 password replacement schemes in terms of 25 factors that form a standard benchmark specifically designed for evaluating the capabilities of user authentication schemes [145]. Recognition- and recall-based graphical password authentication schemes have also been reviewed by a number of researchers [39], [164], [166], [165]. Other reviews also exist that focus on behavioral and physiological biometric authentication schemes, for example, gait identity verification approaches [157], [158], [159], [160], [161].

Although the findings of the above-mentioned reviews may aid our understanding of the strength and limitations of many user authentication schemes, their results cannot be generalized to authentication schemes that employ social knowledge or trust relationships for identity verification. Therefore, a systematic review of the social authentication literature is clearly required. In this paper, we fill this gap by comprehensively reviewing, analyzing, comparing, and investigating the properties, as well as the features, of all social authentication schemes. We also take advantage of the studies that highlight the attacks threatening the security of users in online communities (e.g., [167]) to fully understand the attack surface of social authentication schemes.

## IX. Concluding Remarks

The substantial growth of techniques that allow the properties of users' real-life and online social networks to be extracted and understood has facilitated the adoption of novel socially aware authentication, communication, and networking technologies. In comparison with most other human authentication schemes, which utilize one type of authentication secret for verifying users' identities (e.g., biometrics and passwords), social authentication schemes rely on some forms of social knowledge captured from users' highly dynamic communications, transfer part of the authentication responsibility to trusted friends, or implicitly infer the level of trustworthiness of user actions. In this paper, we presented the first research study that comprehensively and systematically surveyed all the prior work that leveraged social characteristics in identity verification processes. We first proposed a definition of social authentication, identifying the properties that characterize socially aware authentication schemes employed in online or physical contexts. We then developed a taxonomy that classifies all the research lines related to social authentication. We investigated, compared, analyzed, and evaluated the properties and features of all the social authentication schemes leveraged in different contexts, including online social networks, cellular networks, and wireless networks. We also presented a framework that is specifically designed to evaluate the authentication effectiveness of knowledge-based and trust-based social authentication schemes. A comprehensive discussion of all the attack classes that could threaten the security of social authentication schemes and the actions that can be taken against these attacks was also presented. This study also identified some key challenges and promising research directions that we believe will guide and inspire researchers to move with confidence toward developing better social authentication schemes.

According to the findings presented in this paper, we note that (1) the highly sophisticated nature of human interactions, the uncertainty of human behaviors, and the involvement of social factors in social authentication schemes directly impact the authentication accuracy of these schemes, (2) the high vulnerability of social authentication schemes to human error directly impacts their authentication effectiveness, (3) many qualitative and quantitative characteristics of social graphs remain to be exploited for identity verification purposes, and (4) the utilization of data exchanged in communication networks for deriving social features is expected to help reveal a more accurate characterization of the trustworthy social relationships that can best be leveraged in social authentication schemes. We also stress the importance of balancing the purpose of applying a specific social authentication scheme and the abilities of its target users with the security features that it provides. In conclusion, we believe that the full exploitation of social features in identity verification processes will provide very significant opportunities for strengthening existing user authentication schemes. For this reason, we consider this research effort as a starting point for designing novel social authentication schemes.

## Appendix A
## The methodology followed to conduct our systematic review

We follow Kitchenham's procedure for systematically reviewing, evaluating and synthesizing the available studies [168]. The reason for particularly choosing this process is mainly related to its rigorousness and relevance to computing research [169]. Before conducting our searches, the following research questions were formulated: what are the currently used mechanisms for socially authenticating individuals? (**RQ1**), what are the security and usability weaknesses and limitations of these mechanisms? (**RQ2**), what are the strategies that have been proposed for strengthening the security of social authentication techniques? (**RQ3**) and are social authentication mechanisms mostly used as primary or secondary authentication factors? (**RQ4**).

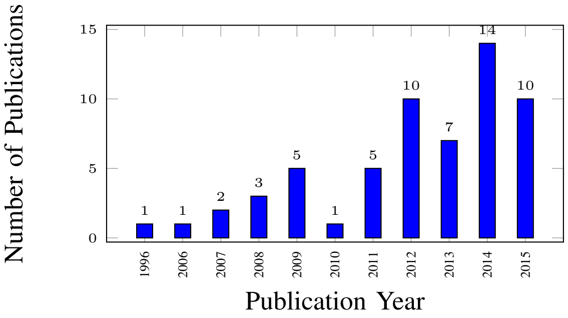


Fig. 13. Distribution of collected publications based on publication years

As shown in Fig. 14, 216 research papers were initially collected and they were classified as either directly related, indirectly related or not related to social authentication. Fifty nine related studies were identified and distributed according to their publication year (as shown in Fig. 13). The majority of studies included in our dataset were published between 2006 and 2015 (inclusive). As shown in Fig. 13, over 77% of the studies were published between 2011 and 2015. This might be due to the fact that Facebook's Trusted Friends and photo-based social authentication mechanisms were established in 2011 [53], [31]. This also shows a significant increase in recent publications related to social authentication which triggers a need for reviewing the literature related to this promising area of research. The following sections summarize the criteria followed to gather, synthesize and assess the quality of research studies included in our review.

### A. Search Strategy

We aimed at covering all the literature related to social authentication. For this reason, we did not restrict our search for primary studies to a specific time period and we used a variety of search terms to query many digital libraries. We performed keyword searches on Google Scholar, ACM [170], Science Direct [171], IEEEXplore [172], Springer [173] and Wiley digital libraries [174] to collect the related literature. We utilized the guidelines presented in [175] to construct boolean search expressions to query the selected digital libraries (see Table VIII). We also prepared a list of popular information security conferences and journals (e.g., IEEE Security and Privacy, USENIX Security, ACM Conference on Computer and Communications Security, SOUPS, and RAID) and focused on investigating all the articles that they published within the last five years (from 2010 to 2015).

Our search started on 20/09/2015 and continued until the submission date of this paper. Because social authentication mechanisms might be either employed as primary authentication factors or in combination with other authentication

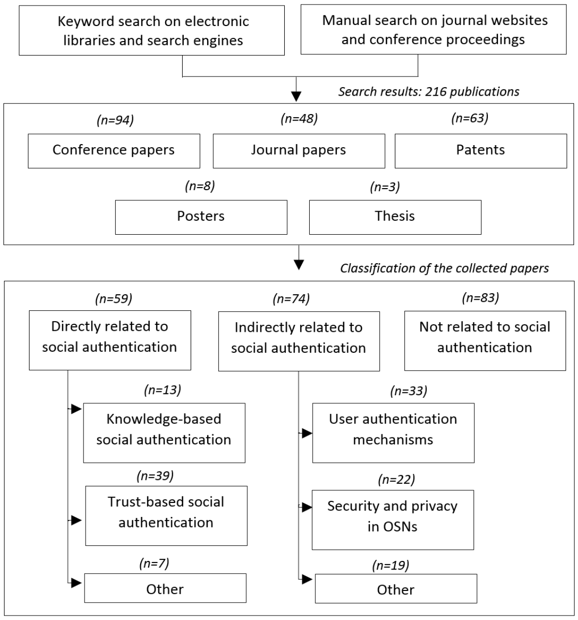

Keyword search on electronic libraries and search engines
Manual search on journal websites and conference proceedings
Search results: 216 publications
(n=94)
Conference papers
(n=48)
Journal papers
(n=63)
Patents
(n=8)
Posters
(n=3)
Thesis
Classification of the collected papers
(n=59)
Directly related to social authentication
(n=74)
Indirectly related to social authentication
(n=83)
Not related to social authentication
(n=13)
Knowledge-based social authentication
(n=39)
Trust-based social authentication
(n=7)
Other
(n=33)
User authentication mechanisms
(n=22)
Security and privacy in OSNs
(n=19)
Other

Fig. 14. The Methodology Followed to Classify Search Results

schemes, our investigation also included studies that might have not directly addressed social authentication. For example, we included some articles that have studied the limitations of knowledge based authentication schemes since their findings might help us in understanding the drawbacks of Facebook's photo-based social authentication scheme [31].

### B. Inclusion and Exclusion Criteria

Because a significant number of studies do not explicitly name the mechanisms they propose as social authentication mechanisms, all the studies that utilize social knowledge or trust relationships for authentication purposes are included. We also consider all the studies that explore the classes of attacks that might threaten the trustworthiness and robustness of social authentication schemes. We give a significant attention to the studies that investigate the security flaws or vulnerabilities that exist in popular social authentication schemes (e.g., Facebook's scheme). We also focus on covering all research papers that discuss the defense strategies that can be employed to enhance the security of previously developed socially-aware authentication techniques. We also included short papers (e.g., abstracts and poster submissions) that include valuable contributions to social authentication. A few number of published theses and all the patents that leverage social knowledge or measure the levels of trust between individuals for building authentication systems were also considered.

TABLE VIII
SOME OF THE FORMULATED SEARCH EXPRESSIONS

| Boolean expression |
|---|
| (social authentication <OR>vouching-based authentication) <AND>(fourth factor <OR>somebody you know) |
| (authentication <AND>(trustee <OR>social knowledge)) |
| (social authentication<AND>(attack<OR> defense<OR>mitigation<OR>vulnerability<OR>threat)) |
| (vouching<OR>trust authentication<OR>vouching code)<AND> (social CAPTCHA<AND>knowledge-based) |

TABLE IX
THE DATA EXTRACTION FORM USED IN THIS STUDY

| | Data Type | Research Question |
|---|---|---|
| 1 | Title | n/a |
| 2 | Publication year | n/a |
| 3 | Publication venue | n/a |
| 4 | Quality score | n/a |
| 5 | Research problem | n/a |
| 6 | Proposed solution | n/a |
| 7 | Social authentication technique | RQ1 and RQ4 |
| 8 | Context of deployment | RQ1 |
| 9 | Attack models | RQ2 |
| 10 | Threat scenarios | RQ2 |
| 11 | security weaknesses | RQ2 |
| 12 | Usability related factors | RQ2 |
| 13 | Limitations | RQ2 |
| 14 | Evaluation techniques | n/a |
| 15 | Defense strategies | RQ3 |

### C. Quality Assessment Criteria

Based on the guidelines presented by Kitchenham et al. [176], we developed a quality assessment checklist consisting of questions we used to judge the quality of the initially selected publications. As adopted in [169] and based on the grading system provided in [177], [178], each reviewer was asked to provide an answer to each question in the checklist. Each of these answers was then mapped to a score that was considered when calculating the overall quality score of each included paper. At the end of this phase, we took the decision to exclude 6 low quality publications as they are published in weak venues and do not present valuable contributions to the literature related to social authentication.

### D. Data Extraction and Synthesis Criteria

For consistently evaluating the research papers included in our dataset, we prepared a data extraction form that was filled for each paper (see Table IX). We then combined the data collected in each form and analyzed the collected data in a comparable way. We further give a significant attention to investigating the details of each study and identifying sub groups of papers that address similar social authentication problems.

We extracted the data related to the type of social authentication scheme addressed by each author (e.g., trust-based or knowledge-based technique) and the security weaknesses and attack classes investigated in each paper (see Table IX). We also recorded the usability and deployability related issues associated with each social authentication scheme. To answer our third research question, the mitigation and defense strategies discussed in each publication were recorded as well.

## ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments which helped us improve the paper to reach its present form. This research work was supported in part by KACST.

## REFERENCES

[1] C. MENLO PARK, "Facebook Reports Second Quarter 2015 Results," Facebook, Tech. Rep., 07 2015. [Online]. Available: https://goo.gl/BuI8X5
[2] "Facebook Users Are Uploading 350 Million New Photos Each Day," http://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9, 2013, [Online; accessed: 20-October-2015].

[3] Y. D. Rubinstein, J. Wiseman, and M. K.-S. Choi, "Trust-based authentication in a social networking system," Mar. 3 2015, US Patent 8,973,100.

[4] V. Narayanan, G. Rose, and L. R. Dondeti, "Social network based PKI authentication," Mar. 13 2012, US Patent Application 13/419,065.

[5] L. J. Donelson and C. W. Sweet III, "Method, apparatus and system for wireless network authentication through social networking," Nov. 2 2011, US Patent Application 13/287,931.

[6] P. C. Castro and U. Topkara, "Social authentication of users," Dec. 2 2014, US Patent 8,904,480.

[7] R. P. Doyle III and P. E. Loeb, "System and method for authenticating users in a social network," Jun. 18 2008, US Patent Application 12/141,896.

[8] N. Z. Gong and D. Wang, "On the security of trustee-based social authentications," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1251–1263, 2014.

[9] C. Colwill, "Human factors in information security: The insider threat–who can you trust these days?" *Information security technical report*, vol. 14, no. 4, pp. 186–196, 2009.

[10] S. Kraemer, P. Carayon, and J. Clem, "Human and organizational factors in computer and information security: Pathways to vulnerabilities," *Computers & Security*, vol. 28, no. 7, pp. 509–520, 2009.

[11] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse social engineering attacks in online social networks," in *Detection of intrusions and malware, and vulnerability assessment*. Springer, 2011, pp. 55–74.

[12] S. Schechter, S. Egelman, and R. W. Reeder, "It's not what you know, but who you know," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2009.

[13] J. Zhan and X. Fang, "Authentication using multi-level social networks," in *Knowledge Discovery, Knowlege Engineering and Knowledge Management*. Springer, 2011, pp. 35–49.

[14] B. Soleymani and M. Maheswaran, "Social authentication protocol for mobile phones," in *International Conference on Computational Science and Engineering (CSE)*, vol. 4. IEEE, 2009, pp. 436–441.

[15] S. Jain, J. Lang, N. Z. Gong, D. Song, S. Basuroy, and P. Mittal, "New directions in social authentication."

[16] H. Kim, J. Tang, and R. Anderson, "Social authentication: harder than it looks," in *Financial Cryptography and Data Security*. Springer, 2012, pp. 1–15.

[17] I. Polakis, M. Lancini, G. Kontaxis, F. Maggi, S. Ioannidis, A. D. Keromytis, and S. Zanero, "All your face are belong to us: Breaking facebook's social authentication," in *Proceedings of the 28th Annual Computer Security Applications Conference*. ACM, 2012, pp. 399–408.

[18] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: somebody you know," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 168–178.

[19] R. W. Reeder and S. Schechter, "When the password doesn't work: Secondary authentication for websites," *Security & Privacy, IEEE*, vol. 9, no. 2, pp. 43–49, 2011.

[20] Y. Jung and E. Rader, "Posters: Transitive privacy concern in social networks," in *Symposium on Usable Privacy and Security*, 2014.

[21] R. Klemm, "Personalizing web applications according to social network user profiles," Feb. 8 2012, US Patent Application 13/368,749.

[22] P. Headley, "User authentication for social networks," May 22 2012, US Patent 8,185,646.

[23] M. Okamoto, "Knowledge-based authentication using twitter," *International Journal of Network Security and Its Applications (IJNSA)*, 2013.

[24] M. Nishigaki and M. Koike, "A user authentication based on personal history-a user authentication system using e-mail history," *The Journal on Systemics, Cybernetics and Informatics*, vol. 5, no. 2, pp. 18–23, 2007.

[25] S. N. Shah, "Social authentication for accessing health records," Jan. 31 2013, US Patent Application 13/756,433.

[26] J. D. Yesberg and M. S. Anderson, "Quantitative authentication and vouching," *Computers & Security*, vol. 15, no. 7, pp. 633–645, 1996.

[27] S. Yardi, N. Feamster, and A. Bruckman, "Photo-based authentication using social networks," in *Proceedings of the first workshop on Online social networks*. ACM, 2008, pp. 55–60.

[28] N. Murarka, "Social authentication," Jun. 5 2014, US Patent Application 13/689,912. [Online]. Available: https://www.google.com/patents/US20140157379

[29] J. Staddon, A. Archer, M. Thakur, and M. Hearn, "Generating authentication challenges based on social network activity information," May 19 2015, US Patent 9,037,864. [Online]. Available: https://www.google.com/patents/US9037864

[30] A. D. Frankel and M. Maheswaran, "Feasibility of a socially aware authentication scheme," in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*. IEEE, 2009, pp. 1–6.

[31] "Facebook: A Continued Commitment to Security," https://www.facebook.com/notes/facebook/a-continued-commitment-to-security/486790652130, 2011, [Online; accessed: 19-October-2015].

[32] L. J. Shepard, W. Chen, T. Perry, and L. Popov, "Using social information for authenticating a user session," Dec. 9 2014, US Patent 8,910,251.

[33] I. Polakis, P. Ilia, F. Maggi, M. Lancini, G. Kontaxis, S. Zanero, S. Ioannidis, and A. D. Keromytis, "Faces in the distorting mirror: Revisiting photo-based social authentication," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 501–512.

[34] "Introducing Login Approvals," https://goo.gl/Fj8h8L, 2011, [Online; accessed: 4-November-2015].

[35] "Google 2-Step Vertification," https://goo.gl/afUasF, [Online; accessed: 4-November-2015].

[36] A. Javed, D. Bletgen, F. Kohlar, M. Durmuth, and J. Schwenk, "Secure fallback authentication and the trusted friend attack," in *IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW)*. IEEE, 2014, pp. 22–28.

[37] "Facebook: Introducing Trusted Contacts," https://www.facebook.com/notes/facebook-security/introducing-trusted-contacts/10151362774980766, 2013, [Online; accessed: 9-October-2015].

[38] S. Schechter, S. Egelman *et al.*, "It's no secret. measuring the security and reliability of authentication via secret questions," in *30th IEEE Symposium on Security and Privacy*. IEEE, 2009, pp. 375–390.

[39] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, p. 19, 2012.

[40] B. Vaishakh and G. Harish, "Captchas: Survey of existing techniques and a new approach," in *National Conference on Recent Trends in Computer Technology Technology Technology*, 2011, pp. 70–73.

[41] M. Wahl, "System and method for authentication in a social network service," Jun. 19 2008, US Patent Application 12/002,370.

[42] E. M. Underwood, J. E. Sullivan, and R. McGeehan, "Social age verification engine," Mar. 11 2014, US Patent 8,671,453.

[43] M. J. Puflea, "System and method for location-aware social networking authentication," Jun. 29 2012, US Patent Application 13/537,585.

[44] "Facebook: The Graph API," https://developers.facebook.com/docs/graph-api/, [Online; accessed: 9-January-2017].

[45] "Google plans to bring password-free logins to Android apps by year-end," http://techcrunch.com/2016/05/23/google-plans-to-bring-password-free-logins-to-android-apps-by-year-end/, 2016, [Online; accessed: 16-June-2016].

[46] S. S. Hamilton, M. C. Carlisle, J. Hamilton *et al.*, "A global look at authentication," in *Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC*. IEEE, 2007, pp. 1–8.

[47] K. R. Ramsaur, "Decentralized peer-based indirect authentication method for personal online social networking profiles," Jan. 28 2014, US Patent Application 14/166,836.

[48] J. Golbeck, *Computing with social trust*. Springer Science & Business Media, 2008.

[49] Y. Xie, F. Yu, Q. Ke, M. Abadi, E. Gillum, K. Vitaldevaria, J. Walter, J. Huang, and Z. M. Mao, "Innocent by association: early recognition of legitimate users," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 353–364.

[50] C. Lunt, "Authorization and authentication based on an individual's social network," Oct. 16 2012, US Patent 8,291,477.

[51] Y. D. Rubinstein, J. A. Brill, A. Bejar, J. H. Frank, and D. Breger, "Using social graph for account recovery," Dec. 23 2010, US Patent Application 12/978,327.

[52] S. Schechter and R. W. Reeder, "Social authentication for account recovery," Jul. 8 2014, US Patent Application 14/326,377.

[53] "Facebook: National Cybersecurity Awareness Month Updates," https://www.facebook.com/notes/facebook-security/national-cybersecurity-awareness-month-updates/10150335022240766, 2011, [Online; accessed: 25-October-2015].

[54] M. Fujita, C. D. Jensen, S. Arimura, Y. Ikeya, and M. Nishigaki, "Physical trust-based persistent authentication," in *13th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2015, pp. 186–190.

[55] S. Arimura, M. Fujita, S. Kobayashi, J.-i. Kani, M. Nishigaki, and A. Shiba, "i/k-contact: A context-aware user authentication using physical social trust," in *Twelfth Annual International Conference on Privacy, Security and Trust (PST)*. IEEE, 2014, pp. 407–413.

[56] K. Jung, E. Ruthruff, and N. Gaspelin, "Automatic identification of familiar faces," *Attention, Perception, & Psychophysics*, vol. 75, no. 7, pp. 1438–1450, 2013.

[57] S. Kasturi, "Online user authentication," Aug. 13 2013, US Patent 8,510,797.

[58] S. Madhu, X. Li, and J. Kamerman, "Analyzing facial recognition data and social network data for user authentication," Sep. 29 2015, US Patent 9,147,117.

[59] Z. Jin and S. Laszlo, "Brain password: Exploring a psychophysiological approach for secure user authentication," *NSF Award TWC SBE-1422417*.

[60] D. Gafurov, E. Snekkenes, and P. Bours, "Gait authentication and identification using wearable accelerometer sensor," in *IEEE Workshop on Automatic Identification Advanced Technologies*. IEEE, 2007, pp. 220–225.

[61] O. Yurur, C. Liu, Z. Sheng, V. Leung, W. Moreno, and K.-S. Leung, "Context-awareness for mobile sensing: a survey and future directions," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 68–93, 2014.

[62] P. Makris, D. N. Skoutas, and C. Skianis, "A survey on context-aware mobile and wireless networking: on networking and computing environments' integration," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 1, pp. 362–386, 2013.

[63] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, and X. Mao, "Incentives for mobile crowd sensing: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 18, no. 1, pp. 54–67, 2016.

[64] N. Vastardis and K. Yang, "Mobile social networks: Architectures, social properties, and key research challenges," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 3, pp. 1355–1371, 2013.

[65] X. Hu, T. H. Chu, V. Leung, E. C.-H. Ngai, P. Kruchten, and H. C. Chan, "A survey on mobile social networks: Applications, platforms, system architectures, and future research directions," *Communications Surveys & Tutorials, IEEE*, vol. 17, no. 3, pp. 1557–1581, 2014.

[66] F. Adib, Z. Kabelac, and D. Katabi, "Multi-person localization via rf body reflections," in *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*. Oakland, CA: USENIX Association, May 2015, pp. 279–292.

[67] I. Traore, *Continuous Authentication Using Biometrics: Data, Models, and Metrics: Data, Models, and Metrics*. IGI Global, 2011.

[68] A. Libonati, A. Kapadia, and M. K. Reiter, "Social security: Combating device theft with community-based video notarization."

[69] L. Li, X. Zhao, and G. Xue, "Searching in the dark: A framework for authenticating unknown users in online social networks," in *Global Communications Conference (GLOBECOM)*. IEEE, 2012, pp. 714–719.

[70] A. W. Young, K. H. McWeeny, D. C. Hay, and A. Ellis, "Matching familiar and unfamiliar faces on identity and expression," *Psychological research*, vol. 48, no. 2, pp. 63–68, 1986.

[71] A. M. Burton, S. Wilson, M. Cowan, and V. Bruce, "Face recognition in poor-quality video: Evidence from security surveillance," *Psychological Science*, vol. 10, no. 3, pp. 243–248, 1999.

[72] E. Callahan, A. Agarwal, C. Cheever, C. Putnam, and B. Trahan, "Determining a trust level in a social network environment," Oct. 1 2013, US Patent 8,549,651.

[73] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in *Proceedings of the 18th international conference on World Wide Web*. ACM, 2009, pp. 551–560.

[74] M. Abramson and D. W. Aha, "User authentication from web browsing behavior," DTIC Document, Tech. Rep., 2013.

[75] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location," *arXiv preprint arXiv:1503.08479*, 2015.

[76] M. U. Ilyas, M. Z. Shafiq, A. X. Liu, and H. Radha, "A distributed algorithm for identifying information hubs in social networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 629–640, 2013.

[77] M. U. Ilyas, M. Z. Shafiq, A. X. Liu, and H. Radha, "A distributed and privacy preserving algorithm for identifying information hubs in social networks," in *Proceedings of INFOCOM*. IEEE, 2011, pp. 561–565.

[78] N. Eagle, A. S. Pentland, and D. Lazer, "Inferring friendship network structure by using mobile phone data," *Proceedings of the national academy of sciences*, vol. 106, no. 36, pp. 15 274–15 278, 2009.

[79] Y. Durmus and K. Langendoen, "Wifi authentication through social networks."

[80] B. Liu, B. Khorashadi, and S. M. Das, "Mobile device authentication and access to a social network," Sep. 12 2011, US Patent Application 13/230,444.

[81] B. Nath, L. Iftode, P. Shankar, and L. Han, "System and method for personal device sharing using social networks," Mar. 29 2011, US Patent Application 13/074,252.

[82] C. M. Tam, P. S. Gill, and B. S. Gill, "System and method for creating a secure trusted social network," Apr. 22 2014, US Patent 8,707,394.

[83] J. Surowiecki, *The wisdom of crowds*. Anchor, 2005.

[84] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, 2012.

[85] D. Guinard, M. Fischer, and V. Trifa, "Sharing using social networks in a composable web of things," in *8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. IEEE, 2010, pp. 702–707.

[86] "WebID specifications," http://www.w3.org/2005/Incubator/webid/spec/, 2013, [Online; accessed: 1-November-2015].

[87] "FOAF Vocabulary Specification 0.99," http://xmlns.com/foaf/spec/, 2014, [Online; accessed: 1-November-2015].

[88] D. Naboulsi, M. Fiore, S. Ribot, and R. Stanica, "Large-scale mobile traffic analysis: a survey," *Communications Surveys & Tutorials, IEEE*, vol. 18, no. 1, pp. 124–161, 2015.

[89] M. U. Ilyas, M. Zubair Shafiq, A. X. Liu, and H. Radha, "Who are you talking to? breaching privacy in encrypted im networks," in *21st IEEE International Conference on Network Protocols (ICNP)*. IEEE, 2013, pp. 1–10.

[90] F. Rebecchi, M. Dias de Amorim, V. Conan, A. Passarella, R. Bruno, and M. Conti, "Data offloading techniques in cellular networks: a survey," *Communications Surveys & Tutorials, IEEE*, vol. 17, no. 2, pp. 580–603, 2015.

[91] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "Large-scale measurement and characterization of cellular machine-to-machine traffic," *IEEE/ACM Transactions on Networking (TON)*, vol. 21, no. 6, pp. 1960–1973, 2013.

[92] Y. He, M. Chen, B. Ge, and M. Guizani, "On wifi offloading in heterogeneous networks: Various incentives and trade-off strategies," *Communications Surveys & Tutorials, IEEE*, pp. 1–41, 2016.

[93] K. Wei, X. Liang, and K. Xu, "A survey of social-aware routing protocols in delay tolerant networks: applications, taxonomy and design-related issues," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 1, pp. 556–578, 2014.

[94] Y. Zhu, B. Xu, X. Shi, and Y. Wang, "A survey of social-based routing in delay tolerant networks: positive and negative social effects," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 1, pp. 387–401, 2013.

[95] A. Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of facebook," in *Proceedings of the 4th symposium on Usable Privacy and Security*. ACM, 2008, pp. 13–23.

[96] J. Bonneau, E. Bursztein, I. Caron, R. Jackson, and M. Williamson, "Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google," in *Proceedings of the 24th International Conference on World Wide Web*, 2015, pp. 141–150.

[97] M. Just, "Designing authentication systems with challenge questions," *Security and Usability: Designing Secure Systems That People Can Use*, pp. 143–155, 2005.

[98] M. Just, "Designing and evaluating challenge-question systems," *IEEE Security & Privacy*, no. 5, pp. 32–39, 2004.

[99] "Guidelines for Identification and Authentication," https://goo.gl/ChN4rZ, 2006, [Online; accessed: 11-November-2015].

[100] W. J. Haga and M. Zviran, "Question-and-answer passwords: an empirical evaluation," *Information Systems*, vol. 16, no. 3, pp. 335–343, 1991.

[101] V. Griffith and M. Jakobsson, "Messin with texas deriving mothers maiden names using public records," in *Applied Cryptography and Network Security*. Springer, 2005, pp. 91–103.

[102] J. Noll, M. M. Chowdhury, G. Kálmán, and J. M. Gomez, "Semantically supported authentication and privacy in social networks," in *The International Conference on Emerging Security Information, Systems, and Technologies*. IEEE, 2007, pp. 83–88.

[103] J. Bonneau, M. Just, and G. Matthews, "Whats in a name?" in *Financial Cryptography and Data Security*. Springer, 2010, pp. 98–113.

[104] S. Schechter, C. Herley, and M. Mitzenmacher, "Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks," in *Proceedings of the 5th USENIX conference on Hot topics in security*. USENIX Association, 2010, pp. 1–8.

[105] J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2012, pp. 538–552.

[106] J. Bonneau, J. Anderson, R. Anderson, and F. Stajano, "Eight friends are enough: social graph approximation via public listings," in *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*. ACM, 2009, pp. 13–18.

[107] K. Renaud and M. Just, "Pictures or questions?: examining user responses to association-based authentication," in *Proceedings of the 24th BCS Interaction Specialist Group Conference*. British Computer Society, 2010, pp. 98–107.

[108] B. C. Becker and E. G. Ortiz, "Evaluation of face recognition techniques for application to facebook," in *8th IEEE International Conference on Automatic Face & Gesture Recognition*. IEEE, 2008, pp. 1–6.

[109] A. Acquisti, R. Gross, and F. Stutzman, "Faces of facebook: Privacy in the age of augmented reality," 2011.

[110] M. Dantone, L. Bossard, T. Quack, and L. Van Gool, "Augmented faces," in *Computer Vision Workshops (ICCV Workshops)*. IEEE, 2011, pp. 24–31.

[111] R. Dey, Z. Jelveh, and K. Ross, "Facebook users have become much more private: A large-scale study," in *Pervasive Computing and Communications Workshops (PERCOM Workshops)*. IEEE, 2012, pp. 346–352.

[112] M. Lancini, "Social authentication vulnerabilities, mitigations, and redesign," in *Proceedings of the DeepSec Conferences*, 2014, pp. 476–492.

[113] F. Nagle and L. Singh, "Can friends be trusted? exploring privacy in online social networks," in *Social Network Analysis and Mining (ASONAM'09)*. IEEE, 2009, pp. 312–315.

[114] H. Kim and J. Bonneau, "Privacy-enhanced public view for social graphs," in *Proceedings of the 2nd ACM workshop on Social web search and mining*. ACM, 2009, pp. 41–48.

[115] L. Jin, J. B. Joshi, and M. Anwar, "Mutual-friend based attacks in social network systems," *Computers & Security*, vol. 37, pp. 15–30, 2013.

[116] Z. Wen and C.-Y. Lin, "On the quality of inferring interests from social neighbors," in *Proceedings of the 16th ACM SIGKDD international conference on knowledge discovery and data mining*. ACM, 2010, pp. 373–382.

[117] J. M. Kleinberg, "Challenges in mining social network data: processes, privacy, and paradoxes," in *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2007, pp. 4–5.

[118] W. Pratte and D. Stephenson, "Method and apparatus for network authentication of human interaction and user identity," Aug. 13 2013, US Patent 8,510,814.

[119] M. Johnson, S. Egelman, and S. M. Bellovin, "Facebook and privacy: it's complicated," in *Proceedings of the eighth symposium on usable privacy and security*. ACM, 2012, p. 9.

[120] R. F. Mills, G. L. Peterson, and M. R. Grimaila, "Insider threat prevention, detection and mitigation," *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions: Threat Analysis and Response Solutions*, vol. 4, no. 5, p. 6, 2009.

[121] M. Toomim, X. Zhang, J. Fogarty, and J. A. Landay, "Access control by testing for shared knowledge," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2008, pp. 193–196.

[122] H. Krasnova, O. Günther, S. Spiekermann, and K. Koroleva, "Privacy concerns and identity in online social networks," *Identity in the Information Society*, vol. 2, no. 1, pp. 39–63, 2009.

[123] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: an online social network with user-defined privacy," in *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 4. ACM, 2009, pp. 135–146.

[124] Z. Tufekci, "Can you see me now? audience and disclosure regulation in online social network sites," *Bulletin of Science, Technology & Society*, vol. 28, no. 1, pp. 20–36, 2008.

[125] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," *Internet Computing, IEEE*, vol. 15, no. 4, pp. 56–63, 2011.

[126] C. Xiao, D. M. Freeman, and T. Hwa, "Detecting clusters of fake accounts in online social networks," in *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*. ACM, 2015, pp. 91–101.

[127] L. Jin, H. Takabi, and J. B. Joshi, "Towards active detection of identity clone attacks on online social networks," in *Proceedings of the first ACM conference on data and application security and privacy*. ACM, 2011, pp. 27–38.

[128] M. Conti, R. Poovendran, and M. Secchiero, "Fakebook: Detecting fake profiles in on-line social networks," in *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*. IEEE Computer Society, 2012, pp. 1071–1078.

[129] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2011.

[130] R. Potharaju, B. Carbunar, and C. Nita-Rotaru, "ifriendu: leveraging 3-cliques to enhance infiltration attacks in online social networks," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 723–725.

[131] M. Just and D. Aspinall, "Personal choice and challenge questions: a security and usability assessment," in *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, 2009, p. 8.

[132] M. Just and D. Aspinall, "Challenging challenge questions: an experimental analysis of authentication technologies and user behaviour," *Policy & Internet*, vol. 2, no. 1, pp. 99–115, 2010.

[133] J. Liu and Y. Xie, "Method and apparatus for user authentication," Sep. 17 2015, US Patent 0264031 A1.

[134] M. E. Hull, F. R. Farmer, and E. S. Perelman, "Method and system for customizing views of information associated with a social network user," Sep. 11 2007, US Patent 7,269,590.

[135] N. Galbreath and C. Lunt, "System and method for managing information flow between members of an online social network," Aug. 30 2011, US Patent 8,010,458.

[136] E. Gilbert and K. Karahalios, "Predicting tie strength with social media," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2009, pp. 211–220.

[137] R. Shishkov and D. A. Baranov, "Authentication based on social graph transaction history data," Feb. 15 2013, US Patent Application 13/768,379.

[138] J. P. de Villiers Prichard and J. C. Shaw, "Systems and methods for identity authentication using a social network," Oct. 1 2013, uS Patent 8,549,590.

[139] J. Mo and J. Ye, "Method and apparatus for sending authentication request message in a social network," Oct. 22 2013, US Patent 8,566,396.

[140] B. Dom, J. Ruvolo, and G. Tewari, "Detect and qualify relationships between people and find the best path through the resulting social network," Dec. 19 2002, US Patent Application 10/323,568.

[141] O. Goga, G. Venkatadri, and K. P. Gummadi, "Exposing impersonation attacks in online social networks."

[142] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in *Presented as part of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12)*, 2012, pp. 197–210.

[143] G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng, and B. Y. Zhao, "You are how you click: Clickstream analysis for sybil detection," in *Proc. USENIX Security*. Citeseer, 2013, pp. 1–15.

[144] Y. Boshmaf, D. Logothetis, G. Siganos, J. Lería, J. Lorenzo, M. Ripeanu, and K. Beznosov, "Integro: Leveraging victim prediction for robust fake account detection in osns." in *NDSS*, vol. 15. Citeseer, 2015, pp. 8–11.

[145] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 553–567.

[146] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on privacy in the electronic society*. ACM, 2005, pp. 71–80.

[147] A. K. Adams and A. J. Lee, "Combining social authentication and untrusted clouds for private location sharing," in *Proceedings of the 18th ACM symposium on Access control models and technologies*. ACM, 2013, pp. 15–24.

[148] L. A. Cutillo, R. Molva, and T. Strufe, "Safebook: A privacy-preserving online social network leveraging on real-life trust," *Communications Magazine, IEEE*, vol. 47, no. 12, pp. 94–101, 2009.

[149] A. Tootoonchian, S. Saroiu, Y. Ganjali, and A. Wolman, "Lockr: better privacy for social networks," in *Proceedings of the 5th international conference on Emerging networking experiments and technologies*. ACM, 2009, pp. 169–180.

[150] C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of facebook and myspace," *AMCIS 2007 Proceedings*, p. 339, 2007.

[151] J. Anderson, C. Diaz, J. Bonneau, and F. Stajano, "Privacy-enabling social networking over untrusted networks," in *Proceedings of the 2nd ACM workshop on Online social networks*. ACM, 2009, pp. 1–6.

[152] W. Viriyasitavat and A. Martin, "A survey of trust in workflows and relevant contexts," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 3, pp. 911–940, 2012.

[153] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 2, pp. 279–298, 2012.

[154] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Computing Surveys (CSUR)*, vol. 45, no. 4, p. 47, 2013.

[155] G. Sabidussi, "The centrality index of a graph," *Psychometrika*, vol. 31, no. 4, pp. 581–603, 1966.

[156] K. Okamoto, W. Chen, and X.-Y. Li, "Ranking of closeness centrality for large-scale social networks," in *Frontiers in Algorithmics*. Springer, 2008, pp. 186–195.

[157] N. Mastali, J. Agbinya *et al.*, "Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: A survey paper," in *Broadband and Biomedical Communications (IB2Com), 2010 Fifth International Conference on*. IEEE, 2010, pp. 1–6.

[158] W. Meng, D. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1268–1293, 2015.

[159] L. O. Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.

[160] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[161] D. Gafurov, "A survey of biometric gait recognition: Approaches, security and challenges," in *Annual Norwegian Computer Science Conference*. Citeseer, 2007, pp. 19–21.

[162] D. L. Jobusch and A. E. Oldehoeft, "A survey of password mechanisms: Weaknesses and potential improvements. part 1," *Computers & Security*, vol. 8, no. 7, pp. 587–604, 1989.

[163] D. L. Jobusch and A. E. oldehoeft, "A survey of password mechanisms: Weaknesses and potential improvements. part 2," *Computers & Security*, vol. 8, no. 8, pp. 675–689, 1989.

[164] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *21st Adnnual Computer Security Applications Conference*. IEEE, 2005, pp. 10–pp.

[165] A. H. Lashkari and S. Farmand, "A survey on usability and security features in graphical user authentication algorithms," *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, pp. 195–204, 2009.

[166] F. Towhidi and M. Masrom, "A survey on recognition based graphical user authentication algorithms," *arXiv preprint arXiv:0912.0942*, 2009.

[167] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: Threats and solutions," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 4, pp. 2019–2036, 2014.

[168] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele University*, vol. 33, no. 2004, pp. 1–26, 2004.

[169] M. Galster, D. Weyns, D. Tofan, B. Michalik, and P. Avgeriou, "Variability in software systems: a systematic literature review," *IEEE Transactions on Software Engineering*, vol. 40, no. 3, pp. 282–306, 2014.

[170] "ACM Digital Library," http://dl.acm.org/, [Online; accessed: 6-June-2016].

[171] "ScienceDirect," www.sciencedirect.com, [Online; accessed: 6-June-2016].

[172] "IEEE Xplore Digital Library," http://ieeexplore.ieee.org/, [Online; accessed: 6-June-2016].

[173] "Springer Link," http://link.springer.com/, [Online; accessed: 6-June-2016].

[174] "Wiley Online Library," onlinelibrary.wiley.com, [Online; accessed: 6-June-2016].

[175] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571–583, 2007.

[176] B. A. Kitchenham, O. P. Brereton, D. Budgen, and Z. Li, "An evaluation of quality checklist proposals: a participant-observer case study," in *Proceedings of the 13th international conference on Evaluation and Assessment in Software Engineering*. British Computer Society, 2009, pp. 55–64.

[177] T. Dyba, T. Dingsoyr, and G. K. Hanssen, "Applying systematic reviews to diverse study types: An experience report," in *First International Symposium on Empirical Software Engineering and Measurement*. IEEE, 2007, pp. 225–234.

[178] N. Salleh, E. Mendes, and J. Grundy, "Empirical studies of pair programming for cs/se teaching in higher education: A systematic literature review," *IEEE Transactions on Software Engineering*, vol. 37, no. 4, pp. 509–525, 2011.