A Survey on the Security of Pervasive Online Social Networks (POSNs)

Takshi Gupta, Gaurav Choudhary, and Vishal Sharma*
Department of Information Security Engineering
Soonchunhyang University, Asan-si, Choongchungnam-do, Republic of Korea
takshi_gupta2012@hotmail.com, gauravchoudhary7777@gmail.com,
vishal_sharma2012@hotmail.com

Abstract

Pervasive Online Social Networks (POSNs) are the extensions of Online Social Networks (OSNs) which facilitate connectivity irrespective of the domain and properties of users. POSNs have been accumulated with the convergence of a plethora of social networking platforms with a motivation of bridging their gap. Over the last decade, OSNs have visually perceived an altogether tremendous amount of advancement in terms of the number of users as well as technology enablers. A single OSN is the property of an organization, which ascertains smooth functioning of its accommodations for providing a quality experience to their users. However, with POSNs, multiple OSNs have coalesced through communities, circles, or only properties, which make service-provisioning tedious and arduous to sustain. Especially, challenges become rigorous when the focus is on the security perspective of cross-platform OSNs, which are an integral part of POSNs. Thus, it is of utmost paramountcy to highlight such a requirement and understand the current situation while discussing the available state-of-the-art. With the modernization of OSNs and convergence towards POSNs, it is compulsory to understand the impact and reach of current solutions for enhancing the security of users as well as associated services. This survey understands this requisite and fixates on different sets of studies presented over the last few years and surveys them for their applicability to POSNs. There is a limited amount of content available for the security of POSNs. However, being an extension to general OSNs, solutions applicable to OSNs are withal included to understand the practicality for POSNs. Moreover, this survey additionally includes content cognate to trust management and anomaly detection in POSNs. In integration, a broad classification is additionally presented for each category with a tabular comparison. At last, certain future challenges, open issues, and research goals are presented, which can be focused by leading or upcoming researchers while emphasizing the security of POSNs.

Keywords: Anomaly, Online Social Networks, POSNs, Security, Trust, IoT.

1 Introduction

Connecting users irrespective of their domain and online platform is studied under Pervasive Online Social Networks (POSNs). POSNs help to facilitate pervasive social networking by eliminating the resource and architectural boundaries of the OSN platforms. POSNs allow inter-connectivity amongst vast domains of OSN applications like contact-building, news-sharing, business modeling, online content-making, career build-ups, etc, as shown in Figure 1. In general, POSNs comprise of a large set of communities which belong to different social network platforms and are combined together on the basis of common interests or roles [136] [140]. Apart from these, POSNs also accommodate vehicular social networks which involve dynamic components as a social networking entity, such as smart cars, robots, drones, or even autonomous vehicles [144] [183] [129].

Journal of Internet Services and Information Security (JISIS), volume: 8, number: 2 (May 2018), pp. 48-86

*Corresponding author: Department of Information Security Engineering, Soonchunhyang University, 22 Soonchunhyang-ro, Shinchang-myeon, Asan-si, Choongchungnam-do, Republic of Korea 31538, Tel: +82-(0)41-530-3099

Figure 1: Applications of pervasive online social networks.

In spite of the tremendous amount of facilities and advantages, POSNs suffer from critical issues related to security, privacy, trust and anomaly detections [37] [51]. POSNs require sufficiently efficient, but low complex solutions to identify and mitigate the threats associated with the smooth functioning over platforms that support its applications. Trust helps to formalize relationships amongst the entities involved in POSNs while leveraging on the popular solutions like reputation building, Peer to Peer, or Peer to Multi-Peer connectivity [150] [106]. However, the success of such requirements depends on the level of security accommodation supported by policies for POSNs.

In addition, operational profilers can be used to determine the roles users as well as for the classification of communities. Successful classification of communities supports easier management of POSNs as well as helps to regulate the common operations without any interruptions. Detection of faulty users in POSNs can be carried either through the involved platforms or multiple platforms can depend on the third-party evaluators. However, these solutions are dependent on the privacy policies as well as the personalized settings of each involved community or a user.

Vulnerabilities in POSNs tend to gain access over the unsecured wireless links and identify systems with failed security patches and software-prone to different attacks [180] [4]. Further, attacks on POSNs expose the passwords, device-information as well as feed users with malicious and undesirable contents. Threats in POSNs can be due to malicious programs such as viruses, trojans, malware, worms, and botnets. Especially, over the last decade, adware has been the leading cause of attacks on most of the OSN platforms and has potential to exploit users in POSNs. Alongside, Denial of Service (DoS), Distributed Denial of Service Attacks (DDoS), Data theft, Sybil attacks, Blackhole attack, Greyhole attack, and zero-hour attacks are other known attacks that can target POSNs [48, 72, 123, 128, 170].

Intentional user-access privileges and the unwanted inclusion of service-requests pose a significant security threat in POSNs. Management of users, marking of communities, identification of platforms,

accessibilities to cross-platform services and data lookups should be prioritized and limited accessibility should be given to a regular user in POSN, as shown in Figure 2 [130]. Such a management can help to reduce the severity of an attack, which might be launched in future. Frequent evaluations should be conducted to check the privileges of maintenance as well as root users. Machine learning and Artificial Intelligence (AI) can be used to develop software that can periodically check user accounts and can help to clean up inactive or largely requesting accounts on cross-platform POSNs.

Moreover, Internet security solutions, strong authentication, and novel key agreement protocols can also help to formalize solutions for preventing any known cyber attack on POSNs [56] [168]. Such solutions can be supported by techniques like packet filtering, stateful packet inspection, firewalls, security tokens, or even through authentication protocols like Extensible Authentication Protocol (EAP), Identity Authentication Protocol (IAP), Password Authentication Protocol (PAP), Host Identity Protocol (HIP), Secure Remote Password protocol (SRP), Challenge-Handshake Authentication Protocol (CHAP), etc [98] [46].

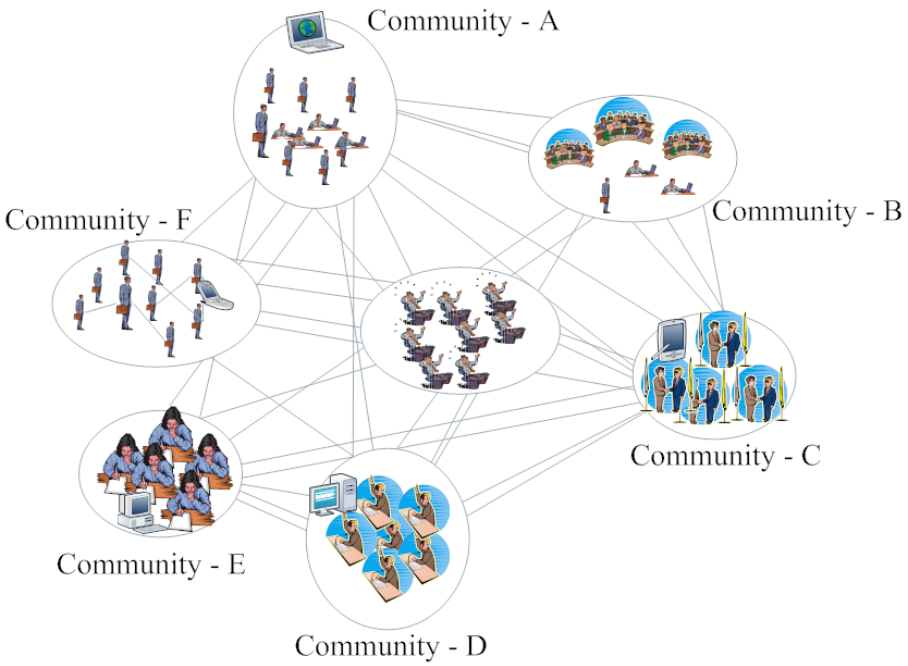

Figure 2: An exemplary illustration of pervasive online social networks through multiple communities.

1.1 Advantages of POSNs

Online social communities emerge exponentially over the POSNs. Social networking platforms like Facebook, Twitter, etc, empower the users and increase their interests to exchange information and resources. Some of the advantages of POSNs, as shown in Figure 3, are discussed below.

- **Marketing benefits :** POSNs plays an important role in business advertisements. Nowadays, companies, artists, and musicians can reach an impossibly large and diverse amount of people using cross-platform services. Social media can be used as of promotional tool for marketing of their products. Targeting specialized community and showcasing results of interest are major advantages of POSNs.

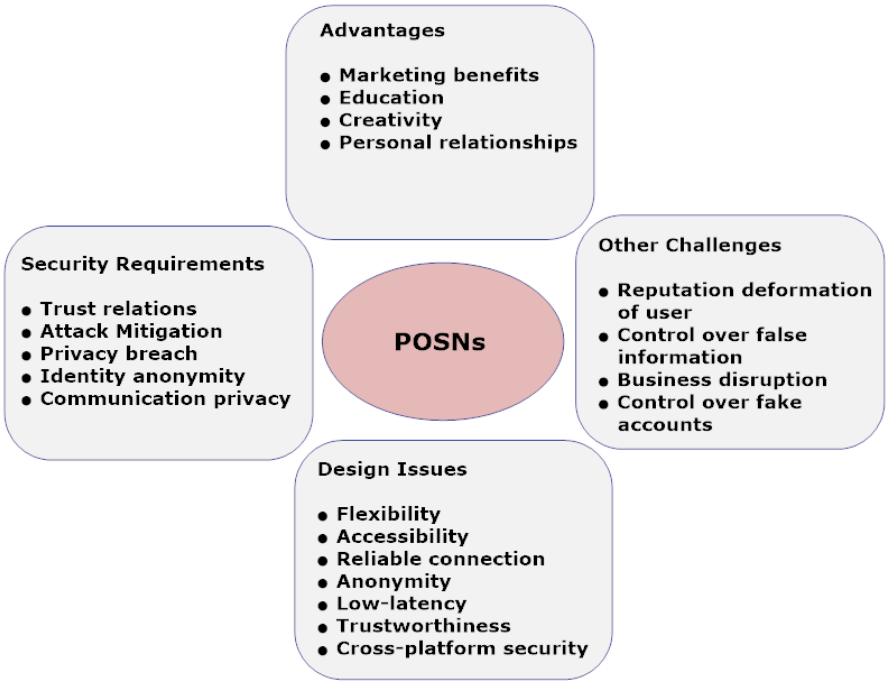

Figure 3: Advantages and challenges associated with the implementation of POSNs.

- **Education :** POSNs can be regarded as a platform allowing academicians and industry-researchers to communicate and collaborate on their requirements.
- **Creativity :** These platforms boost the users to perform creative activities with their friends and communities. These platforms are open to think and share their ideas with different users.
- **Personal relationships :** Social relationships and personal relationships can be maintained through POSNs, and information/profiles on one can be shared with other platforms without recreational overheads.

1.2 Challenges of POSNs

POSNs have considerable constraints in terms of security requirements as discussed below:

- **Developing secure and reliable relationship model :** POSNs rely on relationship models for interaction between the users and the communities. The social relationships involve different paradigms in terms of strength and scope of connections. The relationship models consist of the type of relationship, the strength of trust and the intensity of interactions. An effective relationship model can help to enhance the reliability and scalability of POSNs. Moreover, a relationship model helps to maintain a tradeoff between the complexity and accuracy of search and connection establishment amongst different communities [167].
- **Reputation defamation of user :** Reputation is a very important asset in term of values and credibility. The reputation is directly proportional to the trust of POSNs. If the information is compromised then it destroys the credibility and reputation of a person, institution, organization,

social group, or nation which exists in POSNs [27]. Therefore mitigation of this risk is another primary concern for POSNs.

- **Control over false information :** The information registered over POSNs should be legitimate and it should be verified from the perspective of security. The false information can be used to defame the person or any organization. The spreading false information is very critical over POSNs because it leads to conflicts or any critical loss of any origination or any person. Therefore to resolve this issue, POSNs require protocols and policies to be added for controlling above discussed issues.

- **Business disruption :** The organizational communities are important pillars of POSNs. The information to advertise the business of any organization leads to the misuses of assets if the false or forged information is used for advertisement. Therefore, privacy against the shared information is a considerable challenge to resolve for POSNs.

- **Control over fake accounts :** Recently, forging and duplication of accounts have rapidly increased over social media. The duplicate accounts, which are used by the attacker, spread lots of false information through their fake accounts and should be avoided in POSNs.

1.3 Design Issues of POSNs

The traditional goals of POSNs such as usability and sociability are influenced by the functionalities and designing of cross-platform services [108] [54]. But there exist certain design issues which have to be focused while implementing POSNs. These include,

- **Flexibility :** POSNs utilize centralized web server and all the information is to be processed within the design consideration of the underlaid platform. POSNs provide all the functionalities, like storage, maintenance, and access to OSN services. Therefore, the flexibility of POSNs is required to provide large computation and handling of multi-users at a single instance and at low-complexity.

- **Accessibility :** Many communities are connected through POSNs for accessing diversified services. The accessibility helps to maintain a check on the information and the content which are to be shared among the users of POSNs.

- **Reliable connection :** POSNs are defined over connected graphs where the user can access and share their relationships with other. The connected graphs i.e. reliable connection, are required to maintain communication between different communities, which should be facilitated through reliable connectivity and data exchanges.

- **Anonymity :** The protection of a user's identity helps anonymity. The visibility of a user's profile reveals lots of personal information. Therefore, masking of the identity or pseudo-identity is required to hide the user's personal information. This also prevents stalking and identity thefts.

- **Low-latency :** With an increased use of POSNs, low latency solutions are required for authentication and information access by third-party applications through APIs.

- **Trustworthiness :** In POSNs, two different users communicate with each other, therefore, the evaluation of their trustworthiness along a certain transfer path is mandatory. The trust map can be used for such a requirement that represents the connectivity of users as a result of their trust values and overall trustworthiness.

- **Cross-platform security :** Cross-platform OSNs may allow the same person to have multiple accounts on multiple platforms. Therefore, the cross-platform availability and reputation mechanism are mandatory in POSNs. Web services play a significant role in the interoperability of cross platforms. Therefore, cross-platform services with high security are major issues in POSNs.

1.4 Security requirements in POSNs

POSNs store a huge amount of critical information about users and their private conversations. The cyber-attacks like identity thefts, stalking, cyber bullies, etc, are responsible for information leakage [40] [33]. Therefore, the effective and flexible security mechanisms are required for the safety of POSNs as expressed below:

- **Trust relations :** Trusted security mechanisms help to protect social graphs in POSNs. These security mechanisms are needed to protect POSNs and mitigate different kinds of attacks on the formed online social graphs.
- **Attack mitigation :** A cyber attack is a harmful activity performed by the attacker to gain information relevant to the users. The information and privacy are compromised because of such type of attacks. Therefore, attack mitigation schemes over POSNs are required. The attacks can be reduced by applying some authentication and authorization policies along with cryptographic mechanisms.
- **Privacy :** POSNs consist of large information like user's account details, communication messages, information regarding service provider, third-party applications, and advertisers. Users' sharing diversity and specificity of the personal information over POSNs will increase the risk for cyber and physical attacks. Therefore, fine-grained privacy setting is required in POSNs.
- **Identity anonymity :** The identity of users must be hidden from each other during messages exchange. Some pseudonymous-based identity hidden mechanisms are required to hide the original identity of the user. The random identifiers are the best solution for hiding public identity of users.

Despite the above-discussed security requirements, there are certain other security policies that are required to be incorporated in POSNs.

1.5 Technology enablers for POSNs

POSNs aim at connecting users from different platforms of social media through a common interface, which enables the formation of communities. Despite being advantageous for general online social networks, socializing everyone is tedious and requires considerable efforts in devising solutions which can form a common platform for users from different online social networking platforms. Such a requirement makes it difficult for the security providers and demand extensive solutions which can be easily applied to POSNs and at a low cost of operations.

Existing software and technological solutions can help to overcome the security requirements of POSNs without interrupting its services. However, the subsisting technologies should be improvised to particularly target the applications associated with POSNs. An efficient solution not only helps to determine the responsiveness of a user in POSNs but also supports the classification of communities, detection of anomalous users as well as scanning of vulnerabilities and maintenance of security policies, like confidentiality, integrity, authentication, availability. Moreover, these also facilities the mitigation of cyber threats and prevent the POSNs platform from cyber bullies. To further extend the understandings on the existing solutions and technological advancements, a comparison between various technology enablers for POSNs is presented in Table 1.

1.6 Structure of the survey

At first, the survey covered the basics of POSNs and various technology enablers. Section 2 presents a comparison between the proposed and the existing surveys. Section 3 presents the study on the security and its classification for POSNs. Trust management is covered in Section 4 followed by classification of anomaly detection in Section 5. Discussions and open issues are presented in Section 6. Literature classification and categorization are presented in Section 7. Finally, Section 8 concludes the paper.

Table 1: Key technology enablers for security in POSNs.

Security Technology	Property	Advantages
Firewall and anti-virus [45]	Detect threats	Protecting computers and devices against threats such as malware, clickjacking, and phishing attacks
Intrusion prevention security technology [45]	Detect threats	Protections against broader and more sophisticated attack spectrum
Web App Firewalls(WAF) [114]	Protect web applications from web exploits	Control traffic to allow or block web applications
Deception [67]	Create fake vulnerabilities, systems, shares cookies and find the attacker	Suitable for network, application, endpoint, and data
Machine learning security [160]	Find anomalous behavior	Provides protections against advanced persistent threats
Cloud workload protection platforms [103]	Single management console	Applies security policy
Network Traffic Analysis [118] (NTA)	Monitor network traffic, flows, connections	Finds malicious intent
Cloud Access Security Brokers (CASBs) [107]	Single point of control over multiple cloud services	Address gaps
Software-Defined Perimeters (SDPs) [32]	Logical set of disparate, network-connected participants	Hide the public visibility and reducing the surface area for attack
Endpoint Detection and Response (EDR) [81]	EDR tools record numerous endpoint and network events, and store information in the centralized database	Quickly in response
Remote browser [75]	Browser session from a browser server	Detect malware delivered via email, URLs or malicious websites.
User and Entity Behavioural Analytics (UEBA) [1]	User-centric analytics of user behaviour	More accurate and threat detection more effective
DevSecOps [97]	Use scripts, recipes, blueprints, and templates to the underlying the configuration of security infrastructure	Automatic security scanning for vulnerabilities
Intelligence-driven security Operations centre orchestration solutions [154]	Events-based monitoring.	Used to inform every aspect of security operations
Pervasive trust services [71]	Designed to scale and support the needs of devices with limited processing capability	Trust services include secure provisioning, data integrity, confidentiality, device identity and authentication
Blockchain principles to be applied to data security [12]	Blockchain has the potential to be a major leap forward for securing sensitive information	Mitigate the increasing number of cyber threats to data
Data loss prevention [63]	Provides encryption and tokenization	Protect data down to field and subfield level

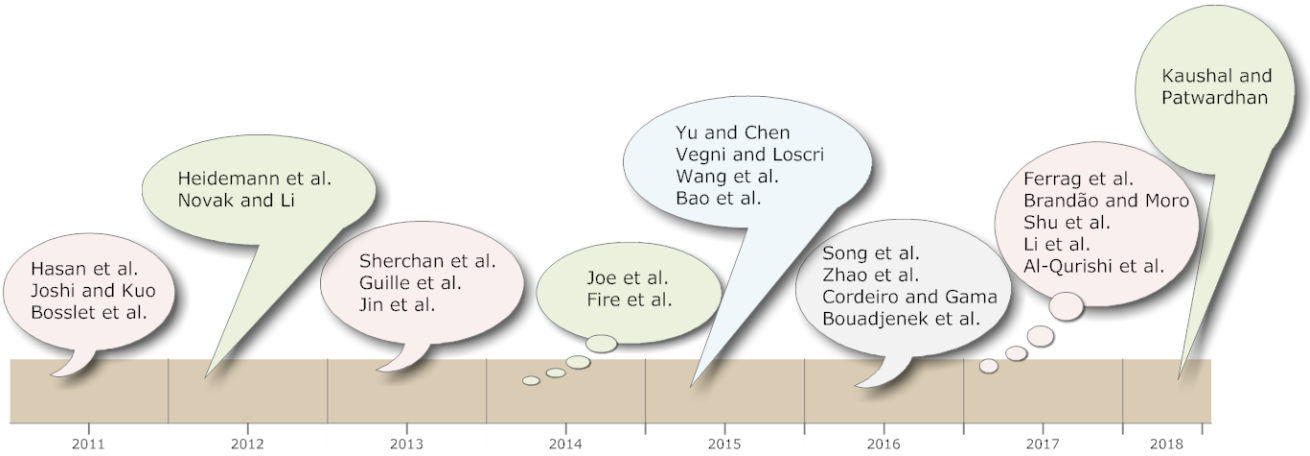

Figure 4: A roadmap of existing surveys and their progressive comparison.

2 Comparison with existing surveys

POSNs aim at providing a reliable platform to make relationships among groups and communities. The emerging effect of POSNs also touches the business market in terms of advertising and dealing.

Many surveys have been conducted to evaluate the challenges and issues of POSNs as highlighted in Figure 4. Some of the surveys fixate to find the trends and the technological enhancement of POSNs. The existing surveys address the problem with the social trends and their impact on the personal and the professional life of users involved in POSNs. Heidemann *et al.* [65] covers functionalities and characteristics of OSNs in their survey. Their survey emphasized emerging trends in OSNs and how advancement takes place with time. The role of OSNs in business perspective is also considered in their survey. Kaushal and Patwardhan [83] focus on the personality trends of users in POSNs. The personality is an attribute or a characteristic of any user and it can be formed on the basis of behavioral, temperamental, emotional, and mental. The authors target the existing approaches and methods for predicting a user's personality and their respective challenges. Their survey shows a tradeoff between the user of POSNs and personality and what linguistic features can be extracted from POSNs to analyze user's profile.

Trust is an important entity for the OSNs. Sherchan *et al.* [142] published a survey on social trust with OSNs. The author considers the information collection of trust, evaluation of the trust, and trust dissemination. Their survey highlights the buildup of social trust systems. Joshi and Kuo [80] presented a survey on the security and privacy issues in OSNs. The authors discussed how privacy is protected in the static and dynamic networks and what techniques exist to follow such a requirement. In the concern of security and privacy of OSNs, Joe and Ramakrishnan [79] presented a survey on various security issues in OSNs. Furthermore, Fire *et al.* [45] discussed the security and privacy risks in OSNs and existing solutions which are used for protection, security, and privacy of OSN users. The authors emphasized the threats of OSNs and the available commercial solutions. Novak and Li [101] presented the survey on the security and privacy issues in OSNs and also presented a review of user data protection mechanisms against malicious attacks. The anonymization and de-anonymization of OSN are also discussed in their survey. Ferrag *et al.* [44] gave a survey on the privacy-preserving schemes for ad-hoc social networks. The models including location privacy, identity privacy, anonymity, traceability, interest privacy, backward privacy, and content-oriented privacy are presented in their survey. In addition, the threats and vulnerabilities are addressed for the mobile social networks (MSNs) and vehicular social networks (VSNs). The challenges of privacy preservation and recommendations for further research are also given in their survey.

Brandão and Moro [19] focused on the social-professional networks. The authors presented the taxonomy for professional networks and their issues. The survey identified relationships among clustering, recommendation and ranking approaches of the social-professional networks. Bouadjenek *et al.* [18] presented the survey on the social information retrieval approaches and platforms for OSNs. The survey included the review of important contributions and their analyses. Al-Qurishi *et al.* [5] published a survey on the Sybil defense techniques in OSNs. The survey focused on the attacks that are possible in OSNs and their defensive schemes and methodologies for prevention. The survey included existing machine learning based solutions like supervised machine learning or unsupervised machine learning to detect Sybil attacks in OSNs. This survey classified all the related schemes based on the methods, datasets, and measurements. The classification of performance measurement and social network datasets of OSNs used in the literature are also given in their survey. A survey in event detection techniques of OSNs is given by Cordeiro and Gama [31]. The challenges faced by OSN in event detection are the main highlight of this survey.

Li *et al.* [90] provided state-of-the-art on link recommendation methods for OSNs. This survey mainly focused on the learning-based methods and proximity-based methods. The authors emphasized the theoretical foundations for link recommendation methods and their future directions. Al Hasan and Zaki [3] gave a survey on the link prediction in OSNs. The authors analyzed existing link prediction models with their strengths and weaknesses in accurately identifying links in OSNs. In the era of link prediction in OSN, Wang *et al.* [164] presented the link prediction techniques and their problems. The link prediction can be obtained by mining and analyzing those helps to find missing links. Their survey mainly focused on the topology-based metrics and learning-based methods for link predictions. The applications and roadmaps are well addressed by the authors.

Bao *et al.* [14] wrote a survey on the recommendations in location-based social networks. The survey focused on data sources and techniques that are used for recommendations. The comparative analysis of the recommender systems is analyzed in their survey. Yu and Chen [179] gave a survey on Point-of-interest (POI) recommendation in location-based social networks. Moreover, POI recommendation in location-based social networks is also discussed by Zhao *et al.* [187]. The survey considers the aspects of POI recommendation, methodologies, and tasks for classification of taxonomies. The contributions and system features are highlighted for each aspect in their survey.

Song *et al.* [147] investigated the cultural variations of different countries with respective of health information on the social networks. The authors mainly focused on the United States, Korea, and Hong Kong. The authors created a hypothesis on the basis of trust and use of experience-based knowledge shared on social Internet sites. Vegni and Loscri [158] gave a survey on the main features of vehicular social networks and the major issues in bridging social networks to vehicular networking are discussed in their article.

Guille *et al.* [57] presented a survey on methods related to information diffusion analysis in OSNs. The authors discussed the challenges related to information diffusion in OSNs and also discussed the alternative approaches for a possible solution. Jin *et al.* [78] wrote a survey on the user behavior in OSNs. The survey discusses the interaction and connectivity of users and analysis of traffic activities. In order to further enhance the understanding of existing works, a comparison is presented in Table 2.

Table 2: A comparison of the proposed survey and the existing surveys on OSNs/POSNs.

Survey	Year	Security	Privacy	Trust	Anomaly detection	OSNs/POSNs
Proposed	2018	✓	✓	✓	✓	POSNs
Kaushal and Patwardhan [83]	2018	✗	✗	✗	✗	OSNs
Al-Qurishi *et al.* [5]	2017	✓	✓	✓	✗	OSNs
Li *et al.* [90]	2017	✗	✗	✓	✗	OSNs
Brandão and Moro [19]	2017	✗	✗	✗	✗	OSNs
Ferrag *et al.* [44]	2017	✓	✓	✓	✓	OSNs
Bouadjenek *et al.* [18]	2016	✗	✓	✓	✗	OSNs
Cordeiro and Gama [31]	2016	✗	✗	✗	✗	OSNs
Zhao *et al.* [187]	2016	✗	✗	✗	✗	OSNs
Song *et al.* [147]	2016	✗	✗	✓	✗	OSNs
Bao *et al.* [14]	2015	✗	✗	✗	✗	OSNs
Wang *et al.* [164]	2015	✗	✗	✗	✗	OSNs
Vegni and Loscri [158]	2015	✓	✓	✓	✗	OSNs
Yu and Chen [179]	2015	✗	✗	✓	✗	OSNs

Continued on next page

Table 2 – continued from previous page

Survey	Year	Security	Privacy	Trust	Anomaly detection	OSNs/POSNs
Fire *et al.* [45]	2014	✓	✓	✓	✓	OSNs
Joe and Ramakrishnan [79]	2014	✓	✓	✗	✓	OSNs
Jin *et al.* [78]	2013	✓	✓	✓	✓	OSNs
Guille *et al.* [57]	2013	✗	✗	✗	✓	OSNs
Sherchan *et al.* [142]	2013	✓	✓	✓	✗	OSNs
Novak and Li [101]	2013	✓	✓	✓	✓	OSNs
Heidemann *et al.* [65]	2012	✓	✓	✓	✗	OSNs
Bosslet *et al.* [17]	2011	✗	✗	✗	✗	OSNs
Joshi and Kuo [80]	2011	✓	✓	✓	✓	OSNs
Al Hasan and Zaki [3]	2011	✗	✗	✗	✗	OSNs

Table 3: State-of-the-art solutions for security enhancement of POSNs.

Approach	Author	Ideology	Application	Parameter	Security	Privacy	Authentication	Encryption	Data Analytic
CenLocShare	[Xiao *et al.* 2017] [173]	Centralized privacy-preserving location-sharing system	mOSNs	Time of location query, Storage space, client interfaces	✓	✓	✗	✓	On-site
UDPLS	[Suno *et al.*2017] [150]	Preserve user's location privacy and network privacy on location server, and preserve user's location privacy on social network server	mOSNs	Computation time,query time	✓	✓	✓	✓	On-site
Safebook	[Antonio Cutillo and Molva 2009] [33]	Cooperation among a number of independent parties	OSNs	Entrypoint registration, data lookup and retrieval	✓	✓	✓	✓	On-site
Secure friend discovery	[Dong *et al.*2011] [38]	Compute social proximity between two users to discover potential friends	mOSNs	CDF of cosine similarity of social coordinates	✓	✓	✓	✓	On-site
SuperNova	[Sharma and Datta 2012] [120]	Heuristics approach on the end user resources and their behaviors	DOSNs	Cumulative availability, system performance	✓	-	✗	✗	-
DECENT	[Jahid *et al.*2012] [74]	Distributed hash table to store user data, and features cryptographic protections	OSNs	Average time to view a newsfeed	✓	✓	✓	✓	Off-site
Protection of PSN	[Yan and Wang 2017] [177]	Two-dimensional trust levels	POSNs	Computational complexity, secret key generation time	✓	✓	✗	✓	-

Continued on next page

Table 3 – continued from previous page

Approach	Author	Ideology	Application	Parameter	Security	Privacy	Authentication	Encryption	Data Analytic
ProGuard	[Zhou *et al.*2017] [190]	Detecting malicious accounts	OSNs	Detection rate, false positive rate, total amount of expenditure	-	-	✗	✗	Off-site
Private data publication	[Zheng *et al.*2018] [188]	Heterogeneous privacy preferences and the correlations among participants	OSNs	Performance for Heterogeneous Users, ratio of the successfully served users	✗	✓	✗	✗	Off-site
NHAD	[Sharma *et al.*2018] [157]	Used paradigms-missing links, reputation gain, significant difference, trust properties, and trust score	OSNs	Detection rate, false postive rate, Accuracy, F-score, precision	✗	✗	✗	✗	On-site
SybilTrap	[Al-Qurishi *et al.*2018] [6]	Graph based supervised learning technique	OSNs	Receiver operating characteris-tic,cumulative distribution function (CDF) of each feature	✗	✗	✗	✗	On-site
lurkers detection	[Amatoi *et al.*2018] [8]	Based on hypergraphs	Heterogeneous OSNs	Loading times, running times	✗	✗	✗	✗	Off-site
Automatic control/block over user comments	[Godse *et al.*2018] [53]	User control system (UCS)	OSNs	Policy, database	✓	✓	✗	✗	-
De-Anonymizing framework	[Su *et al.*2017] [148]	Browsing behaviour	OSNs	De-Anonymizing accuracy	-	-	✗	✗	On-site
Online social network for emergency management	[Roxanne Hiltz and Turoff 2009] [169]	Establishment of global relationships in case of emergency	OSNs	Uses of SNSs for emergency management	✗	✗	✗	✗	-

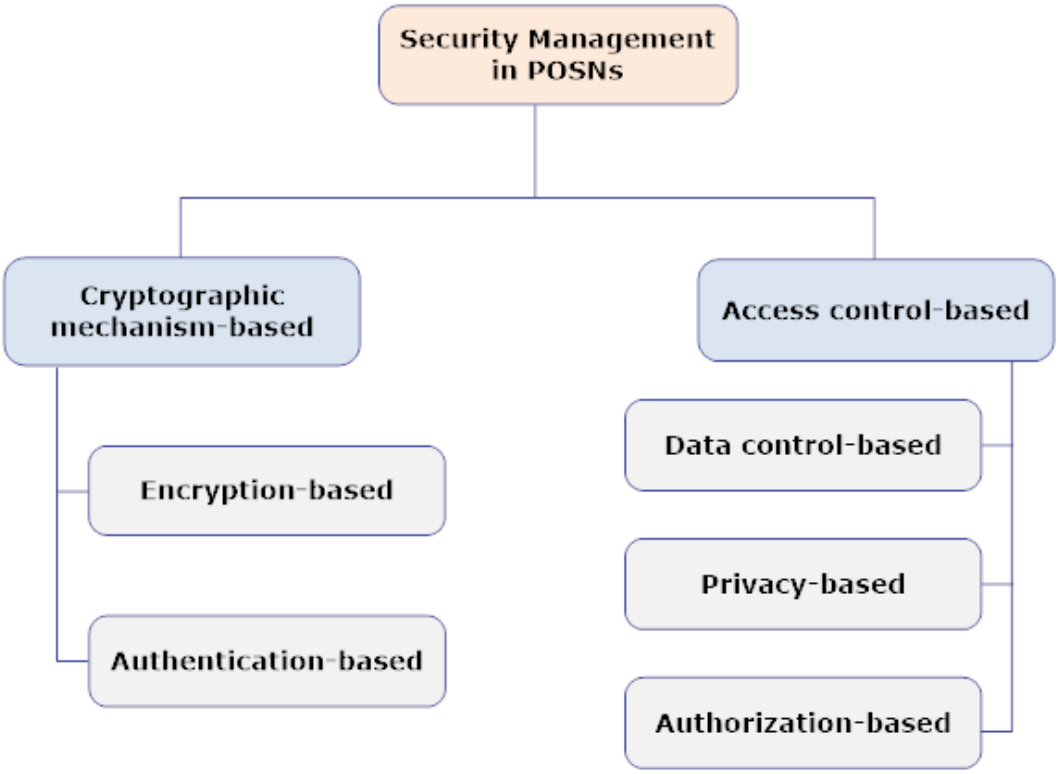

Figure 5: A taxonomy of security solutions for POSNs.

3 Security in POSNs

The users of OSNs, such as Facebook, Twitter, and Google+ are increasing exponentially and so is the possibility of multiple communities in futuristic POSNs. The security of this critical information is required for smooth transmissions in POSNs. The security should be integrated into the user's information and communications. In this survey, the security management is classified into two parts, as shown in Figure 5:

3.1 Cryptographic mechanism-based security

Social media technology mainly uses cryptographic security techniques. Cryptographic techniques are suitable for groups with dynamic memberships [74] [70]. The group is any community or any cluster which shows same properties. The social media problems of security, privacy and anti-piracy can be overcome through cryptographic techniques like authentication, encryption etc.

3.1.1 Encryption-based security

The encryption-based techniques encrypt the location information or all the information of a user. The communication security can be achieved through peer to peer encryption or peer to multi-peer encryption. There are many existing techniques like attribute-based encryption, proxy-based encryption schemes to protect accidental or intentional information leak in POSNs [189] [110].

3.1.2 Authentication-based security

The authentication-based security is achieved by applying authentication protocols among users while sharing their personal information. The authentication is performed mutually either in an individual mode or in a group mode. The authentication schemes provide secure communication and a user-specific data accessibility [92] [172]. The message authentication maintains the integrity in the context of POSNs.

3.2 Access control-based security

The access control based techniques are used for controlling the shared information. The access control provides restriction over unwanted information sharing in the public domain over the social media [30] [155]. The access control can be applied by a user or by a controller, or both in certain situations. The access control based security is further categorized with the attributes as explained below:

3.2.1 Data control-based

Data control refers to the amount of information that is shared among user to maintain anonymity [13]. The data is shared among many communities over different social media. The data leakage leads to the breach of the privacy and the integrity. The access control helps to maintain the integrity by providing limited access to unauthorized users [94].

3.2.2 Privacy-based

The distributed information over social site leads to privacy concerns and requires insights into security problems [131] [186]. The privacy of users provides integrity in the interpersonal relationships and flexibility in POSNs. The privacy based techniques help to preserve the security of private information and prevent data from leakage.

3.2.3 Authorization-based

Authorization is a process of leveraging accessing information by authenticating legitimate users of POSNs. The services are accessible within their role over POSNs. The authorization helps to block the unwanted users from connecting communities or trying to build a relationship with other users [162] [155].

A detailed comparison of existing solutions on the security of POSNs is presented in Table 3.

4 Trust Management in POSNs

Trust has been an important concern for POSNs. POSNs incorporate trust models and algorithms to enhance service qualities, user experiences, and reliability. Trust mechanism of these networks relies on several paradigms like properties, attributes, modes etc. The trust taxonomy, as shown in Figure 6, represents the classification of trust management solutions in the POSNs [136] [157].

4.1 Parameter-based trust management

The trust management relies on several cryptographic techniques which are used to protect information confidentiality and integrity of POSNs. The Trust is achieved by applying trust models and algorithms with a different set of parameters [151] [68]. The parameters are the attributes which are associated with the properties like privacy, identity etc. The parameter based trust management can be further classified into following subcategories.

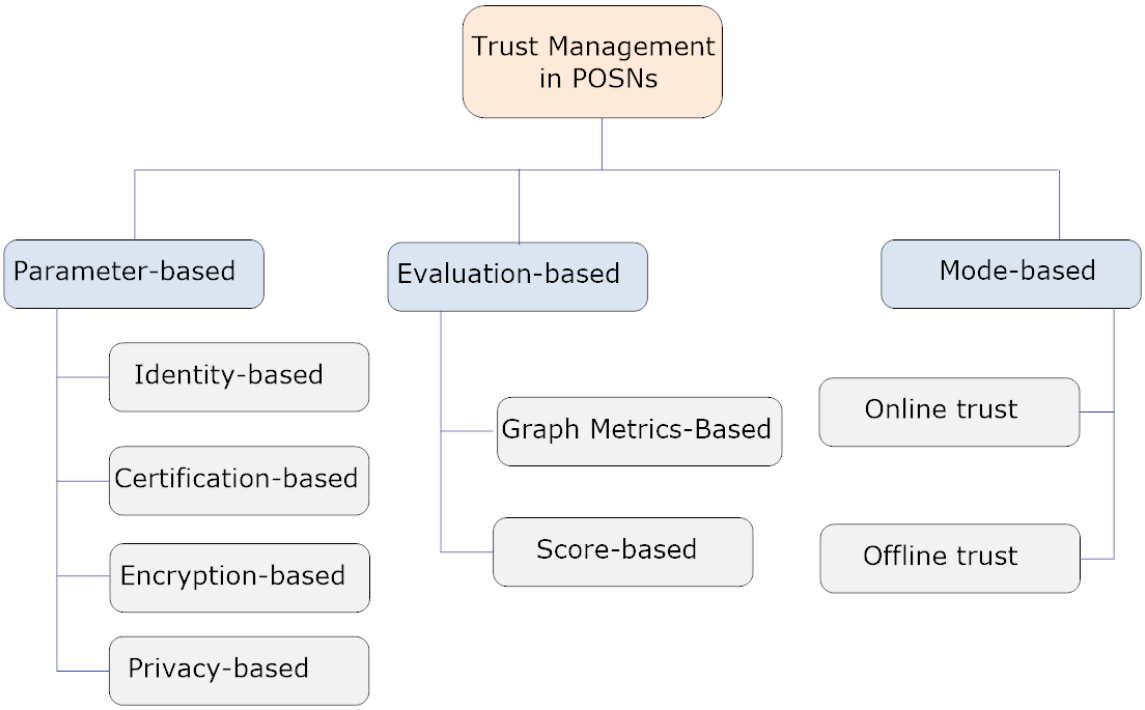

Figure 6: A taxonomy of trust management approaches in POSNs.

4.1.1 Identity-based

The authorization and accounting procedures of the user over POSNs help to construct an Identity-based trust management which supports the transparency of communications and facilitates the agents to establish their reputation [109] [22]. The original Identity of the user is hidden and pseudo-identities are used to enhance the privacy.

4.1.2 Certification-based

The certificates and trusted certification authorities help to build a trust in POSNs by controlling the accessibility of users to services. The certification authorities help to provide central services for automatic public query and for validity checks on self-issued certificates [10] [102].

4.1.3 Encryption-based

The encryption is used to hide the plain text and formulate into a new ciphertext. POSNs contain lots of private conversations and critical information of users [91] [119]. Encryption schemes-Role Based encryption, Homomorphic encryptions, Identity-based encryption, pseudonym-based encryption, attribute-based encryption are used with the POSNs to provide trust for users [156].

4.1.4 Privacy-based

Trust establishment is used as a measure of the perception of security in POSNs. Privacy preservation plays a significant role in trust management. The privacy access controls are established to control the users' information in public domains [109] [116]. These privacy access solutions provide controls based on the data placed on profile pages such as name, pictures, etc.

4.2 Evaluation-based trust management

The interactions among the users rely on trust between the social networks and participants of POSNs. The reputation is usually built on feedback from those who have direct interactions. The reputation-based trust establishment is commonly used mechanism for reliability in POSNs [176] [58] [141]. The trust evolution is relied on following two methods:

4.2.1 Graph metrics-based

In the graph metrics-based trust evaluations, the social networks consider a large graph with many users connected immediately or explicitly to each other. In the graph metrics, the trust value is calculated through a trusted graph [36]. The trust establishment will help enhance the user's experience and the service quality.

4.2.2 Score-based trust

In the score based trust evaluations, the score is calculated for reputation building among users. The rating score is utilized by probability based models that are used for trust establishment [73]. The quantitative trust is helpful to define the trust level over POSNs.

4.3 Mode-based trust management

In the mode-based trust management, the trust establishment is connected to the factor of trust which characterizes the information as well as the users in the online or offline mode of connections [62].

4.3.1 Offline trust

In the offline mode, the trust establishment is performed at the offsite over large data sets which are observed over a long duration of time. Offline trust helps to secure those systems which have a periodic break between their transactions, such as POSN-banking [157] [134].

4.3.2 Online trust

In the online mode, the trust is established on-demand based on the online behaviors and the profiling outcomes such as the adoption of apps, downloads of content, voting, and re-sharing of contents. The online mode contains dynamic adoption of the respective commands used by the users for their accounts or data [157] [134].

A detailed comparison of existing solutions on the trust management in POSNs is presented in Table 4.

Table 4: State-of-the-art solutions for trust management in POSNs.

Approach	Author	Ideology	Application	Parameter	Mechanism	Anomaly Detection	Visualization	Reputation-Formation
User-domain based trusted acquaintance chain discovery algorithm	[Jiang *et al.* 2014] [77]	Trusted graph with the adjustable width breadth-first search algorithms	OSNs	Trust conflict, quality of nodes	Hybrid	✗	✗	✓
Probabilistic recommendation model	[Wang *et al.*2015] [166]	Combining recommendation attributes with inherent similarity	OSNs	Precision, recall, transition probability influence factors	-	✗	✗	✓
Access control scheme	[Pang and Zhang 2015] [104]	Hybrid logic for formulating access control policies	OSNs	Information reliability, relationship hierarchy	Distributed	✗	✓	✓
Consumer perception of knowledge-sharing model	[Bilgihan *et al.*2016] [16]	Structural equation modeling with a sample of travel-related OSN	OSNs	Confirmatory factor analysis	Distributed	✗	✗	✗
Consumers relationship among elements of a brand community Model	[Habibi *et al.*2014] [60]	Based on brand, product, company, and other consumers	OSNs	Internal consistency, discriminant and convergent validity	-	✗	✗	✗
Trust prediction strategy	[Deni Raj and Babu 2017] [112]	Probabilistic reputation features	OSNs	Accuracy comparison,F1 score	-	✗	-	✓
Trustworthiness management	[Nitti *et al.*2014] [99]	Distributed hash table	OSNs	Transaction success rate, dynamic behavior	Distributed	✗	✗	✓
Secure PSN communications scheme	[Yan *et al.*2013] [178]	Multi-dimensional trust levels	OSNs	Security Proofs, communication cost, computation complexity	Distributed	✗	✓	✓

Continued on next page

Table 4 – continued from previous page

Approach	Author	Ideology	Application	Parameter	Mechanism	Anomaly Detection	Visualization	Reputation-Formation
Secure personal data access management scheme	[Yan *et al.* 2014] [175]	Trust level with regard to a concrete context	OSNs	Data confidentiality, computation complexity	Distributed	✗	✗	✓
Anonymous authentication scheme	[Yan *et al.* 2015] [174]	Batch-signature verification	POSNs	Operation time, communication cost	Centralized	✗	✗	-
Secure communication data	[Huang *et al.*2016] [69]	Local trust evaluated by PSN nodes	POSNs	Generation time, operation time	Distributed	✗	✓	✗
Computational Offloading for Efficient Trust Management	[Sharma *et al.*2017] [136]	Osmotic Computing	POSNs	Osmosis time, computational overheads, relation cost	Distributed	✗	✓	✓
Trust evaluation scheme	[Tajbakhsh *et al.*2017] [152]	Three-valued subjective logic (3VSL)	OSNs	Probability of goodness, computational complexity	Distributed	✗	✗	✓

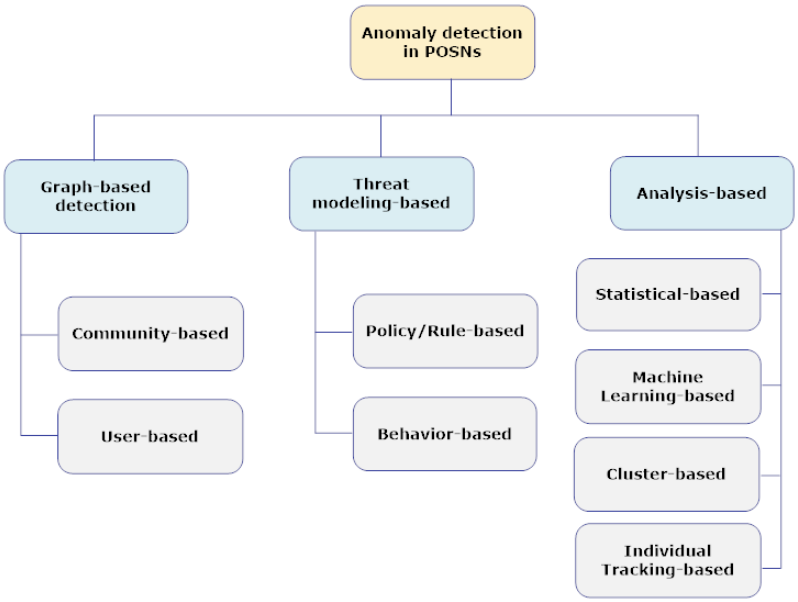

Figure 7: A taxonomy of anomaly detection approaches in POSNs.

5 Anomaly detection in POSNs

The anomalies are the illegal or unwanted behavior in OSNs that show harmful effects on the cross-platform POSNs [159] [136]. Therefore, the solutions against anomaly detection are required in POSNs. The anomalies can be categorized into following parts, as shown in Figure 7:

- **Point Anomalies :** The anomalies over independent data instance is known as point anomalies. For example, in POSNs, the user tries to access a restricted service and leads to different kind of attacks. Such an anomaly is the resultant of an individual's activity [82] [117] [9].
- **Contextual Anomalies :** The anomalies over a specific dataset with a specific context like time, region, etc., are known as contextual anomalies [82] [117] [9].
- **Collective Anomalies :** The anomalies of complete data set is considered as collective anomalies. These anomalies can be detected only when an event occurs in an unexpected order or with an unexpected combination of values or users [82] [117] [9].
- **Horizontal Anomalies :** The anomalies due to the difference in the activity and interaction policies of a user with different sources are categorized as horizontal anomalies. Such anomalies are most difficult and tedious to detect as an error in detection may lead to high values for false positives as well as false negatives [157] [82] [117] [9].

On the basis of nature of data and behavior of users or communities, various anomaly detection techniques can be used to detect an anomaly in POSNs as explained below:

5.1 Graph-based anomaly detection

Some users would have different types of interactions with different communities. Such social relationship among friends can be used to create dependency graph among participants and these graphs can

be used to detect anomalies [100] [2]. These graphs help in finding unexpected behavior or any user or community that shows an abnormal activity. Graph-based anomaly detection can be further categorized into two parts,

5.1.1 Community-based

In such type, the graphs are used to detect abnormal behavior of any community. The dependency graphs are created among communities; therefore, the collected data is large and include many communities [157] [136]. The contextual and collective anomalies in POSNs can be detected through these graphs.

5.1.2 User-based

In this approach, an individual is targeted to detect anomalies. The dependency graph of individual users is used as a data set to find a suspected node or faulty user in the relationships [134].

5.2 Threat-modeling based anomaly detection

The threat is any suspicious or abnormal activity which causes harmful effects or exploits on POSNs. The threat modeling helps to find any type of anomalies in POSNs. The threat modeling is performed with the help of various parameters like behaviors, the flow of information among users, the characteristics of users and communities [96] [55]. Threat-modeling based anomaly detection can be further classified into two types:

5.2.1 Policy/Rule-based

In the policies, the threat modeling is done with the help of characteristics and flow of information over POSNs [165]. The policies or rules decide conditions to find anomalies which show any abnormality over these rules.

5.2.2 Behavior-based

The behavior of user or communities is used as a model for threat detection in POSNs. The threat is considered as bad behavior by users and listed as a bad indicator in the model [121]. When any of the bad behaviors are reflected in the data set, anomalies are detected instantly.

5.3 Analysis based anomaly detection

The information in POSNs is stored in the form of datasets. The anomalies are detected on these datasets with the help of analysis and data mining either by individual or third party operators [7] [184]. Moreover, the analysis can be performed dynamically or statically over the POSN datasets. Analysis based anomaly detection can be broadly classified into following types:

5.3.1 Statistical-based

The simplest approach of data analysis to find an anomaly is statistical analysis. In this type, various common statistical properties of distributions, including mean, median, and mode are used to identify irregularities in data. The statistical analysis based filters are good at anomaly detections but for highly uncertain data sets, these may generate false information [15]. The noise among users is also considered as an abnormal behavior and generated as false anomalies.

Table 5: State-of-the-art anomaly detection solutions for POSNs.

Approach	Author	Ideology	Application	Parameter	Mechanism	Threat Modeling	Recovery
Tension detection approach in online communities	[Burnap *et al.* 2015] [24]	Conversation analysis combined with syntactic and lexicon-based text mining rules	OSNs	Sentiment analysis, machine learning	On-site	✗	✗
Anomaly detection mechanisms	[Garroppo and Niccolini 2018] [50]	Spatial analysis (SA) and time analysis (TA)	Cellular systems	Traffic data and alarms, behaviour, artificial anomalies	On-site	✗	✗
Anomaly detection	[Savage *et al.* 2014] [117]	The selection and calculation of network features, and the classification of observations from this feature space	OSNs	Labelled and unlabelled anomalies	-	✗	✗
OLAIR- behaviors detection	[Wang and Cheng 2005] [163]	Social network analysis	OSNs	SNA indicator, k-core value	Off-site	✗	✗
Utility cloud anomalies detection	[Wang *et al.* 2010] [161]	Metric distributions	OSNs	Baseline methods, entropy time	On-site	✗	✗
Anomaly detection with system feedback	[Horn and Willett 2011] [66]	Filtering and hedging	OSNs	Detection misses, false alarms correct anomalies	On-site	✗	✗
Eigenspace Analysis for threat detection	[Miller *et al.* 2011] [95]	Detection of a threat subgraph	OSNs	Threat detection performance	Off-site	✓	✗
SNAD	[Chen *et al.* 2011] [29]	Assembles the community of users that access a particular subject and assesses if similarities of the community	OSNs	Detection performance	Off-site	✓	✗

Continued on next page

Table 5 – continued from previous page

Approach	Author	Ideology	Application	Parameter	Mechanism	Threat Modeling	Recovery
Link anomaly detection	[Takahashi *et al.*2014] [153]	Sequentially discounting normalized maximum likelihood (SDNML) and with Kleinberg's burst model	OSNs	Dynamic threshold optimization, probability modeling	On-site	✗	✗
Proactive insider threat detection	[Brdiczka *et al.* 2012] [21]	Graph learning and psychological context	Online Games	Personality predictions, network statistics	On-site	✓	✗
iBOAT	[Chen *et al.*2013] [28]	Isolation-based	GPS	Weighting function, anomaly score	Off-site	✗	✗
Rule-based hybrid anomaly detection method	[Hassanzadeh and Nayak 2013] [61]	Graph theory, Fuzzy clustering and Fuzzy rules for modeling user relationships	OSNs	Fuzzy behaviors, graph metrics	Off-site	✗	✗
Anomaly detection method	[Rezaei *et al.*2013] [115]	Structure-based technique	OSNs	Fitting Curve, graph metrics, anomaly score	Off-site	✗	✗
TargetVue: visual analysis system	[Cao *et al.*2016] [26]	Unsupervised learning model-visualizes the behaviors of suspicious users	Online Communication Systems	Relation glyph, Z-glyph, behavior glyph	Off-site	✓	✗
COMPA: Compromised accounts detection method	[Egele *et al.*2017] [39]	Based on a simple observation: social network users develop habits over time, and these habits are fairly stable	OSNs	Behavioral profile stability, False Positives and negative	On-site	✓	✗

Continued on next page

Table 5 – continued from previous page

Approach	Author	Ideology	Application	Parameter	Mechanism	Threat Modeling	Recovery
Voila	[Cao *et al.*2018] [25]	Interactively detecting anomalies in spatiotemporal data collected from a streaming data source	Spatiotemporal data	Ground-truth labeling, baseline methods and evaluation metrics	On-site	✗	✗
COSMOS	[Burnap *et al.*2015] [23]	Hadoop infrastructure	OSNs	Sentiment analysis, social network analysis, hadoop scalability	Off-site	✗	✗
Bayesian anomaly detection methods	[Heard *et al.*2010] [64]	Track the pair wise links of all nodes in the graph to assess normality of behavior	OSNs	Sequential and retrospective analyses	On-site	✗	✗
Bursty keyword detection model	[Guzman and Poblete 2013] [59]	Normalized individual frequency signals per term and a windowing variation technique	OSNs	Stopword analysis, Scalability	Off-site	✗	✗
CatchSync	[Jiang *et al.*2014] [76]	Synchronized behavior and abnormal behavior	OSNs	Detection effectiveness	Off-site	✗	✗

5.3.2 Machine learning-based

The instant anomalies like zero-day attacks or unexploited vulnerabilities are not detected through statistical analysis approaches. Machine learning-based analysis is more effective in such cases. The machine learning approach includes k-nearest neighbors' algorithm, local outlier factor and supervised learning through vector machine approaches. However, the machine learning solutions are quite expensive to maintain because of additional overheads [41] [47].

5.3.3 Cluster-based

The clusters are composed of users and communities with similar properties [20]. On the basis of these common properties, the clusters are created and analyzed for anomaly detections.

5.3.4 Individual tracking-based

The individual group or any user is traced for anomalies detection through this approach [52]. In the individual tracking, every user characteristics are analyzed to obtain any misbehavior in POSNs.

A detailed comparison of existing solutions on the anomaly detection in POSNs is presented in Table 5.

6 Research Challenges and Future Directions

POSNs are in the growing stage as the amalgamation of different OSNs has already started. The rapid growth of such networks causes a considerable impact on the research organizations and demand solutions for different types of issues discussed throughout this article. In order to facilitate the future research, different open issues research challenges are discussed below:

- **Anonymous Authentication :** The possibility of user communication in POSNs needs to judge whether the communication parties are trustworthy or not. The concept of anonymous authenticating supports trust of the involved parties while preserving their privacy in POSNs [43] [49]. It further involves extra computational overheads in terms of operational time and communication costs. The future work should be directed towards the security paradigms of POSNs and should incorporate reliable privacy preservation via trust, anonymity, and unlinkability in the nodes, protect traceability and link predictions through low computational anonymous authentication mechanisms.

- **Inter-vehicular POSNs:** With the advent of vehicular social networks, this field becomes important to cover from POSNs perspective. At the moment, POSNs through vehicular technology has not been studied much and requires some considerable evaluations on demonstrating how V2X can be introduced into the existing setup while showcasing its utility as one of the platforms [133]. Moreover, security aspects are entirely open in this direction of research and it can serve as an important and highly motivated topic for upcoming research. Integration of different technologies like crowdsourcing, the blockchain, osmotic computing, catalytic computing can be performed to use vehicles as one of the nodes in POSNs [42, 111, 132, 135, 138]. In addition, mobility-aware data sharing is also an open issue for inter-vehicular POSNs.

- **Mutual Trust Management :** Trust is considered as an important asset or a property of relationships for networks that help to shape interaction patterns within POSNs. In general, the trust is established among two participants who have direct interactions in a large-scale social network.

Mutual trust is required between the communicating parties to ensure each other and verify the source of information [34, 35, 84, 146]. Different structural and relational properties of users in POSNs need mutual trust amongst its users. The further considerable issues in POSNs include level-wise mutual trust and identification of factors which influence trust.

- **Light-Weight Security :** POSNs contain a wealth of information about its users embedded in the social graph and links. It is important to develop new lightweight cryptographic algorithms which protect the privacy and security of communication between the communities as well as users. The lightweight security requires developing cryptographic algorithms and standards that can work within the confines of a simple POSN network and users [86, 93, 137, 182]. In POSNs, lightweight security algorithm, protocol construction, and implementation are still open issues to resolve.

- **Cross-platform POSNs Management :** POSNs require combined efforts from different platforms to manage its users especially focusing on their security considerations. It is required that low-complex and low-cost solutions should be developed which can facilitate the easier management of multiple platforms of POSNs. Such requirements become severe when the platforms are independent of each other and have the least number of metrics in common [87, 88, 136]. This condition makes it difficult to manage and control the activities of POSNs. Research is required in this direction and it is expected that the developed solutions can be implemented without getting affecting of the cross-platform data exchanges.

- **Secure Recommender Systems:** The recommender systems provide personalized information to users according to their preferences like traveling data, shopping lists, tourism, etc. It is desired that recommender systems which target the audience of POSNs must be secure and should not allow security breaches to prevent manipulation of its users. Recommender systems can be strengthened for data privacy and can use various authentication mechanisms for the end to end security [145] [181].

- **Access Control and Authorization :** The content over POSNs needs to access policies and authorization through permissions. To prevent unwanted access to the content, access control and user-specified policies are required that helps to regulate how a user accesses and controls the information. Some of the future challenges involve multiparty access control in POSNs, relationship-based access controls, and secondary authorizations [85, 105, 124, 125].

- **Resilience to Failures :** Nodes failures are difficult to manage for any kind of networks. However, such an issue becomes critical if the primary node which is an interface between two or more platforms fails. For cross-platform data exchanges in POSNs, it is required that either the system should be made fail-safe, or the network must be checked for a single point of failures [127, 139, 171, 185]. Thus, it is desirable to develop platforms that are resilient to periodic failures.

- **Secure Resource Allocation :** The resources should be efficiently divided amongst POSN users to fulfill the need of an individual without leading to resource-starvations. Owners of the resources must share their computing resources for their friend's circle in a secure manner [122]. At a glance, the distributed resources and infrastructures are shared with the communities in POSNs. Therefore, the secure resource allocation is a considerable challenge to resolve while leveraging the facilities of present solutions. From the research perspective, distributed resource allocations, preference-based resource sharing, and Infrastructure sharing in POSNs need a considerable attention [126, 143, 149].

- **POSNs Survivability :** The survivability of POSNs can be related to its resource allocation and resilience to failures. Accountability of both these factors helps to make POSNs survivable as well

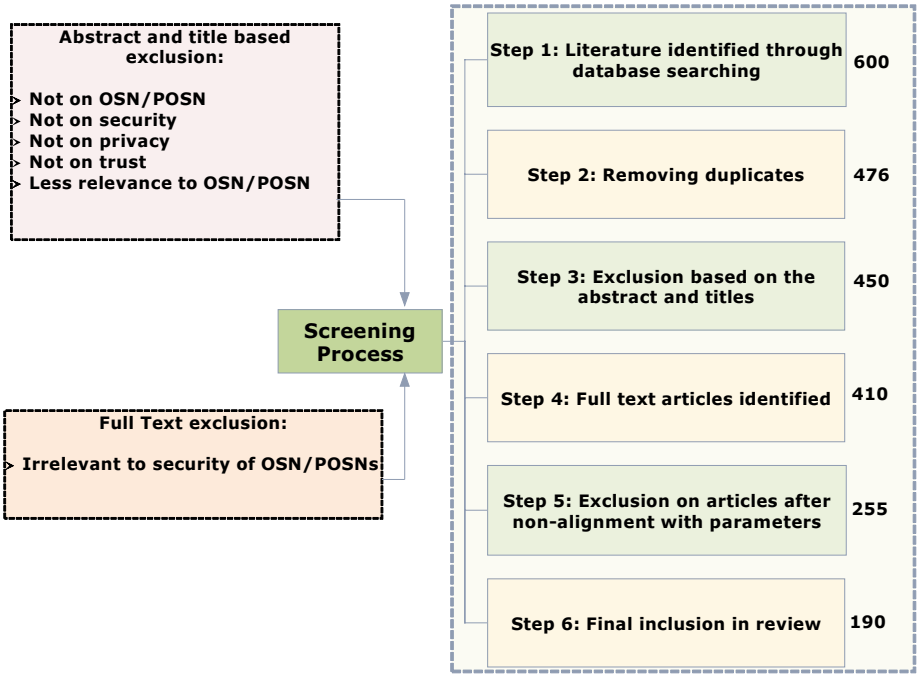

Figure 8: An illustration of the screening strategy opted for this survey.

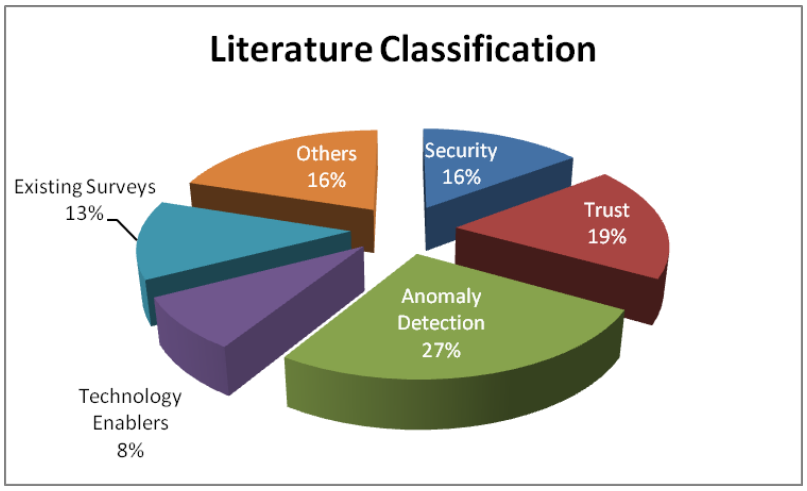

Figure 9: Literature classification for comparative evaluations of 190 articles.

as sustainable irrespective of the functioning conditions and environment [11, 89, 113]. POSNs are focused on supporting a large set of daily activities, thus, it is required that frameworks and middleware should be developed that can ensure the high survivability of POSNs.

7 Literature Classification

The literature was extracted from the online database searches using Google Scholar, IEEE Xplore, ACM Digital libraries, Web of Science directory, Science Direct, university library search, and backtracking the

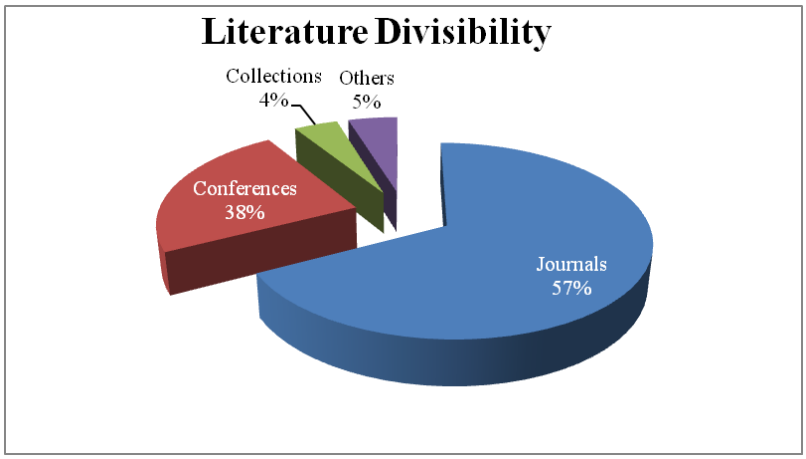

Figure 10: Literature divisibility of 190 articles.

references of existing articles. The procedure followed for identification of relevant material is illustrated in Figure 8. Figures 9 and 10 illustrate the literature classification and divisibility, respectively, for different metrics for a total of 190 articles, which are referred to in this survey.

8 Conclusions

Pervasive Online Social Networks (POSNs) aim at connecting users from different locations, domains, platforms and with different properties of relationships. POSNs focus on cross-platform communications amongst large numbers of users in the form of communities belonging to two or more OSN platforms. Such formations are difficult to handle and security is one of the crucial challenges to tackle for attaining a fully-flexible workflow model for POSNs. At present, there are limited information and contents on the security of POSNs. Irrespective of this, different sets of solutions which emphasize on social networking are studied and a detailed classification is presented for enhancing the knowledge about such solutions. In addition, this survey included content related to trust management and anomaly detection in POSNs. A broad classification is also presented for each category with a tabular comparison. Future challenges, open issues, and research goals are presented to provide a direction of research to the upcoming researchers. A total of 190 articles from different journals, conference-proceedings, and collections are referred with the majority of them focusing on closely related aspects of OSNs and POSNs. The understanding of this literature suggests that although there has been a tremendous amount of works on the security of OSNs, the challenge becomes crucial when cross-platform security is involved which is the dominant aspect of POSNs. Considering this, there is a huge amount of scope and gap that has to be filled with efficient and effective strategies.

References

[1] A. Acquisti, L. Brandimarte, and G. Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, January 2015.

[2] L. Akoglu, H. Tong, and D. Koutra. Graph based anomaly detection and description: a survey. *Data Mining and Knowledge Discovery*, 29(3):626–688, May 2015.

[3] M. Al Hasan and M. J. Zaki. A survey of link prediction in social networks. In C. C. Aggarwal, editor, *Social network data analytics*, pages 243–275. Springer, Boston, MA, 2011.

[4] A. Al Hasib. Threats of online social networks. *IJCSNS International Journal of Computer Science and Network Security*, 9(11):288–93, November 2009.

[5] M. Al-Qurishi, M. Al-Rakhami, A. Alamri, M. Alrubaian, S. M. M. Rahman, and M. S. Hossain. Sybil defense techniques in online social networks: a survey. *IEEE Access*, 5:1200–1219, January 2017.

[6] M. Al-Qurishi, S. M. M. Rahman, A. Alamri, M. A. Mostafa, M. Al-Rubaian, M. S. Hossain, and B. Gupta. Sybiltrap: A graph-based semi-supervised sybil defense scheme for online social networks. *Concurrency and Computation: Practice and Experience*, 30(5):e4276, March 2018.

[7] S. Aljawarneh, M. Aldwairi, and M. B. Yassein. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, 25:152–160, March 2017.

[8] F. Amato, V. Moscato, A. Picariello, F. Piccialli, and G. Sperlí. Centrality in heterogeneous social networks for lurkers detection: An approach based on hypergraphs. *Concurrency and Computation: Practice and Experience*, 30(3):1–12, February 2018.

[9] K. Anand, J. Kumar, and K. Anand. Anomaly detection in online social network: A survey. In *Proc. of the 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT'17), Coimbatore, India*, pages 456–459. IEEE, March 2017.

[10] C. A. Ardagna, R. Asal, E. Damiani, T. Dimitrakos, N. El Ioini, and C. Pahl. Certification-based cloud adaptation. *IEEE Transactions on Services Computing*, pages 1–1, January 2018.

[11] D. Armitage, S. Alexander, M. Andrachuk, S. Berdej, S. Brown, P. Nayak, J. Pittman, and K. Rathwell. Communities, multi-level networks and governance transformations in the coastal commons. *Governing the Coastal Commons: Communities, Resilience and Transformation*, page 231, April 2017.

[12] L. Bahri, B. Carminati, and E. Ferrari. Decentralized privacy preserving services for online social networks. *Online Social Networks and Media*, 6:18–25, June 2018.

[13] L. Bahri, B. Carminati, E. Ferrari, and A. Bianco. Enhanced audit strategies for collaborative and accountable data sharing in social networks. *ACM Transactions on Internet Technology (TOIT)*, 18(4):44, April 2018.

[14] J. Bao, Y. Zheng, D. Wilkie, and M. Mokbel. Recommendations in location-based social networks: a survey. *GeoInformatica*, 19(3):525–565, July 2015.

[15] E. Bigdeli, M. Mohammadi, B. Raahemi, and S. Matwin. A fast and noise resilient cluster-based anomaly detection. *Pattern Analysis and Applications*, 20(1):183–199, February 2017.

[16] A. Bilgihan, A. Barreda, F. Okumus, and K. Nusair. Consumer perception of knowledge-sharing in travel-related online social networks. *Tourism Management*, 52:287–296, February 2016.

[17] G. T. Bosslet, A. M. Torke, S. E. Hickman, C. L. Terry, and P. R. Helft. The patient–doctor relationship and online social networks: results of a national survey. *Journal of general internal medicine*, 26(10):1168–1174, October 2011.

[18] M. R. Bouadjenek, H. Hacid, and M. Bouzeghoub. Social networks and information retrieval, how are they converging? a survey, a taxonomy and an analysis of social information retrieval approaches and platforms. *Information Systems*, 56:1–18, March 2016.

[19] M. A. Brandão and M. M. Moro. Social professional networks: A survey and taxonomy. *Computer Communications*, 100:20–31, March 2017.

[20] A. Brandsæter, E. Vanem, and I. K. Glad. Cluster based anomaly detection with applications in the maritime industry. In *Proc. of the 2017 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC'17), Shanghai, China*, pages 328–333. IEEE, August 2017.

[21] O. Brdiczka, J. Liu, B. Price, J. Shen, A. Patil, R. Chow, E. Bart, and N. Ducheneaut. Proactive insider threat detection through graph learning and psychological context. In *Proc. of the 2012 IEEE Symposium on Security and Privacy Workshops (SPW'12), San Francisco, CA, USA*, pages 142–149. IEEE, May 2012.

[22] C. Burmann, N.-M. Riley, T. Halaszovich, and M. Schade. The concept of identity-based brand management. In *Identity-Based Brand Management*, pages 17–90. Springer Gabler, Wiesbaden, 2017.

[23] P. Burnap, O. Rana, M. Williams, W. Housley, A. Edwards, J. Morgan, L. Sloan, and J. Conejero. Cosmos: Towards an integrated and scalable service for analysing social media on demand. *International Journal of Parallel, Emergent and Distributed Systems*, 30(2):80–100, March 2015.

[24] P. Burnap, O. F. Rana, N. Avis, M. Williams, W. Housley, A. Edwards, J. Morgan, and L. Sloan. Detecting tension in online communities with computational twitter analysis. *Technological Forecasting and Social Change*, 95:96–108, June 2015.

[25] N. Cao, C. Lin, Q. Zhu, Y.-R. Lin, X. Teng, and X. Wen. Voila: Visual anomaly detection and monitoring with streaming spatiotemporal data. *IEEE transactions on visualization and computer graphics*, 24(1):23–33, January 2018.

[26] N. Cao, C. Shi, S. Lin, J. Lu, Y.-R. Lin, and C.-Y. Lin. Targetvue: Visual analysis of anomalous user behaviors in online communication systems. *IEEE transactions on visualization and computer graphics*, 22(1):280–289, January 2016.

[27] J. Carter, E. Bitting, and A. A. Ghorbani. Reputation formalization for an information–sharing multi–agent system. *Computational Intelligence*, 18(4):515–534, November 2002.

[28] C. Chen, D. Zhang, P. S. Castro, N. Li, L. Sun, S. Li, and Z. Wang. iboat: Isolation-based online anomalous trajectory detection. *IEEE Transactions on Intelligent Transportation Systems*, 14(2):806–818, June 2013.

[29] Y. Chen, S. Nyemba, W. Zhang, and B. Malin. Leveraging social networks to detect anomalous insider actions in collaborative environments. In *Proc. of the 2011 IEEE International Conference on Intelligence and Security Informatics (ISI'11), Beijing, China*, pages 119–124. IEEE, July 2011.

[30] Y. Cheng, J. Park, and R. Sandhu. Relationship-based access control for online social networks: Beyond user-to-user relationships. In *Proc. of the 2012 International Confernece on Social Computing (SocialCom'12) and Privacy, Security, Risk and Trust (PASSAT'12), Amsterdam, Netherlands*, pages 646–655. IEEE, January 2012.

[31] M. Cordeiro and J. Gama. Online social networks event detection: a survey. In S. Michaelis, N. Piatkowski, and M. Stolpe, editors, *Solving Large Scale Learning Tasks. Challenges and Algorithms*, volume 9580 of *Lecture Notes in Computer Science*, pages 1–41. Springer, Cham, 2016.

[32] L. Cui, H. Hu, S. Yu, Q. Yan, Z. Ming, Z. Wen, and N. Lu. Ddse: A novel evolutionary algorithm based on degree-descending search strategy for influence maximization in social networks. *Journal of Network and Computer Applications*, 103:119–130, February 2018.

[33] L. A. Cutillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine*, 47(12), December 2009.

[34] P. De Meo, F. Messina, D. Rosaci, and G. M. Sarné. Combining trust and skills evaluation to form e-learning classes in online social networks. *Information Sciences*, 405:107–122, September 2017.

[35] P. De Meo, F. Messina, D. Rosaci, and G. M. Sarné. Forming time-stable homogeneous groups into online social networks. *Information Sciences*, 414:117–132, November 2017.

[36] A. De Salve, B. Guidi, L. Ricci, and P. Mori. Discovering homophily in online social networks. *Mobile Networks and Applications*, pages 1–12, May 2018.

[37] E. Dincelli and S. Goel. Can privacy and security be friends? a cultural framework to differentiate security and privacy behaviors on online social networks. In *Proc. of the 50th Hawaii International Conference on System Sciences (HICSS'17), Waikoloa Village, Hawaii, USA*. AIS Electronic Library (AISeL), January 2017.

[38] W. Dong, V. Dave, L. Qiu, and Y. Zhang. Secure friend discovery in mobile social networks. In *Proc. of IEEE INFOCOM 2011, Shanghai, China*, pages 1647–1655. IEEE, April 2011.

[39] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna. Towards detecting compromised accounts on social networks. *IEEE Transactions on Dependable and Secure Computing*, 14(4):447–460, July 2017.

[40] N. B. Ellison, C. Steinfield, and C. Lampe. The benefits of facebook "friends:" social capital and college students' use of online social network sites. *Journal of computer-mediated communication*, 12(4):1143–1168, July 2007.

[41] A. Faigon, K. Narayanaswamy, J. Tambuluri, R. Ithal, S. Malmskog, and A. Kulkarni. Machine learning based anomaly detection, December 2017. US Patent App. 15/256,483.

[42] R. Fantacci, E. Dei, and F. Chiti. Bio-communities communications paradigms for vehicular social networks. In P. Cong-Vinh, editor, *Nature-Inspired Networking*, pages 55–72. CRC Press, 2018.

[43] M. S. Farash, S. A. Chaudhry, M. Heydari, S. Sadough, S. Mohammad, S. Kumari, and M. K. Khan. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable

security. *International Journal of Communication Systems*, 30(4), March 2017.

[44] M. A. Ferrag, L. Maglaras, and A. Ahmim. Privacy-preserving schemes for ad hoc social networks: A survey. *IEEE Communications Surveys & Tutorials*, 19(4):3015–3045, January 2017.

[45] M. Fire, R. Goldschmidt, and Y. Elovici. Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, 16(4):2019–2036, January 2014.

[46] A. B. Forouzan. *Data communications & networking (sie)*. Tata McGraw-Hill Education, 2006.

[47] C.-z. Gao, Q. Cheng, X. Li, and S.-b. Xia. Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network. *Cluster Computing*, pages 1–9, February 2018.

[48] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen. Security issues in online social networks. *IEEE Internet Computing*, 15(4):56–63, July 2011.

[49] T. Gao, X. Deng, and N. Guo. An anonymous authentication scheme based on group ibs for pmipv6 network. In *Proc. of the 2017 International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'17), Torino, Italy*, volume 612 of *Advances in Intelligent Systems and Computing*, pages 330–341. Springer, Cham, July 2017.

[50] R. G. Garroppo and S. Niccolini. Anomaly detection mechanisms to find social events using cellular traffic data. *Computer Communications*, 116:240–252, January 2018.

[51] M. Gavrilova, F. Ahmed, S. Azam, P. Paul, W. Rahman, M. Sultana, and F. Zohra. Emerging trends in security system design using the concept of social behavioural biometrics. In I. M. Alsmadi, G. Karabatis, and A. Aleroud, editors, *Information Fusion for Cyber-Security Analytics*, volume 691 of *Studies in Computational Intelligence*, pages 229–251. Springer, Cham, 2017.

[52] D. F. Glas, K. Wada, M. Shiomi, T. Kanda, H. Ishiguro, and N. Hagita. Personal greetings: Personalizing robot utterances based on novelty of observed behavior. *International Journal of Social Robotics*, 9(2):181–198, April 2017.

[53] A. R. Godse, S. B. Nemade, P. S. Patil, B. P. Rane, and B. Student. Automatic control/block over user comments on online social network. *International Journal of Engineering Science*, 2018:16105–16108, February 2018.

[54] R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *Proc. of the 2005 ACM workshop on Privacy in the electronic society, Alexandria, VA, USA*, pages 71–80. ACM, November 2005.

[55] R. L. Grossman, K. B. Alexander, J. E. Heath, and R. L. Garrett. Simulation and virtual reality based cyber behavioral systems, March 2018. US Patent 9,910,993.

[56] J. Guan, V. Sharma, I. You, and M. Atiquzzaman. Extension of mih to support fpmipv6 for optimized heterogeneous handover. *arXiv preprint arXiv:1705.09835*, 2017.

[57] A. Guille, H. Hacid, C. Favre, and D. A. Zighed. Information diffusion in online social networks: A survey. *ACM Sigmod Record*, 42(2):17–28, June 2013.

[58] J. Guo, J. Ma, and T. Wan. A mutual evaluation based trust management method for wireless sensor networks. *Chinese Journal of Electronics*, 26(2):407–415, March 2017.

[59] J. Guzman and B. Poblete. On-line relevant anomaly detection in the twitter stream: an efficient bursty keyword detection model. In *Proc. of the 2013 ACM SIGKDD Workshop on Outlier Detection and Description (ODD'13), Chicago, IL, USA*, pages 31–39. ACM, August 2013.

[60] M. R. Habibi, M. Laroche, and M.-O. Richard. The roles of brand community and community engagement in building brand trust on social media. *Computers in Human Behavior*, 37:152–161, August 2014.

[61] R. Hassanzadeh and R. Nayak. A rule-based hybrid method for anomaly detection in online-social-network graphs. In *Proc. of the 25th International Conference on Tools with Artificial Intelligence (ICTAI'13), Herndon, VA, USA*, pages 351–357. IEEE, November 2013.

[62] Y. He, G. Zhang, J. Wu, and Q. Li. Understanding a prospective approach to designing malicious social bots. *Security and Communication Networks*, 9(13):2157–2172, September 2016.

[63] Z. He, Z. Cai, and J. Yu. Latent-data privacy preserving with customized data utility for social network data. *IEEE Transactions on Vehicular Technology*, 67(1):665–673, January 2018.

[64] N. A. Heard, D. J. Weston, K. Platanioti, and D. J. Hand. Bayesian anomaly detection methods for social

networks. *The Annals of Applied Statistics*, pages 645–662, June 2010.

[65] J. Heidemann, M. Klier, and F. Probst. Online social networks: A survey of a global phenomenon. *Computer Networks*, 56(18):3866–3878, December 2012.

[66] C. Horn and R. Willett. Online anomaly detection with expert system feedback in social networks. In *Proc. of the 2011 International Conference on Acoustics, Speech and Signal Processing (ICASSP'11), Prague, Czech Republic*, pages 1936–1939. IEEE, May 2011.

[67] B. Howard. Analyzing online social networks. *Communications of the ACM*, 51(11):14–16, November 2008.

[68] M.-H. Hsu, T. L. Ju, C.-H. Yen, and C.-M. Chang. Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International journal of human-computer studies*, 65(2):153–169, February 2007.

[69] C. Huang, Z. Yan, N. Li, and M. Wang. Secure pervasive social communications based on trust in a distributed way. *IEEE Access*, 4:9225–9238, 2016.

[70] R. Hussain, J. Son, D. Kim, M. Nogueira, H. Oh, A. O. Tokuta, and J. Seo. Pbf: A new privacy-aware billing framework for online electric vehicles with bidirectional auditability. *Wireless Communications and Mobile Computing*, 2017, October 2017.

[71] P. Ifinedo. Applying uses and gratifications theory and social influence processes to understand students' pervasive adoption of social networking sites: Perspectives from the americas. *International Journal of Information Management*, 36(2):192–206, April 2016.

[72] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu. Reverse social engineering attacks in online social networks. In *Proc. of the 2011 International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA'11), Amsterdam, The Netherlands*, volume 6739 of *Lecture Notes in Computer Science*, pages 55–74. Springer, Berlin, Heidelberg, July 2011.

[73] F. Jabeen, Z. Hamid, W. Abdul, S. Ghouzali, A. Khan, S. U. R. Malik, M. S. Khan, and S. Nawaz. Anonymity-preserving reputation management system for health sector. *PloS one*, 13(4):e0195021, April 2018.

[74] S. Jahid, S. Nilizadeh, P. Mittal, N. Borisov, and A. Kapadia. Decent: A decentralized architecture for enforcing privacy in online social networks. In *Proc. of the 2012 International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops'12), Lugano, Switzerland*, pages 326–332. IEEE, March 2012.

[75] G. Jakobson. Collaborative web browsing system integrated with social networks, July 2014. US Patent 8,769,004.

[76] M. Jiang, P. Cui, A. Beutel, C. Faloutsos, and S. Yang. Detecting suspicious following behavior in multimillion-node social networks. In *Proc. of the 23rd International Conference on World Wide Web, Seoul, Korea*, pages 305–306. ACM, April 2014.

[77] W. Jiang, G. Wang, and J. Wu. Generating trusted graphs for trust evaluation in online social networks. *Future generation computer systems*, 31:48–58, February 2014.

[78] L. Jin, Y. Chen, T. Wang, P. Hui, and A. V. Vasilakos. Understanding user behavior in online social networks: A survey. *IEEE Communications Magazine*, 51(9):144–150, September 2013.

[79] M. M. Joe and D. B. Ramakrishnan. A survey of various security issues in online social networks. *International Journal of Computer Networks and Applications*, 1(1):11–14, November 2014.

[80] P. Joshi and C.-C. J. Kuo. Security and privacy in online social networks: A survey. In *Proc. of the 2011 International Conference on Multimedia and Expo (ICME'11), Barcelona, Spain*, pages 1–6. IEEE, July 2011.

[81] B. Karamani. Improving data loss prevention using classification. In *Advances in Internet, Proc. of the 6th International Conference on Emerging Internetworking, Data & Web Technologies (EIDWT'18), Tirana, Albania*, volume 17 of *Lecture Notes on Data Engineering and Communications Technologies*, pages 183–189. Springer, Cham, 2018.

[82] R. Kaur and S. Singh. A survey of data mining and social network analysis based anomaly detection techniques. *Egyptian informatics journal*, 17(2):199–216, July 2016.

[83] V. Kaushal and M. Patwardhan. Emerging trends in personality identification using online social net-

works—a literature survey. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 12(2):15, January 2018.

[84] I. Kotenko, I. Saenko, and A. Kushnerevich. Parallel big data processing system for security monitoring in internet of things networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 8(4):60–74, December 2017.

[85] T. M. Levergood, L. C. Stewart, S. J. Morris, A. C. Payne, and G. W. Treese. Internet server access control and monitoring systems, February 2018. US Patent 9,900,305.

[86] G. Li, H. Zhou, G. Li, and B. Feng. Application-aware and dynamic security function chaining for mobile networks. *Journal of Internet Services and Information Security (JISIS)*, 7(4):21–34, November 2017.

[87] J. Li, J. Li, D. Xie, and Z. Cai. Secure auditing and deduplicating data in cloud. *IEEE Transactions on Computers*, 65(8):2386–2396, August 2016.

[88] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen. Privacy-preserving outsourced classification in cloud computing. *Cluster Computing*, pages 1–10, April 2017.

[89] X. Li, B. Guo, S. Yin, S. Huang, X. Zhang, P. Yu, and P. Wu. Improving the survivability of elastic optical datacenter networks for cloud services with joint spectrum and storage resource backup. In *Proc. of the 2017 Opto-Electronics and Communications Conference (OECC'17) and Photonics Global Conference (PGC'17), Singapore, Singapore*, pages 1–5. IEEE, July 2017.

[90] Z. L. Li, X. Fang, and O. R. L. Sheng. A survey of link recommendation for social networks: Methods, theoretical foundations, and future research directions. *ACM Transactions on Management Information Systems (TMIS)*, 9(1):1, October 2017.

[91] J. Lotspiech, S. Nusser, and F. Pestoni. Anonymous trust: Digital rights management using broadcast encryption. *Proceedings of the IEEE*, 92(6):898–909, June 2004.

[92] C.-G. Ma, D. Wang, and S.-D. Zhao. Security flaws in two improved remote user authentication schemes using smart cards. *International Journal of Communication Systems*, 27(10):2215–2227, October 2014.

[93] X. Ma, J. Ma, H. Li, Q. Jiang, and S. Gao. Armor: A trust-based privacy-preserving framework for decentralized friend recommendation in online social networks. *Future Generation Computer Systems*, 79:82–94, Feburary 2018.

[94] A. Masoumzadeh. Security analysis of relationship-based access control policies. In *Proc. of the 8th ACM Conference on Data and Application Security and Privacy (CODASPY'18), Tempe, AZ, USA*, pages 186–195. ACM, March 2018.

[95] B. A. Miller, M. S. Beard, and N. T. Bliss. Eigenspace analysis for threat detection in social networks. In *Proc. of the 14th International Conference on Information Fusion (FUSION'11), Chicago, IL, USA*, pages 1–7. IEEE, August 2011.

[96] S. Myagmar, A. J. Lee, and W. Yurcik. Threat modeling as a basis for security requirements. In *Proc. of the 3rd Symposium on requirements engineering for information security (SREIS'05), La Sorbonne, France*, volume 2005, pages 1–8. IEEE, August-September 2005.

[97] H. Myrbakken and R. Colomo-Palacios. Devsecops: A multivocal literature review. In *Proc. of the 2017 International Conference on Software Process Improvement and Capability Determination (SPICE'17), Palma de Mallorca, Spain*, volume 770 of *Communications in Computer and Information Science*, pages 17–29. Springer, Cham, October 2017.

[98] M. Nakhjiri and M. Nakhjiri. *AAA and network security for mobile access: radius, diameter, EAP, PKI and IP mobility*. John Wiley & Sons, 2005.

[99] M. Nitti, R. Girau, and L. Atzori. Trustworthiness management in the social internet of things. *IEEE Transactions on knowledge and data engineering*, 26(5):1253–1266, May 2014.

[100] C. C. Noble and D. J. Cook. Graph-based anomaly detection. In *Proc. of the 9th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'03), Washington, DC, USA*, pages 631–636. ACM, March 2003.

[101] E. Novak and Q. Li. A survey of security and privacy in online social networks. *College of William and Mary Computer Science Technical Report*, pages 1–32, 2012.

[102] M. Omar, Y. Challal, and A. Bouabdallah. Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. *Journal of Network and Computer Applications*, 35(1):268–286, January 2012.

[103] G. Pallis, D. Zeinalipour-Yazti, and M. D. Dikaiakos. Online social networks: status and trends. In A. Vakali and L. C. Jain, editors, *New Directions in Web Data Management 1*, volume 331 of *Studies in Computational Intelligence*, pages 213–234. Springer, Berlin, Heidelberg, 2011.

[104] J. Pang and Y. Zhang. A new access control scheme for facebook-style social networks. *Computers & Security*, 54:44–59, October 2015.

[105] J. S. Park. Role-based access control to computing resources in an inter-organizational community, September 2017. US Patent 9,769,177.

[106] T. D. P. Perera, D. N. K. Jayakody, S. Chatzinotas, and V. Sharma. Wireless information and power transfer: Issues, advances, and challenges. In *Proc. of the 86th Vehicular Technology Conference (VTC-Fall'17), Toronto, ON, Canada*, pages 1–7. IEEE, September 2017.

[107] T. Poell and J. van Dijck. Social media and new protest movements. *SAGE Handbook of Social Media*, 2018:1–17, December 2017.

[108] J. Preece and D. Maloney-Krichmar. Online communities: Design, theory, and practice. *Journal of Computer-Mediated Communication*, 10(4):JCMC10410, July 2005.

[109] U. S. Premarathne, I. Khalil, Z. Tari, and A. Zomaya. Cloud-based utility service framework for trust negotiations using federated identity management. *IEEE Transactions on Cloud Computing*, 5(2):290–302, April 2017.

[110] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, and H. Zhao. Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. *Future Generation Computer Systems*, 80:421–429, March 2018.

[111] A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, and S. K. Das. Vehicular social networks: A survey. *Pervasive and Mobile Computing*, 43:96–113, December 2017.

[112] E. D. Raj and L. D. Babu. An enhanced trust prediction strategy for online social networks using probabilistic reputation features. *Neurocomputing*, 219:412–421, January 2017.

[113] A. Rajaram, D. N. K. Jayakody, K. Srinivasan, B. Chen, and V. Sharma. Opportunistic-harvesting: Rf wireless power transfer scheme for multiple access relays system. *IEEE Access*, 5:16084–16099, August 2017.

[114] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood. Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In *Proc. of the 11th International Symposium on Autonomous Decentralized Systems (ISADS'13), Mexico City, Mexico*, pages 1–6. IEEE, March 2013.

[115] A. Rezaei, Z. M. Kasirun, V. A. Rohani, and T. Khodadadi. Anomaly detection in online social networks using structure-based technique. In *Proc. of the 8th International Conference for Internet Technology and Secured Transactions (ICITST'13), London , UK*, pages 619–622. IEEE, December 2013.

[116] P. Ruotsalainen. Chapter 5 – privacy, trust and security in two-sided markets. In V. Vimarlund, editor, *E-Health Two-Sided Markets*, pages 65–89. Elsevier, 2017.

[117] D. Savage, X. Zhang, X. Yu, P. Chou, and Q. Wang. Anomaly detection in online social networks. *Social Networks*, 39:62–70, October 2014.

[118] A. M. Shalita, I. Kabiljo, K. Lau, A. D. Sharma, and A. M. Laslavic. Routing network traffic based on social information, January 2018. US Patent 9,860,316.

[119] W. Shang, Z. Wang, A. Afanasyev, J. Burke, and L. Zhang. Breaking out of the cloud: local trust management and rendezvous in named data networking of things. In *Proc. of the 2nd International Conference on Internet-of-Things Design and Implementation (IoTDI'17), Pittsburgh, PA, USA*, pages 3–14. IEEE, April 2017.

[120] R. Sharma and A. Datta. Supernova: Super-peers based architecture for decentralized online social networks. In *Proc. of the 4th International Conference on Communication Systems and Networks (COMSNETS'12), Bangalore, India*, pages 1–10. IEEE, January 2012.

[121] V. Sharma, H.-C. Chen, and R. Kumar. Driver behaviour detection and vehicle rating using multi-uav coordinated vehicular networks. *Journal of Computer and System Sciences*, 86:3–32, June 2017.

[122] V. Sharma, G. Choudhary, I. You, J. D. Lim, and J. N. Kim. Self-enforcing game theory-based resource allocation for lorawan assisted public safety communications. *Journal of Internet Technology*, 19(2):515–530, March 2018.

[123] V. Sharma, J. Kim, S. Kwon, I. You, K. Lee, and K. Yim. A framework for mitigating zero-day attacks in iot. *arXiv preprint arXiv:1804.05549*, 2018.

[124] V. Sharma, J. Kim, S. Kwon, I. You, and F.-Y. Leu. Fuzzy-based protocol for secure remote diagnosis of iot devices in 5g networks. In *Proc. of the 3rd EAI International Conference on IoT as a Service (IoTaaS 2017), Taichung, Taiwan*, volume 3, pages 1–6. EAI, September 2017.

[125] V. Sharma, J. Kim, S. Kwon, I. You, and F.-Y. Leu. An overview of 802.21a-2012 and its incorporation into iot-fog networks using osmotic framework. In *Proc. of the 3rd EAI International Conference on IoT as a Service (IoTaaS'17), Taichung, Taiwan*, volume 3, pages 1–6. EAI, September 2017.

[126] V. Sharma, R. Kumar, and R. Kaur. Uav-assisted content-based sensor search in iots. *Electronics Letters*, 53(11):724–726, April 2017.

[127] V. Sharma, R. Kumar, and P. S. Rana. Self-healing neural model for stabilization against failures over networked uavs. *IEEE Communications Letters*, 19(11):2013–2016, November 2015.

[128] V. Sharma, K. Lee, S. Kwon, J. Kim, H. Park, K. Yim, and S.-Y. Lee. A consensus framework for reliability and mitigation of zero-day attacks in iot. *Security and Communication Networks*, 2017, November 2017.

[129] V. Sharma, J. D. Lim, J. N. Kim, and I. You. Saca: Self-aware communication architecture for iot using mobile fog servers. *Mobile Information Systems*, 2017, April 2017.

[130] V. Sharma, K. Srinivasan, D. N. K. Jayakody, O. Rana, and R. Kumar. Managing service-heterogeneity using osmotic computing. *arXiv preprint arXiv:1704.04213*, 2017.

[131] V. Sharma, I. You, D. N. K. Jayakody, and M. Atiquzzaman. Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social internet of things. *Future Generation Computer Systems, https://doi.org/10.1016/j.future.2017.12.039*, December 2017.

[132] V. Sharma, I. You, and G. Kul. Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain. In *Proc. of the 2017 ACM CCS Workshop on Managing Insider Security Threats (MIST'17), Dallas, Texas, USA*, pages 81–84. ACM, October 2017.

[133] V. Sharma, I. You, and R. Kumar. Energy efficient data dissemination in multi-uav coordinated wireless sensor networks. *Mobile Information Systems*, 2016, May 2016.

[134] V. Sharma, I. You, and R. Kumar. Isma: Intelligent sensing model for anomalies detection in cross platform osns with a case study on iot. *IEEE Access*, 5:3284–3301, March 2017.

[135] V. Sharma, I. You, and R. Kumar. Resource-based mobility management for video users in 5g using catalytic computing. *Computer Communications*, 118:120–139, March 2018.

[136] V. Sharma, I. You, R. Kumar, and P. Kim. Computational offloading for efficient trust management in pervasive online social networks using osmotic computing. *IEEE Access*, 5:5084–5103, March 2017.

[137] V. Sharma, I. You, F.-Y. Leu, and M. Atiquzzaman. Secure and efficient protocol for fast handover in 5g mobile xhaul networks. *Journal of Network and Computer Applications*, 102:38–57, January 2018.

[138] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li. Secure and energy-efficient handover in fog networks using blockchain-based dmm. *IEEE Communications Magazine*, 56(5):22–31, May 2018.

[139] V. Sharma, I. You, G. Pau, M. Collotta, J. D. Lim, and J. N. Kim. Lorawan-based energy-efficient surveillance by drones for intelligent transportation systems. *Energies*, 11(3):573, March 2018.

[140] S. Shehnepoor, M. Salehi, R. Farahbakhsh, and N. Crespi. Netspam: A network-based spam detection framework for reviews in online social media. *IEEE Transactions on Information Forensics and Security*, 12(7):1585–1595, July 2017.

[141] J. Shen, C. Wang, A. Castiglione, D. Liu, and C. Esposito. Trustworthiness evaluation-based routing protocol for incompletely predictable vehicular ad hoc networks. *IEEE Transactions on Big Data*, June 2017.

[142] W. Sherchan, S. Nepal, and C. Paris. A survey of trust in social networks. *ACM Computing Surveys (CSUR)*, 45(4):47, August 2013.

[143] D. M. Shila, W. Shen, Y. Cheng, X. Tian, and X. S. Shen. Amcloud: Toward a secure autonomic mobile ad hoc cloud computing system. *IEEE Wireless Communications*, 24(2):74–81, April 2017.

[144] D. Shin, V. Sharma, J. Kim, S. Kwon, and I. You. Secure and efficient protocol for route optimization in pmipv6-based smart home iot networks. *IEEE Access*, 5:11100–11117, June 2017.

[145] E. Shmueli and T. Tassa. Secure multi-party protocols for item-based collaborative filtering. In *Proc. of the*

11th ACM Conference on Recommender Systems, Como, Italy, pages 89–97. ACM, August 2017.

[146] K. N. E. A. Siddiquee, K. Andersson, F. F. Khan, and M. S. Hossain. A scalable and secure manet for an i-voting system. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 8(3):1–17, September 2017.

[147] H. Song, K. Omori, J. Kim, K. E. Tenzek, J. M. Hawkins, W.-Y. Lin, Y.-C. Kim, and J.-Y. Jung. Trusting social media as a source of health information: online surveys comparing the united states, korea, and hong kong. *Journal of medical Internet research*, 18(3), March 2016.

[148] J. Su, A. Shukla, S. Goel, and A. Narayanan. De-anonymizing web browsing data with social networks. In *Proc. of the 26th International Conference on World Wide Web, Perth, Australia*, pages 1261–1269. ACM press, April 2017.

[149] Z. Su and Q. Xu. Security-aware resource allocation for mobile social big data: A matching-coalitional game solution. *IEEE Transactions on Big Data*, May 2017.

[150] G. Sun, Y. Xie, D. Liao, H. Yu, and V. Chang. User-defined privacy location-sharing system in mobile online social networks. *Journal of Network and Computer Applications*, 86:34–45, May 2017.

[151] T. Sun and M. K. Denko. A distributed trust management scheme in the pervasive computing environment. In *Proc. of the 2007 Canadian Conference on Electrical and Computer Engineering, Vancouver, BC, Canada*, pages 1219–1222. IEEE, April 2007.

[152] S. E. Tajbakhsh, G. Chen, and J. Coon. On computational approaches to trust evaluation in large-scale social networks. In *Proc. of the 2017 International Black Sea Conference on Communications and Networking (BlackSeaCom'17), Istanbul, Turkey*, pages 1–6. IEEE, June 2017.

[153] T. Takahashi, R. Tomioka, and K. Yamanishi. Discovering emerging topics in social streams via link-anomaly detection. *IEEE Transactions on Knowledge and Data Engineering*, 26(1):120–130, December 2014.

[154] W. Tounsi and H. Rais. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 72:212–233, September 2017.

[155] R. Tourani, S. Misra, T. Mick, and G. Panwar. Security, privacy, and access control in information-centric networking: A survey. *IEEE Communications Surveys & Tutorials*, 20(1):566–600, 2018.

[156] Y.-F. Tseng, C.-I. Fan, T.-C. Kung, J.-J. Huang, and H.-N. Kuo. Homomorphic encryption supporting logical operations. In *Proc. of the 2017 International Conference on Telecommunications and Communication Engineering, Osaka, Japan*, pages 66–69. ACM, October 2017.

[157] v. sharma, R. KUMAR, W. H. Cheng, M. Atiquzzaman, K. Srinivasan, and A. Zomaya. Nhad: Neuro-fuzzy based horizontal anomaly detection in online social networks. *IEEE Transactions on Knowledge and Data Engineering*, pages 1–1, March 2018.

[158] A. M. Vegni and V. Loscri. A survey on vehicular social networks. *IEEE Communications Surveys & Tutorials*, 17(4):2397–2419, July 2015.

[159] B. Viswanath, M. A. Bashir, M. Crovella, S. Guha, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Towards detecting anomalous user behavior in online social networks. In *Proc. of the 2014 USENIX Security Symposium, San Diego, CA, USA*, pages 223–238. USENIX, August 2014.

[160] A. H. Wang. Detecting spam bots in online social networking sites: a machine learning approach. In *Proc. of the 2010 IFIP Annual Conference on Data and Applications Security and Privacy (DBSec'10), Rome, Italy*, volume 6166 of *Lecture Notes in Computer Science*, pages 335–342. Springer, Berlin, Heidelberg, June 2010.

[161] C. Wang, V. Talwar, K. Schwan, and P. Ranganathan. Online detection of utility cloud anomalies using metric distributions. In *Proc. of the 2010 Network Operations and Management Symposium (NOMS'10), Osaka, Japan*, pages 96–103. IEEE, April 2010.

[162] F. Wang, B. Ge, L. Zhang, Y. Chen, Y. Xin, and X. Li. A system framework of security management in enterprise systems. *Systems Research and Behavioral Science*, 30(3):287–299, May 2013.

[163] J.-C. Wang and C. Chiu. Detecting online auction inflated-reputation behaviors using social network analysis. In *Proc. of the 2005 Annual conference of the North American association for computational social and organizational science (NAACSOS'05), Notre-Dame, Indiana*, June 2005.

[164] P. Wang, B. Xu, Y. Wu, and X. Zhou. Link prediction in social networks: the state-of-the-art. *Science China*

Information Sciences, 58(1):1–38, January 2015.

[165] R. Wang, A. M. Azab, W. Enck, N. Li, P. Ning, X. Chen, W. Shen, and Y. Cheng. Spoke: Scalable knowledge collection and attack surface analysis of access control policy for security enhanced android. In *Proc. of the 2017 ACM on Asia Conference on Computer and Communications Security (AsiaCCS'17), Abu Dhabi, United Arab Emirates*, pages 612–624. ACM, April 2017.

[166] Y. Wang, G. Yin, Z. Cai, Y. Dong, and H. Dong. A trust-based probabilistic recommendation model for social networks. *Journal of Network and Computer Applications*, 55:59–67, September 2015.

[167] E. Waters and E. M. Cummings. A secure base from which to explore close relationships. *Child development*, 71(1):164–172, January 2000.

[168] C.-E. Weng, V. Sharma, H.-C. Chen, and C.-H. Mao. Peer: Proximity-based energy-efficient routing algorithm for wireless sensor networks. *J. Internet Serv. Inf. Secur.*, 6(1):47–56, February 2016.

[169] C. White, L. Plotnick, J. Kushma, S. R. Hiltz, and M. Turoff. An online social network for emergency management. *International Journal of Emergency Management*, 6(3-4):369–382, January 2009.

[170] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. *computer*, 35(10):54–62, October 2002.

[171] D. D. Woods and E. Hollnagel. Prologue: resilience engineering concepts. In *Resilience Engineering: Concepts and Precepts*, pages 13–18. CRC Press, 2017.

[172] S. Wu, Y. Zhu, and Q. Pu. Robust smart-cards-based user authentication scheme with user anonymity. *Security and communication Networks*, 5(2):236–248, February 2012.

[173] X. Xiao, C. Chen, A. K. Sangaiah, G. Hu, R. Ye, and Y. Jiang. Cenlocshare: a centralized privacy-preserving location-sharing system for mobile online social networks. *Future Generation Computer Systems*, 86:863–872, September 2018.

[174] Z. Yan, W. Feng, and P. Wang. Anonymous authentication for trustworthy pervasive social networking. *IEEE Transactions on Computational Social Systems*, 2(3):88–98, September 2015.

[175] Z. Yan, X. Li, and R. Kantola. Personal data access based on trust assessment in mobile social networking. In *Proc. of the 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'14), Beijing, China*, pages 989–994. IEEE, September 2014.

[176] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos. Flexible data access control based on trust and reputation in cloud computing. *IEEE Transactions on Cloud Computing*, 5(3):485–498, July 2017.

[177] Z. Yan and M. Wang. Protect pervasive social networking based on two-dimensional trust levels. *IEEE Systems Journal*, 11(1):207–218, March 2017.

[178] Z. Yan, M. Wang, V. Niemi, and R. Kantola. Secure pervasive social networking based on multi-dimensional trust levels. In *Proc. of the 2013 International Conference on Communications and Network Security (CNS'13), National Harbor, MD, USA*, pages 100–108. IEEE, October 2013.

[179] Y. Yu and X. Chen. A survey of point-of-interest recommendation in location-based social networks. In *Proc. of the 2015 Workshops at the 29th AAAI Conference on Artificial Intelligence, Austin, Texas, USA*, volume 130. AAAI, January 2015.

[180] C. Zhang, J. Sun, X. Zhu, and Y. Fang. Privacy and security for online social networks: challenges and opportunities. *IEEE network*, 24(4), July 2010.

[181] F. Zhang, V. E. Lee, R. Jin, S. Garg, K.-K. R. Choo, M. Maasberg, L. Dong, and C. Cheng. Privacy-aware smart city: A case study in collaborative filtering recommender systems. *Journal of Parallel and Distributed Computing, https://doi.org/10.1016/j.jpdc.2017.12.015*, Feburary 2018.

[182] Y. Zhang, Z. Li, K. Bian, Y. Bai, Z. Yang, and X. Li. Population distribution projection by modeling geo homophily in online social networks. In *Proc. of the 2nd International Conference on Crowd Science and Engineering, Beijing, China*, pages 1–8. ACM, July 2017.

[183] Y. Zhang, L. Song, C. Jiang, N. H. Tran, Z. Dawy, and Z. Han. A social-aware framework for efficient information dissemination in wireless ad hoc networks. *IEEE Communications Magazine*, 55(1):174–179, January 2017.

[184] Z. Zhang, K.-K. R. Choo, and B. B. Gupta. The convergence of new computing paradigms and big data analytics methodologies for online social networks, May 2018.

[185] J. Zhao. Analyzing resilience of interest-based social networks against node and link failures. *IEEE Transactions on Signal and Information Processing over Networks*, 3(2):252–267, June 2017.

[186] R. Zhao, M. Ding, K. Koyanagi, Y. Sun, and L. Zhou. A privacy-preserving community-based p2p osns using broadcast encryption supporting recommendation mechanism. *arXiv preprint arXiv:1706.01324*, 2017.

[187] S. Zhao, I. King, and M. R. Lyu. A survey of point-of-interest recommendation in location-based social networks. *arXiv preprint arXiv:1607.00647*, 2016.

[188] X. Zheng, G. Luo, and Z. Cai. A fair mechanism for private data publication in online social networks. *IEEE Transactions on Network Science and Engineering, 10.1109/TNSE.2018.2801798*, February 2018.

[189] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos. Security and privacy for cloud-based iot: Challenges. *IEEE Communications Magazine*, 55(1):26–33, January 2017.

[190] Y. Zhou, D. W. Kim, J. Zhang, L. Liu, H. Jin, H. Jin, and T. Liu. Proguard: Detecting malicious accounts in social-network-based online promotions. *IEEE Access*, 5:1990–1999, January 2017.

Author Biography

Takshi Gupta received the B.Tech. degree in Computer Science and Engineering from Punjab Technical University in 2012 and the PG Diploma in Business Administration from SCDL, Symbiosis University, India in 2014 both with distinction. She is currently associated with the MobiSec Lab, Department of Information Security Engineering, Soonchunhyang University, Asan, South Korea. Prior to this, she worked at Kochar InfoTech followed by Gen-XT Infosystems and was a co-founder at Future Info-Systems. Her areas of research and interests are database management and security, artificial intelligence, semantic webs, and human resource management.

Gaurav Choudhary received the B.Tech. degree in Computer Science and Engineering from Rajasthan Technical University in 2014 and the Master Degree in Cyber Security from Sardar Patel University of Police in 2017. He is currently pursuing Ph.D. degree in the Department of Information Security Engineering, Soonchunhyang University, Asan, South Korea. His areas of research and interests are UAVs, Mobile and Internet security, IoT security, Network security, and Cryptography.

Vishal Sharma received the Ph.D. and B.Tech. degrees in computer science and engineering from Thapar University (2016) and Punjab Technical University (2012), respectively. He worked at Thapar University as a Lecturer from Apr'16-Oct'16. From Nov. 2016 to Sept. 2017, he was a joint post-doctoral researcher in MobiSec Lab. at Department of Information Security Engineering, Soonchunhyang University, and Soongsil University, Republic of Korea. Dr. Sharma is now a Research Assistant Professor in the Department of Information Security Engineering, Soonchunhyang University, The Republic of Korea. Dr. Sharma received three best paper awards from the IEEE International Conference on Communication, Management and Information Technology (ICCMIT), Warsaw, Poland in April 2017; from CISC-S'17 South Korea in June 2017; and from IoTaas Taiwan in September 2017. He is the member of IEEE, a professional member of ACM and past Chair for ACM Student Chapter-TU Patiala. He has authored/coauthored more than 60 journal/conference articles and bookchapters. He serves as the program committee member for the Journal of Wireless Mobile Networks, Ubiquitous

Computing, and Dependable Applications (JoWUA). He was the track chair of MobiSec'16 and AIMS-FSS'16, and PC member and reviewer of MIST'16 and MIST'17, respectively. He was the TPC member of ITNAC-IEEE TCBD'17 and serving as TPC member of ICCMIT'18, CoCoNet'18 and ITNAC-IEEE TCBD'18. Also, he serves as a reviewer for various IEEE Transactions and other journals. His areas of research and interests are 5G networks, UAVs, estimation theory, and artificial intelligence.