# A Two-phase Analyzer for Vulnerabilities of Online Social Media Users

Saman Mirza Abdullah, *IAENG Member*

*Abstract*—**Vulnerabilities of online social network (OSN) users constantly pose different problems and questions. Among those issues are measuring and analyzing the type and size of existing users' vulnerabilities in different cultures. This measure requires the evaluation of OSN user behaviors used in serious threats and attacks and their alignment with major policies. In this work, behaviors of OSN users have been collected to cover user activities in social media websites on their Internet-connected devices. The methodology of this work proposes categorizing the behavior of OSN users by using two phases, namely, analyzing the approach based on Shamir's theory for computing the user's vulnerability rate and k-mean clustering technique for user categorization. This approach discusses the relation between the user's vulnerability and attack policies. As the analysis considers data from two different countries, the probability of targeting an area with specific attacks can be clearly identified. Finally, the low or high rates of vulnerabilities of OSN users in these two countries are analyzed and discussed.**

*Index Terms*—**Online Social Networks, User Vulnerabilities, Behavior Analyzing, Culture Influenced Vulnerabilities.**

## I. Introduction

As of 2018, Facebook (FB) alone accounts for 2.2 billion of social network users [1]. This figure shows the increase in the number of online social network (OSN) users. Location and time limitations no longer pose as challenges to OSN users due to device portability. Each user can do activities he/she likes anywhere and anytime. Moreover, OSN websites provide new services and facilities for their users daily. This availability enables Internet users to stay connected to OSN websites as much as they want and do a wide range of activities. For example, FB users do around 3.21 billion activities per day. However, not all activities are clean in the viewpoint of security and privacy standards. The variety of user activities and OSN websites facilitates the work of attackers in finding more gaps toward penetrating an increased number of users and systems. Attackers and intruders have learned to override systems through OSN users' vulnerabilities rather than systems' vulnerabilities. This trend changed the direction of research on analyzing user behavior more than operating system gaps.

Researchers aim to improve user behaviors instead of system gaps. Therefore, the majority of studies provide security and privacy solutions to OSN users [2-4]. However, only a few OSN users can understand these solutions completely. To simplify these solutions for users, the majority of investigations have classified and even sub classified these attacks and threats on OSN users into security- and privacy-related works [5]. These studies usually provide an overview of the types of OSN attacks and explain the possibility of threats to users. Furthermore, they provide recommendations and suggestions as solutions for OSN users to protect their privacy and security. Ref.[6] classified OSN threats and attacks into four groups and offered many commercial and scientific solutions for protecting OSN users. Aside from threats and attacks, many studies have conducted general investigations on privacy, security, and behavior of OSN users [3]. Other studies have focused on one type of user vulnerability called third-party applications (TPAs) and highlighted a unique security and privacy design that challenges the core functionalities of OSN websites. They argued some opportunities for utilizing the social network theory to mitigate these design conflicts and provide possible solutions to limit information disclosure [3]. An increased number of studies have investigated OSN-related topics and offered many solutions (Section 3). However, OSN users are still open to attacks and intruders continue to find vulnerabilities for system penetration. Therefore, studies on the analysis of OSN users' vulnerabilities or behaviors are necessary.

In this work, vulnerabilities or OSN user behaviors will be classified into four scales of privacy and security. This study will then identify the relationship of each class with the type of attacks or threats. Moreover, the impact of culture on privacy and security issues may also indicate the need for further analysis on OSN user behaviors. The rest of the paper is structured as follows. The next section offers the contributions of the work. Section 3 presents the literature review. Section 4 discusses the work methodology. Section 5 and 6 cover the results and analysis, respectively. Section 7 draws the conclusions of the study.

## II. Contribution of the Works

The main contribution of this work is the analysis of OSN user's vulnerabilities and their alignment with the policies that attackers misuse for system penetration. This work utilizes a new approach that combines Shamir's theory and k-mean clustering techniques. The output of this analysis can illustrate the scale of OSN users' privacy and security. The analysis can also explain the common vulnerabilities of an area that may be further analyzed to investigate the impact of cultural characteristics on security and privacy of an individual (OSN user).

Manuscript received May 11, 2019; revised February 13, 2020.

Saman is working as lecturer with Koya University, Department of Software Engineering (saman.mirza@koyauniversity.org). He is also working as a part-time lecturer with Ishik University (saman.mirza@ishik.edu.iq)

## III. Related Works

Recent works on OSN technologies and users have discussed privacy and security issues [2-4]. They have reviewed different perspectives about the challenges that restrict OSN users to ensure security against threats and attacks. Although different studies have focused on the structure and framework of social media websites as a gap in this field, other studies have focused on OSN user behaviors or vulnerabilities as research problems. Recent studies have argued that OSN user behaviors rather than OSN frameworks should be investigated and analyzed as threats because misuse is often exploited during system penetrations [7]. The gaps left by user behaviors are difficult to mitigate as different users have different behaviors, thereby causing a variety of vulnerabilities. Therefore, studies need to investigate the (1) type of threats and attacks that often misuse user vulnerabilities, (2) types of user behaviors that threats and attacks target or scan, and (3) techniques and tools that can reveal the relationship between user behaviors and attacks. This work categorizes the reviewed works based on these three types of investigations. First, the major types of OSN-based threats and attacks that are mentioned in recent literature has been reviewed. The relationship between threats and attacks on OSN user vulnerabilities are then explained. Finally, recent techniques that have classified OSN attacks are discussed.

### *A. Threats and attacks*

A wide range of attacks and threats target OSN users and their systems. We first define the meaning, functionalities, and differences between threats and attacks. A threat could be anything that can interrupt a process, slowdown performance, or disrupt the integrity and availability of a network or system. An attack is a specific technique used by an unauthorized user for exploiting systems or user vulnerabilities. In the OSN field, an attack could be a type of technique used by threats for penetrating the social network's users and controlling them as victims [8]. Different attacks use a variety of techniques to lure OSN users in performing activities that facilitate system penetration. Therefore, classifying threats and attacks has become the target research of many studies [6, 9]. The major and recent threats attacks on OSN users and websites are as follows.

1) Worm Malwares. Social media is an area conducive to malware propagation. Worms are a type of serious malware on social networks that propagate and execute without the need of user interaction. For example, Koobface, a special type of social media worm, is considered the largest Web 2.0 botnet [10]. This worm can propagate over Facebook, myspace, Twitter, hi5, Bebo, and Friendster. These special worms can enlist additional Internet connected devices into its botnet, hijack many accounts, and send spam messages [11].
2) Trojan Malware. Social network becomes a great vector for trojans. Trojans, such as Zeus, can be sent to an OSN user by using an interest link ("Click here and you will get") to lure users [12]. This type of malware can steal critical information, such as bank account and credit card information.
3) Phishing Attack. This type of attack constantly lures OSN users to relog into their social media accounts for interesting information, images, or videos by using social engineering techniques [13].
4) Data or Information Leakage. Social media involves sharing activities and information. This type of leakage has a negative implication on OSN users because it allows a TPA to create an application programming interface that can automatically collect and steal sensitive data without prior knowledge of users. This process is true for location leakage attacks, which cause privacy issues for OSN users [14].
5) Botnet. Accounts of many social media platforms, such as Twitter, are used as command and control (C&C) channels for botnet propagation. Some botnets use file sharing applications as the C&C channel [15]. These botnets are known as SocilBot. In most cases, botnet propagation depends on connecting devices to insecure networks, which are typically accessed for free.
6) Identity Impersonation Attack. This type of attack steals the personal information, identity, or personal behaviors of the victim (an OSN user that operates under unsafe privacy and security configurations). The attack will usually steal information from well-known persons, businessmen, or persons with high-level positions and use this stolen information to impersonate them and conduct fake businesses and activities [16].
7) Hashtag or/and Brand Jacking. This type of attack aims to confuse customers of a specific brand product or mislead the attention of the brand itself. The attacker will create a fake account that uses similar characters and logos of the original brand. The attack will then act as the original brand account and create panic for customers and companies [16].
8) Socware Attack. This type of attack lures OSN users with false rewords by installing/accepting applications, webpages, or interest events that contain malicious links. Once accepted or installed, the malicious code will inject the user's account and control all posts and activities [5, 17].
9) Rumor Attack. This type of attack propagates misinformation among OSN users. The main vulnerability misused by this attack is the trust of OSN users on interesting information shared with them. At the end, the large misinformation pooled among users causes instability in society and among OSN users.
10) Sybil Attack. This type of attack creates fake accounts. A user can create many anonymous accounts that any single user can control. The user can then use these fake accounts to gain undue benefits, launch attacks through them, and spread misinformation. Many types of threats, such as phishing, spams, and malicious links can be propagated through such vulnerabilities.

The majority of studies have been categorized based on their targets and aims. A group of studies could focus only on a specific type of threat that attacks systems through OSN user behavior or weaknesses in social media websites. Another group attempted to cover as much threats as possible in their OSN attack analysis, thereby including all types of attacks or threats mentioned above in the analysis.

The next section explains the types of vulnerabilities that can affect OSN users and the relationship between each vulnerability and attack.

### B. Users' vulnerabilities

Studies that have focused on one specific type of OSN vulnerability have scoped their evaluation process on the attack's technique and the counter measures that my proposed for detecting or preventing this attack only. For example, a work investigating the impact of facial disclosure (user vulnerability) in face authentication systems of smart devices analyzes the differences between the vulnerable and nonvulnerable images of OSN profiles [18, 19]. Other works have focused on the specific attack called drive-by download (a user vulnerability when downloading through a malicious link). This attack is propagated through Twitter's OSN, benefits from the popularity of Twitter and the automatic system of URL shortening, and creates an obfuscate URL, which is distributed to Twitter users. Once clicked, the system of endpoint users will be infected and controlled [20]. Other works have focused on multiple attacks that depend on intelligent and mining techniques. For example, [21] uses a self-organizing map (SOM) to analyze user behaviors, security incidents, and fraud against OSN users. Another study investigated behavior similarity for specific vulnerabilities of OSN users by using mining techniques [22, 23]. Regardless of whether the study focuses on one or more attacks, defining the types of user behavior or system weakness related to a particular attack is important. Therefore, in this work, we define the vulnerabilities and their relationship with the attacks and frauds mentioned in Section 3.1. Listed below are the recent and major vulnerabilities that our work addresses [2-4, 7, 8]:

1) Accepting links from friends ($V_1$)
2) Clicking interesting subjects from strangers ($V_2$)
3) Number of followers is more interesting than quality of followers ($V_3$)
4) Downloading interesting apps without considering sources (websites or senders) ($V_4$)
5) Disclosing personal information ($V_5$)
6) Sharing and forwarding information without any enquiry ($V_6$)
7) Joining groups and forwarding messages ($V_7$)
8) Connecting devices to any free and insecure Wi-Fi ($V_8$)
9) Trusting offers available on social media, even if relogging is needed ($V_9$)
10) Accepting any connection requests from friends, classmates, workmates, and people from the same interest fields or subjects ($V_{10}$)

### C. Vulnerability analyzer techniques

When the type of focused attacks and related vulnerabilities have been defined, a study must define an analyzer tool to build a vulnerability detection or prevention model. The majority of studies on OSN vulnerability analyzers address the social network's security, privacy, or both. Different techniques, such as statistical, mining, or intelligent methods, are utilized for classifying security or privacy challenges or building systems for fraud and vulnerability detection or prevention [2, 16, 19].

The majority of attacks mentioned in Section 3.1 have been addressed in many studies. Faking or cloning accounts is a security- and privacy-challenged issue for OSN users. Through this attack, malicious links will be separated, and different privacy issues will be breached. A comparison study between cosine and n-gram similarity was conducted in [9] for detecting fraud vulnerability in Twitter accounts. This work distinguished fraud profiles from real accounts effectively. Another work achieved a two-phase clustering method to identify malicious behaviors of OSN users [5]. This work depended on clustering users into similar groups and then identifying normal and malicious groups for each user group. Artificial neural network (ANN) is a widely used intelligent algorithm for classifying threats in OSNs. An ANN has been designed and utilized in [13] to build an intelligent model for vulnerability detection among OSN users. This work argued that their model could easily support OSN users to measure the rate of their vulnerabilities and understand the type of vulnerabilities they are facing. Another common OSN threat called phishing is studied in [24]. Authors of this work proposed an ANN in the design of a phishing detection model that showed up to 92% accuracy in distinguishing phishing websites with legitimate features. Other works depended on fuzzy technique for building ruff-set feature selection that supports classifying spammers. Another serious threat to OSNs is the spam attack. Spams are common problems that can be found in different forms over the Internet. Ref. [25] used the support vector machine to build a spam detector based on account and user information of Twitter users. Compared with the mentioned works, this study proposes an intelligent classifier model for categorizing OSN users based on their vulnerability rates in security and privacy. This study then analyzes users in each category to identify the impact of each feature on the vulnerability rate and the impact of culture on each feature.

## IV. Methodology

Fig. 1 presents the methodology of this study. This work first utilizes and refines datasets and then uses a machine learning clustering method to obtain similar groups of OSN users. Finally, OSN users in each group are analyzed further to determine the relation between vulnerability rates and each OSN vulnerability and culture impact.

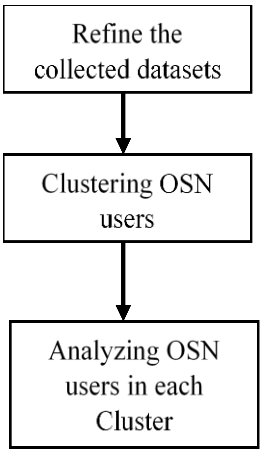

Refine the collected datasets
Clustering OSN users
Analyzing OSN users in each Cluster

Fig. 1 Work Methodology for Clustering and Analyzing OSN User Vulnerability

### A. *Dataset*

This work used the dataset that collected and prepared in [13]. The study distributed questionnaires in two different countries (Istanbul, Turkey and Kurdistan, Iraq). Although the cleansing process of the dataset has been applied by the authors of [13], the dataset was still unbalanced. Therefore, in our work, considerable cleansing processes have been used to balance the number of samples between different attributes and countries. Table I shows the demographics of two balanced datasets, namely, Istanbul, Turkey and Kurdistan, Iraq.

The first and second datasets contain 209 and 214 samples that represent Turkey and Iraq OSN users, respectively. Samples are composed of females and males in four age ranges and three education level categories. Both datasets have 31 attributes and each one is linked to a question listed in the distributed questionnaire. Each question is related to a security- or privacy-related issue of an OSN user behavior. The answer in each question is leveled from 1 (strongly disagree) to 5 (strongly agree). The first nine attributes (questions) are related to OSN user behaviors that are vulnerable to security issues. For example, one question asks the possibility of clicking a link that came from a stranger that shows something interesting and attractive. These types of behaviors may cause a high possibility of clicking an infected link, inserting a malicious code into systems, and creating malware infection. Therefore, when a user rates this question as five, this user has high vulnerability against malware infection. The 22 other attributes (questions) are related to privacy issues of OSN users. For example, information or location leakage is a type of attack that collects and misuses information from websites and browsers. Banner grabbing is an attack that aims at collecting information to infect systems. However, if an OSN user discloses his/her privacy on a social network website, banner grabbing attack, which can infect the system, is possible [8]. Similar to this study, each question is related to an OSN user behavior linked to a security or a privacy issue.

### B. *Measuring User's Vulnerability*

Section 4.1 mentions that each observation in the constructed dataset represents an OSN user, and each attribute is linked to a question that rates the user's vulnerability against security or privacy issues. However, measuring the vulnerability rate is important. This work uses the Shamir's secret sharing algorithm, which divides a secret into shares and statistics, wherein the secret can only be recovered by combining a certain number of shares. In this study, this theory is called the $f(n,t)$ secret-sharing scheme. In this scheme, n shares of the original secret are created. If an attack wants to recover this secret, then it should have at least $t$ number of shares, and any $t-1$ or fewer shares is not enough to reconstruct the original message. This value of $t$ is called the Shamir's threshold scheme [26, 27].

The vulnerability of an OSN user could be explained by privacy disclosure or abnormal behaviors. If we consider disclosing privacy as a type of sharing privacy, then an attack can recover all privacies of this user when the attacker has $t$ number of disclosing privacies. Hence, an OSN user may have $n$ levels of vulnerabilities against a certain type of abnormal behavior. An attacker needs to reach a certain level, which should be equal to $t$, to gain advantage of these vulnerabilities in taking over the system. Only at that level can the disclosed secrets or opened vulnerabilities be useful for that attacker. Another possibility is when a type of vulnerability becomes the target of more than one attack. Hence, more than one attack is sharing the disclosed vulnerability.

Assume that $V = \{v_1, v_2, v_3, \dots v_m\}$ is a set of all available OSN user vulnerabilities, where $v_a : v_a \subseteq V$ is a subset wherein a specific attack (such as a) can be active only when $v_a$ exists. Assume also that A$= \{a_1, a_2, a_3, \dots a_n\}$ is a set of available attacks and $a_i : a_i \subseteq A$ is a subset of attacks that each one shares the advantages from a specific vulnerability ($v_i$), where $i = 1,2,3, \dots m$.

On the basis of the above conditions, this study proposes a multi-secret sharing approach for measuring the vulnerability rate of an OSN user. Equation 1 is utilized in this work to measure the vulnerability rate of an OSN user.

TABLE I
DEMOGRAPHIC TABLE OF COLLECTED DATA

| City - Countries | Gender | | Age | | | | Education Level | | |
|---|---|---|---|---|---|---|---|---|---|
| | Male | Female | 10-15 | 16-25 | 26-40 | 40 above | High school / Diploma | Bachelor 's degree | Higher Education |
| Istanbul - Turkey | 103 | 106 | 47 | 59 | 69 | 34 | 116 | 88 | 5 |
| Erbil – Iraq | 102 | 112 | 51 | 53 | 70 | 40 | 112 | 93 | 9 |

This equation can be verified for an attack only if the coefficient number of $t-1$ satisfies the number of shares that makes the attack active.

$$V(v,w) = v_1w_1 + v_2w_2^2 + v_3w_3^3 + \cdots v_tw_t^t, \qquad (1)$$

where $V$ is the set of vulnerabilities, $v_i$ is an element in $V$, and the weight $W_i$ shows the degree of risks caused by $v_i$. If an OSN user performs activities that announce all or some vulnerabilities of $V$ to create $V_a$ for an attack, then Equation 1 can be used to measure the rate of user's vulnerability against that attack. The following section determines the measurement of the value of $W_i$.

### C. *Measuring Weight's Value*

According to Sections 3.2 and 4.1, a significant relation exists between each attack and the questions mentioned in the distributed questionnaire sheet. An attack can also gain advantages from more than one vulnerability to infect the system. The attack only needs one available vulnerability to override the system. Therefore, an attack related to more vulnerabilities is more dangerous than that with only a specific available vulnerability. Therefore, an increased weight is given to an attack that has relations with an increased number of vulnerabilities. Table II shows the relation between each threat/attack with a specific vulnerability.

TABLE II
ATTACKS-VULNERABILITIES RELATIONSHIP

| Vulnerability' s Features | Worm | Trojan | Phishing | Data Leakage | Botnet | Impersonation | Brand Jacking | Socware | Rumors | Sybils Account |
|---|---|---|---|---|---|---|---|---|---|---|
| $V_1$ | X | X | X |  | X |  |  |  | X | X |
| $V_2$ | X | X |  |  |  |  |  |  | X | X |
| $V_3$ |  |  |  | X |  | X | X | X | X | X |
| $V_4$ | X | X | X |  | X |  |  | X |  |  |
| $V_5$ |  |  | X | X |  | X | X | X | X | X |
| $V_6$ | X | X |  |  | X |  | X |  | X | X |
| $V_7$ |  |  |  | X |  | X | X |  |  | X |
| $V_8$ | X | X | X |  | X |  |  |  |  |  |
| $V_9$ |  |  | X | X |  | X | X | X | X | X |
| $V_{10}$ |  |  |  | X |  | X | X | X | X | X |

## V. ANALYSIS PHASE

This work uses a two-phase analysis process. The first classifies all users into similar groups by using k-nearest algorithms for clustering. The second phase analyzes users at each cluster based on the type of vulnerabilities that dominantly available at each group by using the SOM algorithm to show which attributes have more weight in the cluster.

### A. *Group Identification Phase*

In this phase, OSN users are clustered into groups based on their privacy–security behaviors. Section 4.1 mentions that out of the 31 attributes in the recruited datasets, 9 and 22 attributes are related to security and privacy behaviors, respectively. By using Equation 1, the rate of security and privacy for each observation (an OSN user) can be obtained. Fig. 2 and Fig. 3 illustrate the scatter plot of the privacy–security relation for OSN users in both datasets (Erbil-Iraq and Istanbul-Turkey).

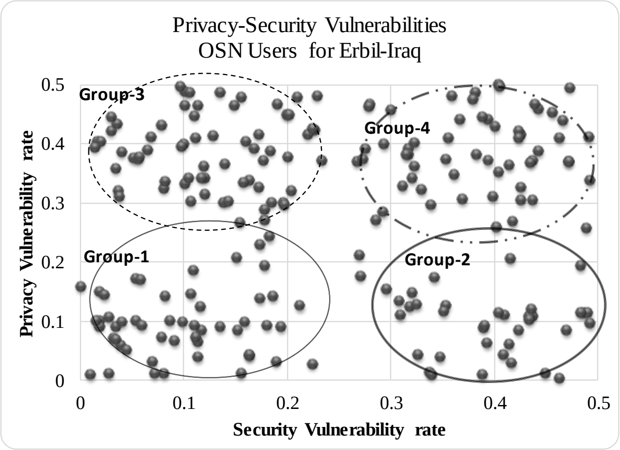


Fig. 2 Privacy-Security Relationship for OSN users in Erbil-Iraq

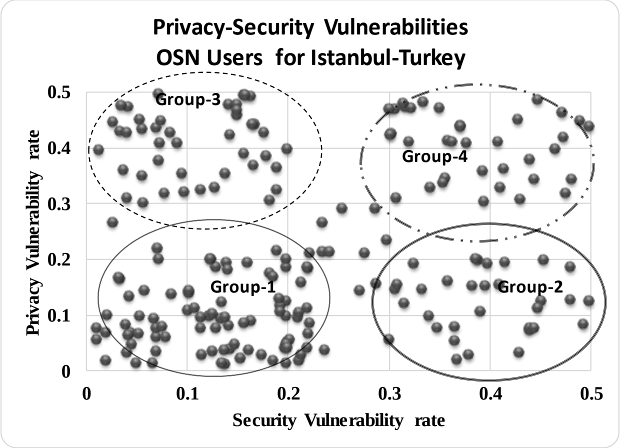


Fig. 3 Privacy-Security Relationship for OSN users in Istanbul-Turkey

On the basis of the scattered points in Figures 2 and 3, behaviors of OSN users can be clustered into four groups. A point in each group represents the privacy–security behavior of an OSN user. Therefore, points in a group should have similar behaviors or should be located in the same range of vulnerability rates. Hence, groups could be defined based on their vulnerability ranges as follows:

1) Group-1. Users with privacy and security vulnerability rates located in the range [0,0.25] can be assessed as securable users that keep their privacy well.
2) Group-4. Users with privacy and security vulnerability rates located in the range [0.25, 0.5] can be assessed as risky users in the viewpoint of security that highly disclose their privacy.
3) The two types of OSN users who have good security [0, 0.25] but have exposed privacy [0.25, 0.5] (Group-3) or

conduct very risky and unsecured activities [0.25, 0.5] but still keep their privacy well [0, 0.25] (Group-2).

To confirm the ranges mentioned above, this work depends on the k-nearest method to measure the distance between the grouped points and identify the optimum center for each group. The k-nearest method utilized in this work depends on the Minkowski distance (Equation 2) to measure the average or mean distance between points in a group.

$$D(X,Y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{1/p} \qquad (2)$$

where $X$ and $Y$ are two points, such that $X = \{x_1, x_2, x_3, \dots x_n\}$ and $Y = \{y_1, y_2, y_3, \dots y_n\}$; and the value of $p = 2$. Fig. 4 shows that the scatter point with the location of optimum center has a minimum distance among all points in the group. On the basis of the obtained vulnerability range and the center of each group, four similar OSN users in the viewpoint of security and privacy issues can be distinguished.

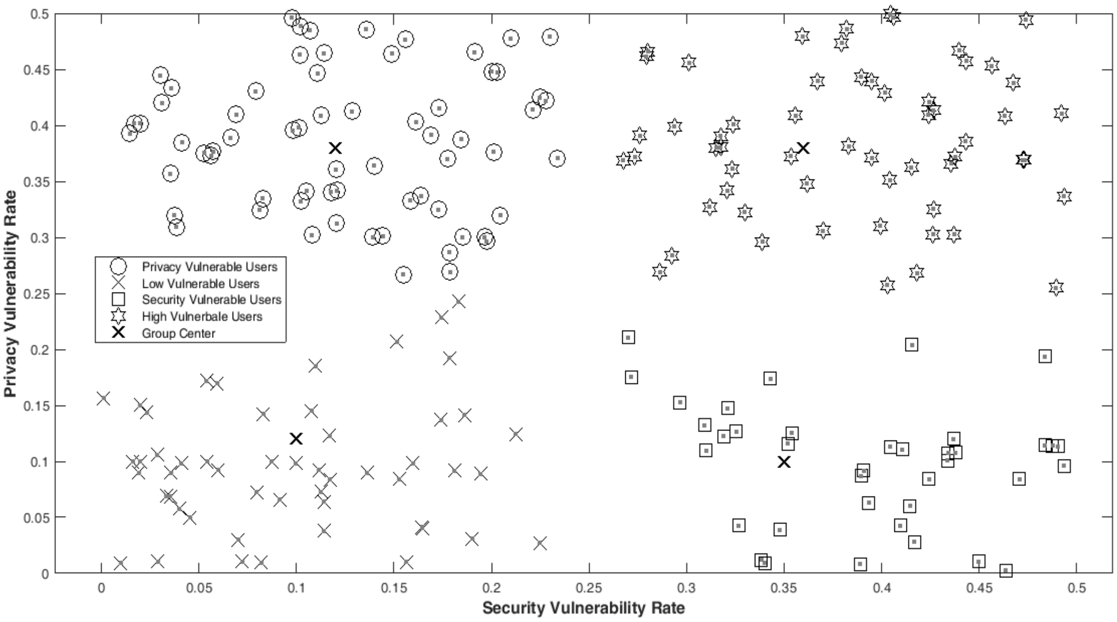


Fig. 4 Location of the optimum Center in OSN user vulnerability groups using KNN

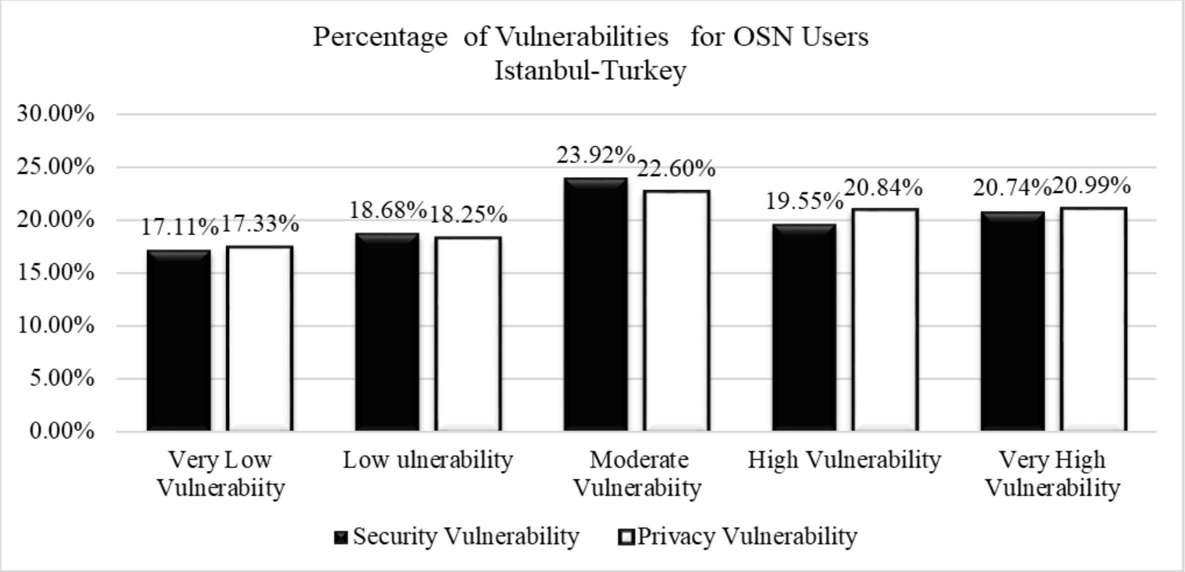


Fig. 5 Percentage of OSN users associated with security–privacy vulnerability rates in Istanbul-Turkey

The next section identifies the common vulnerabilities inside each group.

### *B. Vulnerability Identification Phase*

This work investigates the security and the privacy vulnerabilities of OSN users by evaluating users' behavior in two datasets obtained from two different cultures (Iraq and Turkey). Section 5.1 presents the work identified the user group based on the measured distance similarity of vulnerability rates among the users. In this section, the common types of vulnerabilities in each group are identified. The evaluation starts with datasets, groups in each dataset, and types of vulnerabilities (security or privacy) in each group.

TABLE III
NUMBER OF OSN USERS ASSOCIATED WITH DIFFERENT TYPES OF VULNERABILITIES

| Vulnerability's Features | Type of Vulnerability | No. of users / Rates | | |
|---|---|---|---|---|
| | | 1-2 | 3 | 4-5 |
| $V_1$ | Security | 59 | 52 | 103 |
| $V_2$ | Security | 51 | 39 | 134 |
| $V_3$ | Privacy | 81 | 38 | 95 |
| $V_4$ | Security | 58 | 56 | 100 |
| $V_5$ | Privacy | 43 | 45 | 126 |
| $V_6$ | Privacy | 59 | 39 | 116 |
| $V_7$ | Privacy | 59 | 61 | 94 |
| $V_8$ | Security | 43 | 32 | 139 |
| $V_9$ | Security | 55 | 62 | 97 |
| $V_{10}$ | Privacy | 83 | 46 | 85 |

Fig. 6 shows the percentage of security and privacy vulnerabilities of OSN users in Erbil, Iraq. The figure shows that a small number of OSN users in Erbil, Iraq have low rates of vulnerabilities, whereas a high number of OSN users possess very high vulnerability. This figure shows that only 24.84% of OSN users in Erbil behave within good security and 31.07% have good privacy. The rest of OSN users in Erbil have a high probability of receiving attacks from threats and attackers. However, we need to identify the types of attacks with high probabilities. Thus, we divided OSN users into three groups. The first comprises users who rated their behaviors with 1 or 2. The second and third groups consist of moderate users and those who rated their behaviors with 4 or 5, respectively. Fig. 5 shows the result of this grouping.

Table III shows that the highest-ranking security vulnerability among OSN users in Erbil, Iraq comes from connecting to free Wi-Fi connections. The threats associated with this vulnerability involve botnet propagation. The next vulnerability is clicking interesting subjects, which are malicious links that cause the insertion of malicious codes in the system in most cases. The vulnerability ranked third is trusting all links forwarded by a friend, thereby leading to

TABLE IV
NUMBER OF OSN USERS ASSOCIATED WITH DIFFERENT TYPES OF VULNERABILITIES

| Vulnerability's Features | Type of Vulnerability | No. of users / Rates | | |
|---|---|---|---|---|
| | | 1-2 | 3 | 4-5 |
| $V_1$ | Security | 65 | 37 | 107 |
| $V_2$ | Security | 79 | 64 | 66 |
| $V_3$ | Privacy | 96 | 64 | 49 |
| $V_4$ | Security | 85 | 41 | 83 |
| $V_5$ | Privacy | 56 | 36 | 117 |
| $V_6$ | Privacy | 62 | 64 | 83 |
| $V_7$ | Privacy | 69 | 27 | 113 |
| $V_8$ | Security | 71 | 49 | 89 |
| $V_9$ | Security | 74 | 59 | 76 |
| $V_{10}$ | Privacy | 91 | 59 | 59 |

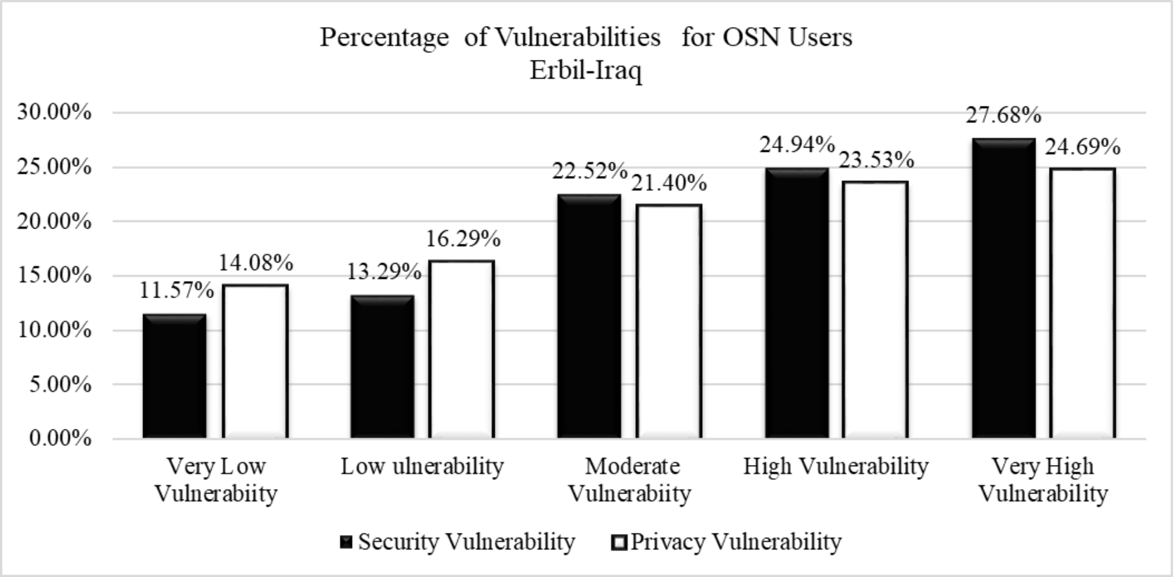
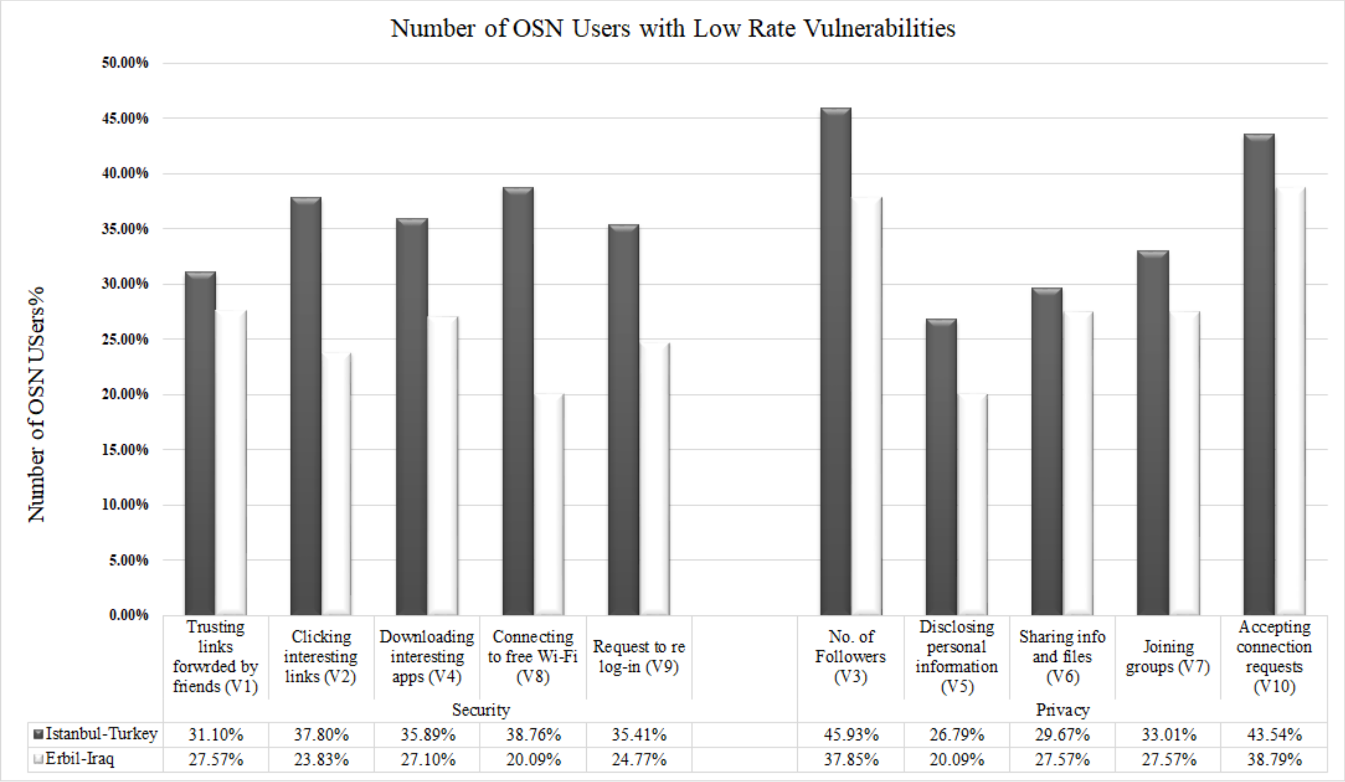


Fig. 6 Percentage of OSN users associated with security–privacy vulnerability rates in Erbil-Iraq



| | Trusting links forwrded by friends (V1) | Clicking interesting links (V2) | Downloading interesting apps (V4) | Connecting to free Wi-Fi (V8) | Request to re log-in (V9) | | No. of Followers (V3) | Disclosing personal information (V5) | Sharing info and files (V6) | Joining groups (V7) | Accepting connection requests (V10) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ■ Istanbul-Turkey | 31.10% | 37.80% | 35.89% | 38.76% | 35.41% | | 45.93% | 26.79% | 29.67% | 33.01% | 43.54% |
| □ Erbil-Iraq | 27.57% | 23.83% | 27.10% | 20.09% | 24.77% | | 37.85% | 20.09% | 27.57% | 27.57% | 38.79% |

Fig. 7 Number of OSN users with low security–privacy vulnerability rates

the insertion of malicious codes in the system. Rumor or hashtag (hijacking) attacks often occur and subsequently cause misinformation among OSN users.

The last two security vulnerabilities are downloading apps forwarded by friends and requiring to log-in again to the user's social media account. These types of vulnerabilities likely involve phishing or Socware attacks. Regarding the privacy vulnerabilities among OSN users in Erbil, Table III shows that the highest-ranking vulnerability is disclosing personal information. When an OSN user opens his/her account on social media, knowing the privacy setting is an important step.

The majority of social media set an open account on default, which means that no privacy is reserved, and all personal information is disclosed to others. Certain social media platforms encourage users to complete and publish their account data. Disclosing personal information may lead to many panic-related problems. The creation of Sybil accounts is a common problem with impersonation. Data leakage is another problem caused by this vulnerability. The second ranked privacy vulnerability is sharing files and information among users in their contact list or groups. This behavior is very popular among OSN users in Erbil, Iraq. The risk of this behavior increases the possibility of phishing attacks, data leakage, and brand jacking misinformation. OSN users often share and forward videos within their social groups. This video-sharing activity increases the possibility of worm or trojan propagation and the insertion of malicious codes through Socware attackers. The third ranked privacy vulnerability is the number of followers. Increasing the number of followers and friends among some OSN users has become a competition, thereby increasing the risk of Sybil account attackers. Finally, the last two vulnerabilities are accepting many requests and joining groups. These two behaviors increase the possibility of brand jacking misinformation, Socware, information leakage, and Sybil account attacks.

Fig. 6 shows that the highest percentage of the OSN users in Istanbul, Turkey exhibits moderate vulnerability. However, the very high vulnerability ranked as a second highest present and the very low vulnerability users is last.

Table IV shows that most OSN users in Istanbul, Turkey are exposed to security vulnerability by clicking links that are forwarded by trusted friends. The second risk comes from connecting to free Wi-Fi. The third risk involves downloading interest apps via social media. The last two risks that target OSN users in Istanbul, Turkey are clicking interesting links forwarded by strangers with the possibility of asking to log-in again on their social media accounts. Regarding privacy vulnerability, the highest risk comes from disclosing personal information, which can cause panic and further problems. Sybil account attackers usually depend on public personal information to create fake accounts and use the data for misinformation and brand jacking. The second highest risk comes from joining similar interest groups. This vulnerability likely leads to Sybil account attacks, which, in turn, may cause information leakage, brand jacking attack, and impersonation. In certain cases, this vulnerability may lead to Socware attacks that can lure OSN users to trust many advertisements that may contain malicious activities or steal very sensitive information about users. The third risk comes from sharing sensitive information, files, or live videos. This vulnerability increases the possibility of collecting very sensitive data and information on OSN users via TPA. The remaining two vulnerabilities involve accepting requests and the interest to increase the number of followers.

## VI. Cultural Influence on User's Vulnerability

By analyzing the two collected datasets, top risks and vulnerabilities can vary with different cultures or countries. Fig. 7 compares OSN users in Turkey and Iraq with low vulnerability rates. This figure divides OS users of each country into two main groups (security and privacy vulnerabilities). Each group has five types of vulnerabilities. Sections V-A and V-B analyzed the behaviors of OSN users with corresponding vulnerabilities in each country. The possible risks and attacks are then identified. In this section, the percentage of low rate vulnerabilities of OSN users in each country is analyzed.

Fig. 7 shows that the number of OSN users with low vulnerability rates in Istanbul, Turkey is higher than that in Erbil, Iraq by an average of 8.27%. Hence, OSN users in Erbil, Iraq perform risky behaviors 8.27% more than those in Istanbul, Turkey. The main target of this work was addressing the impact of culture on the OSN user's behaviors. This work has not focused on studying the current situation of the OSN users in both countries. Therefore, the discussed behaviors reflecting the times of collecting the data, which was 2017. Based on the collected data in the both datasets and according to the analyses done bay this work, below findings could be emphasized:

1) Behaviors of OSN users certainly changed within the change of the cultures. It might be varied within the same culture over the change of time.
2) An OSN user should have time to access and do activities over social media platforms. Users in a society, where time worth nothing, will stay connected more than other users. More connected to Internet and do variety of activities increase the possibility of malware infection.
3) Propagating daily hot topics through links becomes a habit among OSN users. In a society where the quality of resources is not an issue, thousands of links will be spread in a second. In such cultures, malicious links have higher possibility to be spread and number of system infection will be more increase.
4) Accessing social media needs Internet connection. In a society where Internet connection costs high, the behavior of looking for free connections will be very common among OSN users. With such habit, botnets and DDoS attacks can more actively and increasingly penetrate networks and systems.
5) In some societies, privacy is not a big issue for OSN users, instead, increasing the number of followers through sharing information, accepting requests from whoever, and making grouping are much concerned. Users in such society have no idea about the problems that might be faced by such information leakage.

Through these findings, it becomes clear how behaviors of OSN users influenced by cultures, and how such influences affect security and/or privacy of OSN users.

## VII. Conclusions

Threats and attacks constantly look for vulnerabilities to penetrate systems and resources of personal or industrial devices successfully. Given that vulnerabilities in the system could be easily updated and maintained, threats exploit user behaviors for malicious activities. To propagate more violations, threats usually look for areas with many users, such as social media websites. To investigate the impact of culture on the rate of vulnerabilities, this work analyzed OSN user behaviors in two different countries. This study determined the common threats in each country more and which country had more users with low vulnerability rates. Users were grouped based on their security and privacy vulnerabilities, thereby identifying users with good security and privacy behaviors, bad behavior in both vulnerabilities, and good behavior in only one vulnerability. Moreover, this study determined that users from different cities, countries, or cultures were influenced by threats and attacks differently.

## References

[1] T. Black and L. Schwab-Reese, "Keeping up with the technology? Technological advances and child maltreatment research," vol. 2018, no. 85, 98, pp. 185-186, 2018.

[2] I. Kayes and A. Iamnitchi, "Privacy and security in online social networks: A survey," *Online Social Networks and Media,* vol. 3, no. 17, pp. 1-21, 2017.

[3] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions," *Information Sciences,* vol. 421, no. 18, pp. 43-69, 2017.

[4] Y. Xiang, E. Bertino, and M. Kutylowski, "Security and privacy in social networks," *Concurrency and Computation: Practice and Experience,* vol. 29, no. 7, p. e4093, 2017.

[5] N. Laleh, B. Carminati, and E. Ferrari, "Risk assessment in Social Networks based on User Anomalous Behaviors," *IEEE Transactions on Dependable and Secure Computing,* vol. 15, no. 2, pp. 295-308, 2018.

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

[7] M. A. Al-Garadi *et al.*, "Analysis of Online Social Network Connections for Identification of Influential Users: Survey and Open Research Issues," *ACM Computing Surveys (CSUR),* vol. 51, no. 1, p. 16, 2018.

[8] M. M. Ameen, B. Ahmed, and S. M. Abdullah, "A New Taxonomy of Mobile Banking Threats, Attacks and User Vulnerabilities," in *International Engineering Conference*, Erbil Iraq, 2018, vol. 3, no. 3: EAJSE Journal, pp. 12-20.

[9] M. Chatterjee, "Detection of Fake and Cloned Profiles in Online Social Networks," in *Conference on Technologies for Future Cities (CTFC)*, India, 2019: SSRN, pp. 1-5.

[10] P. Chaudhary, B. Gupta, and S. Gupta, "A Framework for Preserving the Privacy of Online Users Against XSS Worms on Online Social Network," *International Journal of Information*

*Technology and Web Engineering (IJITWE),* vol. 14, no. 1, pp. 85-111, 2019.

[11] Q. Zhu, Y. Jiang, and Y. Zhang, "The Impact of Predators on Malicious Worms Propagation: a Theoretical Approach," *IAENG International Journal of Computer Science,* vol. 45, no. 3, pp. 371-376, 2018.

[12] C. de la Torre and J. C. Polo, "Cloud computing and network analysis," in *International Conference on Information Systems Architecture and Technology*, 2018: Springer, pp. 190-198.

[13] F. R. Abubaker and P. S. Boluk, "An Intelligent Model for Vulnerability Analysis of Social Media User," presented at the Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on, Vienna, Austria, 22-24 Aug. 2016.

[14] W. Daniel, X. Xu, M. Bai, Z. Chen, X. Meng, and Y. Wang, "Privacy Issues in Online Social Networks: User Behaviors and Third-Party Applications," in *Pacific Asia Conference on Information Systems (PACIS)*, 2014, p. 42.

[15] M. Mazza, S. Cresci, M. Avvenuti, W. Quattrociocchi, and M. Tesconi, "RTbust: Exploiting Temporal Patterns for Botnet Detection on Twitter," *arXiv preprint arXiv:1902.04506,* 2019.

[16] M. Apte, G. K. Palshikar, and S. Baskaran, "Frauds in Online Social Networks: A Review," in *Social Networks and Surveillance for Society*, T. Özyer Ed.: Springer, Cham, 2019, pp. 1-18.

[17] B. Ning, W. Junwei, and H. Feng, "Spam Message Classification Based on the Naïve Bayes Classification Algorithm," *IAENG International Journal of Computer Science,* vol. 46, no. 1, pp. 46-53, 2019.

[18] J. Komulainen, Z. Boulkenafet, and Z. Akhtar, "Review of Face Presentation Attack Detection Competitions," in *Handbook of Biometric Anti-Spoofing*: Springer, 2019, pp. 291-317.

[19] Y. Li, Y. Li, K. Xu, Q. Yan, and R. H. Deng, "Empirical study of face authentication systems under OSNFD attacks," *IEEE Transactions on Dependable and Secure Computing,* vol. 15, no. 2, pp. 231-245, 2018.

[20] A. Javed, P. Burnap, and O. Rana, "Prediction of drive-by download attacks on Twitter," *Information Processing & Management,* vol. 56, no. 3, pp. 1133-1145, 2019.

[21] A. U. López *et al.*, "Analysis of Computer User Behavior, Security Incidents and Fraud Using Self-Organizing Maps," *Computers & Security,* 2019.

[22] Z.-l. Xiong, C.-h. Xia, B. Sun, and M.-j. Hou, "Mining Similarity of Users in Location-Based Social Networks for Discovering Overlapping Communities," in *Recent Developments in Intelligent Computing, Communication and Devices*: Springer, 2019, pp. 417-428.

[23] A. U. López *et al.*, "Analysis of computer user behavior, security incidents and fraud using self-organizing maps," *Computers & Security,* vol. 83, pp. 38-51, 2019.

[24] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Systems with Applications,* vol. 117, no. 1, pp. 345-357, 2019 2019.

[25] K. V. Kumari and C. Kavitha, "Spam Detection Using Machine Learning in R," in *International Conference on Computer Networks and Communication Technologies*, India S. Smys, Ed., 2019, vol. 15: Springer, pp. 55-64.

[26] M. H. Dehkordi and H. Oraei, "How to construct a verifiable multi-secret sharing scheme based on graded encoding schemes," *IET Information Security,* vol. 13(4), 2019.

[27] P. Li, Z. Liu, and C.-N. Yang, "A construction method of (t, k, n)-essential secret image sharing scheme," *Signal Processing: Image Communication*, vol. 65, pp. 210-220, 2018.