Impact of Social Media Behavior on Security and Privacy Risks

#1PENCHIKALA KOUSALYA #2 K.UDAY KIRAN
#1 MCA Scholar
#2 Assistant professor
Department of Master of Computer Applications,
QIS College of Engineering and Technology

Abstract

Attacks and threats against the amount of time spent on online networks have been growing in tandem with the daily increase in the number of users of online social networks (OSNs). Attacks on OSN users take advantage of both system and user-induced weaknesses, which inevitably influences the hacker's approach. The purpose of this study is to look into how social media users' actions affect how vulnerable they are to privacy and security threats. Social media users in Turkey and Iraq were the subjects of the study, which used survey methods. The habits of 700 OSN users across two nations are recorded and examined in this study. In order to determine whether there is a correlation between the actions of social media users and security and privacy risks, this study looks at the behaviors of users from two different countries. The results of the study show a strong correlation between the views and behaviors of OSN users about security and privacy. Furthermore, compared to Iraqi users, Turkish social media users are more conscious of their privacy and security-related habits.

I. INTRODUCTION

The lives of billions of people now revolve around online social networks, or OSNs. These networks, which have attained extremely extensive penetration, are visited by people of all ages and from all parts of the world, and their prevalence is still growing [1]. Social media users can add other users, make user profiles, and view each other's activity thanks to social networks. Users of Facebook (FB), Twitter, and numerous other social media platforms can publish images, update and comment on almost anything every minute, and engage in a variety of other activities. These first appeared online and have since begun to proliferate on what are known as social network sharing websites. In a way, this evolution has stabilized and consolidated into the contemporary communication channel that we know as "Social Network Sites," which are networks that function through channels that allow individuals to engage with one another through the sharing of multi-media material [2]. The websites "We Are Social" and "Hoot Suite" released statistics on Internet, social media, and mobile users during the second quarter of

2019. According to the survey, there are 4.38 billion Internet users worldwide, which accounts for 56% of the global population. Of them, 3.48 billion utilize social media. Of the 4.02 billion Internet users in 2018, 42% (3.19 billion) used social media, according to Kemp's 2018 research [3]. Two-thirds of the global Internet population spend time on social networking sites, which accounts for 10% of all Internet time, according to Nielsen's social networks report "Global Faces and Networked Places" [4]. Our lives are significantly impacted by social media. However, as social networks have been more widely used, users' security concerns have grown in importance. According to study on online privacy views by Cranor et al. [5], social media users are quite concerned about their online privacy. Users are also worried about how their information will be used. Facebook is the ideal example to use to back up their assertions. Facebook gave application developers (NGOs, academics, analysis firms, software developers, etc.) access to a wide range of data in all user accounts in 2010. On the other side, the Global Science Research Company introduced a personality test application on Facebook in 2014. This application gave Facebook developers access to their friends' personal information as well as their own. In this way, the profiles of almost 50 million Facebook users were compromised. Following the event, Facebook offered the following explanation: "Passwords and sensitive information were not stolen or hacked; people knowingly shared their information and there was no entry to any system." [6]. Here, it is evident that information security is significantly impacted by the actions of Online Social Network (OSN) users. This study examines how users of social networks behave in relation to privacy and information security. Our goal is to ascertain how OSN user behavior relates to security and privacy. Users from two distinct cultural backgrounds—Iraqi and Turkish—are included in this study. As a result, the impact of cultural differences on security and privacy awareness is also examined. The remainder of the document is structured as follows: Related work is introduced in Section 2. Our work is described in Section 3. Our findings are shown in Section 4. Lastly, Section 5 provides a conclusion and recommendations for further work.

II. RELATEDWORKS

The growing influence of social media on daily life has prompted researchers to investigate how user behavior impacts security and privacy. This area explores how content sharing, friend networks, location tagging, and emotional expression contribute to digital vulnerabilities. Various studies have addressed psychological, technical, and algorithmic perspectives.

1. Behavioral Privacy Leakage

Gross & Acquisti (2005) were among the first to study privacy risks on Facebook, revealing how users often overshare personal information due to low awareness of privacy settings.

Liu et al. (2011) analyzed user profiles and found that even with privacy settings enabled, indirect information could be inferred through friends' activity, leading to **inference attacks**.

Merits: Identifies privacy gaps in user practices.
Demerits: Limited to earlier versions of social networks.

2. Oversharing and Location Exposure

Zang & Bolot (2011) studied geo-tagging and found that users inadvertently disclose real-time location, enabling **stalking, theft, or surveillance**.

Pontes et al. (2012) analyzed oversharing behaviors and showed that even non-sensitive posts can be exploited through **data correlation** and profiling.

Merits: Highlights risks of location-based content.
Demerits: Often overlooks real-time preventive mechanisms.

3. Social Engineering and Phishing

Jagatic et al. (2007) showed that personalized phishing attacks using social media data are significantly more effective than random ones.

Fire et al. (2014) demonstrated how attackers can build fake identities and infiltrate networks based on common interests and weak privacy barriers.

Merits: Explains real-world exploitation of public data.
Demerits: Focus is mostly on attackers, less on user defense.

4. Personality Traits and Risk Behavior

Ross et al. (2009) found a link between personality traits and information sharing, noting that extroverts tend to reveal more personal data, making them more vulnerable.

Tufekci (2008) emphasized that cultural and psychological traits influence privacy perceptions, leading to riskier behaviors online.

Merits: Adds psychological understanding to technical risk.
Demerits: Results may vary by region or demographic.

5. Privacy Settings and Awareness

Madejski et al. (2012) found a significant gap between users' intended privacy and actual settings due to complex UI design.

Egelman et al. (2013) proposed that even tech-savvy users underestimate how much of their data is visible to others, increasing the attack surface.

Merits: Focus on usability of privacy tools.
Demerits: Assumes users are passive rather than adaptive.

6. Algorithmic Profiling and Targeted Ads

Kosinski et al. (2013) used Facebook Likes to predict sensitive attributes like political orientation, sexual preference, and IQ with high accuracy.

Ghosh & Scott (2018) studied data brokers and showed how seemingly harmless data from social media can be repurposed for profiling, affecting insurance, credit, and employment decisions.

Merits: Exposes risks beyond the platform (third-party abuse).
Demerits: Focused mostly on Western data practices.

7. Youth Behavior and Vulnerability

Livingstone & Haddon (2009) studied children's behavior on social platforms, highlighting how curiosity, peer pressure, and lack of awareness lead to unsafe sharing.

Marwick & boyd (2014) analyzed teenage privacy strategies and found that young users engage in **"social steganography"** to hide meaning from unintended audiences.

Merits: Focused on at-risk populations.
Demerits: May not generalize to adult behavior.

8. Fake Profiles and Identity Theft

Kontaxis et al. (2011) showed how fake profiles can impersonate users to collect private data from their network.

Stringhini et al. (2010) demonstrated that automated bots could infiltrate social networks and harvest large volumes of private data.

Merits: Illustrates dangers of weak friend/follower filtering.

Demerits: Requires platform-level intervention to address.

III. SYSTEMANALYSIS

Existing System

Christo_des *et al.* [7] studied awareness of users' privacy on social networking sites and how this awareness is reflected in their attitudes, observing that although users have some awareness of privacy issues, they still reveal a lot of information about themselves. The reason for this was reported as being their desire to build their own identities. O'Brien and Torres [8] subsequently supported these findings with their 2012 study on the awareness of OSN users on privacy and how their behavior was affected by this awareness. In the study, they observed that the level of trust in social networking sites was low. In particular, they found that users older than 30 years of age were the least trusting group. However, they also observed that low trust levels did not affect what OSN users shared on social media. The youngest group (those between 18 and 21 years of age) was the one divulging the highest amount of information about themselves. Although users between the ages of 26 and 29 spent less time on social media compared to others, the number of their friends on social media accounts was found to be higher. At the same time, the 26 - 29 age group was found to be more cautious in using protective security tools, with a rate of 92.3%. On the other hand, a major finding of the study was that OSN users neglect security issues to ensure social interaction. The authors additionally remarked that both social media tools and

OSN users are responsible for the protection of privacy.

In addition, the rate of profile updates shows that OSN users do not feel uncomfortable about privacy. On the other hand, [9] observed that most of social media users are aware of security settings, but they do not change the default privacy settings. Madden [10] observed that half of social media users have difficulty in managing their privacy settings. In all, 48% of OSN users have difficulty managing the privacy controls on their social media accounts while 49% OSN users say that it is ``not difficult at all''. However, [11] reached analyzing the threats related to user activities, they observed that 68.90% of the users updated their privacy settings against threats and dangers that may come from the social media environment. They concluded that users generally are aware of and think about privacy settings, in addition to the fact that young users post more information at a higher rate than all other age groups. The authors observed that young online social network users are concerned about the confidentiality of information. In particular, 90% of them keep their privacy settings up to date. Nonetheless, a review of the literature suggests that a definitive judgment has not yet been reached on the variable observations of user behaviors regarding security settings.

Disadvantages

- The system is not implemented Hash Code techniques to find user behavior.
- The system decreases the usability of the suggested models and doesn't have an impact on reducing the effect of OSN based threats.

Proposed System

In order to collect data on user behavior, we applied the field research method in the study and obtained data using the questionnaire technique. The population, sampling, data collection tools, data analysis, and research hypotheses were determined within the framework of this methodology in the study.

In the proposed system, due to their behavior identification common usage, we selected three types of classical attacks used by the attackers. We investigated the behaviors of these attacks to identify the channel or the process that an attack pursues to penetrate systems. In most cases, attackers try to find open channels to access or to connect with OSN users. Through these channels, attackers can victimize OSN users. Each attack has its own policy to find an open channel(s) toward the victim. In this paper, we consider three main group of attacks which are Classic Threat (Internet Fraud attacks, Phishing, XSS), Modern Threat (Information Leakage attacks) and Threats Targeting Children attacks (Cyber Bullying attacks).

Advantages

- In the proposed system, significant techniques have used in which relationship between parents' follow-

up of their children's activities on OSN.

- In the proposed system, there is a strong techniques in which the behaviors of
  OSN users and their attitudes towards privacy/security.

IV. Methodology

Modules:

Admin

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as
Login, View All User and Authorize, View All Friend Request and Response, View All Users Datasets, View All Datasets By Block chain, View All Reviews, View All Attackers, View Behavior Type Results, View All Attackers Results.

View and Authorize Users
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

End User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Register and Login, View My Profile, Search Friend, View Friend Request, View My Friends, Upload Datasets, View All Datasets, Find Attack Type, View All Friends Review.

Methodology:

The methodology aims to systematically evaluate how individual and group behaviors on social media platforms contribute to security and privacy risks. A **mixed-methods approach** combining **data mining**, **user surveys**, and **behavioral analysis** is employed.

1. Research Design

- **Approach**: Mixed-method (quantitative + qualitative)
- **Objective**: To identify and quantify the relationship between user behavior (e.g., oversharing, tagging, public profiles) and resulting security/privacy threats.

2. Data Collection

A. Survey-Based User Data

- **Target Group**: 300–500 social media users (diverse in age, region, and platform usage)
- **Platform**: Google Forms / Microsoft Forms
- **Parameters Measured**:
  - Frequency of posting personal information
  - Use of location tags and hashtags
  - Privacy settings awareness

- Incidence of spam, phishing, or identity theft
- Demographic factors (age, gender, tech-literacy)

B. Social Media Behavioral Dataset

- **Source**: Public datasets or API scraping (e.g., Twitter API, Reddit data, or open Facebook pages)
- **Collected Features**:
  - Number of followers/friends
  - Post frequency and types (text, photo, check-in)
  - Engagement patterns (likes, comments, shares)
  - Privacy settings status (where available)
  - Use of links and external sharing

C. Case Study Reports (Optional)

- Analyze publicly documented cases of data breaches or cyberstalking via social media for real-world relevance.

3. Data Preprocessing

- **Anonymization**: All personally identifiable data is anonymized to comply with ethical research practices.
- **Cleaning**: Remove duplicates, irrelevant records, and non-English posts.
- **Categorization**: Group behaviors into high-risk, medium-risk, and low-risk clusters.

4. Feature Engineering

- Convert behavioral patterns into measurable variables:
  - overshare_score = weighted index of exposed personal details
  - privacy_score = level of control over shared content
  - engagement_score = frequency of interaction with unknown users

5. Data Analysis Techniques

A. Quantitative Analysis

- **Statistical Correlation**:
  - Use Pearson/Spearman correlation to identify relationships between behaviors and reported incidents.
- **Regression Models**:
  - Apply logistic regression to predict risk likelihood based on behavior patterns.
- **Cluster Analysis**:
  - Use k-means or hierarchical clustering to identify risk-prone behavior groups.

B. Qualitative Analysis

- Thematic analysis of survey responses to uncover common beliefs, misconceptions, or risky habits.
- Sentiment analysis (on posts/comments) to study emotional

triggers linked with impulsive sharing.

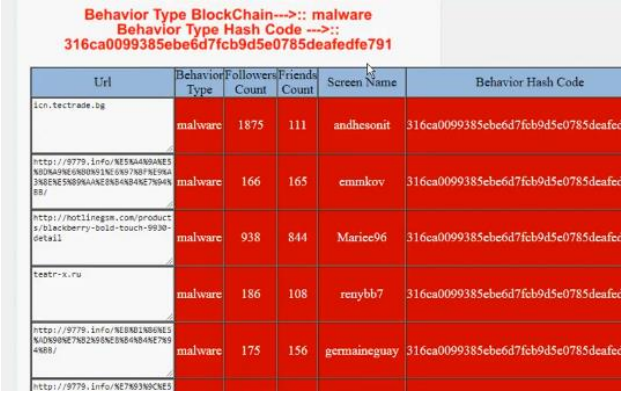
6. Risk Scoring Framework (Optional)

- Develop a **Behavior-Risk Scoring Model** to assign a risk level to each participant or profile based on:
  - Content sensitivity
  - Audience exposure
  - Network connections
  - Reported incidents

7. Validation & Evaluation

- **Cross-validation**: Applied to any predictive models.
- **Expert Review**: Cybersecurity experts may be consulted to validate the behavioral risk criteria.
- **Accuracy Metrics**: Precision, recall, F1-score (for model validation, if applicable).

V. RESULTS AND DISCUSSION



Behavior Type BlockChain--->:: malware
Behavior Type Hash Code --->::
316ca0099385ebe6d7fcb9d5e0785deafedfe791

Url	Behavior Type	Followers Count	Friends Count	Screen Name	Behavior Hash Code
lcn.tectrade.bg	malware	1875	111	andhesonit	316ca0099385ebe6d7fcb9d5e0785deafed
http://9779.info/%E5%A4%9A%E5%8D%A9%E6%B0%91%E6%97%8F%E9%A3%8E%E5%89%AA%E8%B4%B4%E7%94%BB/	malware	166	165	emmkov	316ca0099385ebe6d7fcb9d5e0785deafed
http://hotlinegsm.com/products/blackberry-bold-touch-9930-detail	malware	938	844	Mariee96	316ca0099385ebe6d7fcb9d5e0785deafed
testr-x.ru	malware	186	108	renybb7	316ca0099385ebe6d7fcb9d5e0785deafed
http://9779.info/%E8%B1%86%E5%A0%90%E7%B2%98%E8%B4%B4%E7%94%BB/	malware	175	156	germaineguay	316ca0099385ebe6d7fcb9d5e0785deafed
http://9779.info/%E7%93%9C%E5					

Fig1. Behavioral Type

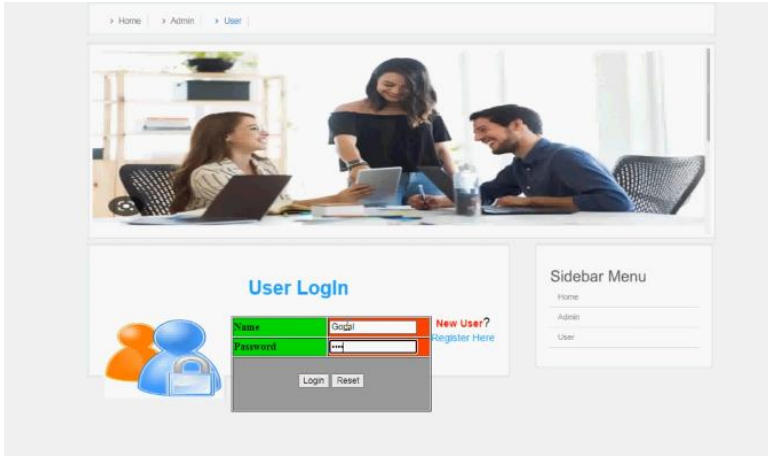


Fig 2. User menu

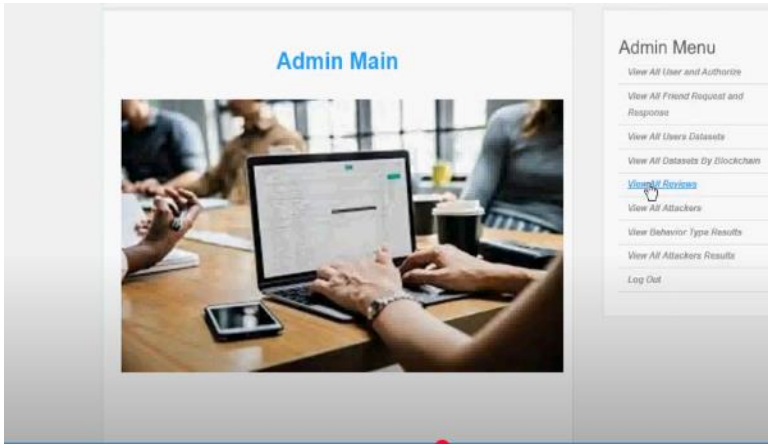


Fig 3. Admin Menu

VI. FUTURE SCOPE AND CONCLUSION

Our goal in this article was to examine the security and privacy practices of social media users. Our research involved conducting surveys in Turkey and Iraq to examine user behavior. Then, in order to illustrate how geography and culture impact user behavior, we examined data collected from social media users in Turkey and Iraq. Based on their actions, we then determined the two cultures' levels of susceptibility (insecure, moderate, and secure) to attacks

involving cyberbullying, information leakage and conduct, and online fraud.

Iraqi social media users use social media more regularly than Turkish users, according to the results of our behavior analysis. Furthermore, compared to Iraqi users, a greater proportion of Turkish social media users utilize pseudonyms. We found that when OSN users' Internet usage increased, so did their number of followers in the OSN environment. Given that the number of followers is linked to the perception of popularity on social media, this might be read as indicating that users of social media pay attention to and value the number of followers.

Furthermore, when social media users' opinions on parental follow-up are analyzed, Turkish OSN users are more likely than Iraqi users to think that parents should monitor their kids' online activity. Our study's findings simply showed that social media usage habits are influenced by cultural variations. We draw the conclusion that, for every kind of assault covered in our study, Iraqi social media users are more vulnerable than Turkish users. These findings have confirmed the notion that their views about privacy and security are significantly correlated with their behavior and the threats they are exposed to. Furthermore, it appears that OSN users' understanding of security and privacy will increase as they become more conscious of their social media activities. There appears to be a correlation between OSN users' growing security awareness and their growing privacy awareness. Since we could only get data from these two cultures for this study, the boundaries of this investigation are established by taking into account two cultures (Iraq and Turkey). We intend to investigate and evaluate the differences between additional civilizations as part of our future work. To further analyze our findings, we also intend to look at how user profiles—such as age, education, and so forth—affect user behavior. By taking into account various security attack scenarios, our article offers some fresh information and insights into the Security and Privacy Area with regard to user behavior. Two distinct recommendations are derived from our resource findings.
It is crucial that software security developers and security experts have thoroughly explained our findings. Then, taking into account the findings of our article, they should modify new security and privacy solutions according to user behavior and post-security attack treatment techniques. _ By strengthening security and privacy regulations, governments (Iraq, Turkey) and the private sector are encouraged to establish and continuously update the framework and resources for an effective social media communications system.

References

[1] R. Gross, A. Acquisti, and H. J. Heinz, ``Information revelation and privacy in online social networks," in *Proc. ACMWorkshop Privacy Electron. Soc.*, 2005, pp. 71_80.
[2] J. Nagy and P. Pecho, ``Social networks security," in *Proc. 3rd Int. Conf. Emerg.*

Secur. Inf., Syst. Technol., 2009, pp. 321_325.

[3] S. Kemp, ``The state of digital in April 2019: All the numbers you need to know," Tech. Rep., 2019. [Online]. Available: https://wearesocial. com/us/blog/2019/04/the-state-of-digital-in-april-2019-all-the-numbersyouneed-to-know/

[4] G. Faces and N. Places, ``A Nielsen report on social networking's new global footprint," Nielsen Company, New York, NY, USA, Tech. Rep., 2009.

[5] L. F. Cranor, J. Reagle, and M. S. Ackerman, ``Beyond concern: Understanding net users-attitudes about online privacy," in *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*. Cambridge, MA, USA: MIT Press, 2000, pp. 47_70.

[6] (2018). *5 Soruda Facebook Verilerini `Usulsuz Kullanmakla' Suclanan Cambridge Analytica*. [Online]. Available: https://www.bbc.com/ turkce/haberler-dunya-43469094[7] E. Christo_des, A. Muise, and S. Desmarais, *Privacy and Disclosure on Facebook: Youth and Adult's Information Disclosure and Perceptions of Privacy Risks*. Guelph, ON, Canada: Univ. of Guelph, 2011.

[8] D. O'Brien and A. M. Torres, ``Social networking and online privacy: Facebook users' perceptions," *Irish J. Manage.*, vol. 31, no. 2, p. 63, 2012.

[9] N. Aldhafferi, C. Watson, and A. S. M. Sajeev, ``Personal information privacy settings of online social networks and their suitability for mobile internet devices," 2013, *arXiv:1305.2770*.

[10] M. Madden, ``Privacy management on social media sites," Pew Internet Rep., 2012, pp. 1_20.

[11] K. Williams, A. Boyd, S. Densten, R. Chin, D. Diamond, and C. Morgenthaler, ``Social networking privacy behaviors and risks," Seidenberg School CSIS, Pace Univ., New York, NY, USA, Tech. Rep., 2009.

[12] N. B. Ellison, C. Stein_eld, and C. Lampe, ``The bene_ts of Facebook `friends': Social capital and college students' use of online social network sites," *J. Comput.-Mediated Commun.*, vol. 12, no. 4, pp. 1143_1168, Jul. 2007.

[13] P. B. Brandtzæg and J. Heim, ``Why people use social networking sites," in *Proc. Int. Conf. Online Communities Social Comput.* San Diego, CA, USA: Springer, 2009, pp. 143_152.

[14] S. M. Ghafari, A. Beheshti, A. Joshi, C. Paris, A. Mahmood, S. Yakhchi, and M. A. Orgun, ``A survey on trust prediction in online social networks," *IEEE Access*, vol. 8, pp. 144292_144309, 2020.

[15] A. Beheshti, V. Moraveji-Hashemi, S. Yakhchi, H. R. Motahari-Nezhad, S. M. Ghafari, and J. Yang, ``personality2vec: Enabling the analysis of behavioral disorders in social networks," in *Proc. 13th Int. Conf. Web Search Data Mining (WSDM)*. New York, NY, USA: Association for Computing Machinery, Jan. 2020, pp. 825_828, doi: 10.1145/3336191.3371865.

[16] V. Moustaka, Z. Theodosiou, A. Vakali, A. Kounoudes, and L. G. Anthopoulos, ``Enhancing social networking in smart cities: Privacy and security borderlines," *Technol. Forecasting Social Change*, vol. 142, pp. 285_300, May 2019.

[17] M. Tsay-Vogel, J. Shanahan, and N. Signorielli, ``Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and selfdisclosure behaviors among Facebook users," *New Media Soc.*, vol. 20, no. 1, pp. 141_161, Jan. 2018, doi: 10.1177/1461444816660731.

[18] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong, ``The effect of social in_uence on security sensitivity," in *Proc. 10th Symp. Usable Privacy Secur. (SOUPS)*. Menlo Park, CA, USA: USENIX Association, Jul. 2014, pp. 143_157. [Online]. Available: https://www.usenix.org/conference/soups2014/proceedings/presentation/das

[19] •. Sar_, ``Çocuk ve bili³im sanaldan gerçe§e sorunlar: Çözüm önerileri ve iyi uygulama örnekleri. SAMER yay_nlar_, accessed: Jul. 14, 2019," Tech. Rep., 2013.

[20] M. Anderson, ``Parents, teens and digital monitoring," Internet, Sci. Tech., Pew Res. Center, Washington, DC, USA, Tech. Rep., 2016.