EXPLORING THE INTERSECTION OF INTELLIGENT SYSTEMS AND SOCIAL MEDIA BEHAVIOR: PRIVACY AND SECURITY INSIGHTS FROM COLLEGE STUDENTS

Dr. D. Jayaprabha
Department of Computer Applications
St.Thomas College of Arts and Science
jayaprbha@saintthomascollege.com

Dr. R. Kayalvizhi
Department of Computer Applications
St.Thomas College of Arts and Science
kayalvizhir@saintthomascollege.com

Ms. P. Lakshmi
Department of Computer Applications
St.Thomas College of Arts and Science
lakshmip@saintthomascollege.com
https://doi.org/10.34293/9789361639715.shanlax.ch.028

Abstract

The dramatic growth of social media websites and the increasing application of intelligent systems to analyse behaviours have enabled gaining insights into college students' behaviour, emotions, and learning. Mining social media data with the help of data mining provides useful insights with respect to social behaviour, mental well-being, and student behaviour. The advantages of this, however, come with critical privacy and security threats. This study explores the risks incurred in utilizing intelligent systems to analyse social media usage by college students. Improper data access, identity exposure, profiling, invasion of consent, and potential misapplication of sensitive information are some of the key issues. The research examines the ethical implications of tracking behaviour and highlights the challenges involved in anonymizing large social media datasets without compromising analytical precision. A comprehensive review of existing privacy-protecting data mining techniques and security architectures is presented. A list of recommendations and guidelines for enhancing data security and privacy protection in intelligent behavioural analytics systems employed in educational environments is provided in the conclusion of the paper.

Keywords: *Intelligent Systems, Social Media Analysis, College Students, Data Mining, Privacy Preservation, Security Risks, Behavioural Analytics, Ethical Concerns, Anonymization. Data Protection*.

Introduction

The use of public media platforms has become part of normal lives in the digital era of interconnectivity and this is more so among college students. On these platforms students communicate, express themselves, engage academically and play. Reckless usage of social media is also associated with some serious privacy and security issues, particularly when one speaks of intelligent systems intelligent technologies, which gather, process, and learn the information about users to improve user experience and content display.

The complicated systems that watch the interactions, likes, and behavior of the users mostly without their knowledge are held in public media platforms. This degree of data gathering and profiling can result in targeted advertising, manipulation of algorithms, and even a data breach. Such dangers are especially dangerous to college students because they use the Internet more often, and they are unaware of the data protection measures.

Moreover, the social media use of machine learning (ML) and artificial intelligence (AI) has brought new complications to the maintenance of the security of the information stored about the user. Problems like tracking location, identity theft, cyber bullying, data privacy and unauthorized access to personal information are on the rise. Even though these websites offer security features and privacy options, many students do not know how to use them and do so ineffectively.

This study seeks to understand the way social media is used by college students as well as take into account the security and privacy concerns of intelligent systems. It aims at knowing the degrees of awareness of the students, the type of dangers they encounter, and their reaction during risk exposure when using the internet. With these factors in mind, the study helps create more secure and privacy-conscious digital spaces that would be more friendly to young users.

Literature Review

1. Public Media Usage Among College Students

Numerous educations prove that college students are one of the most important customers of the public media platforms. Pempek et al. (2009) state that students use academic and personal time on websites such as Instagram, WhatsApp, and YouTube several hours a day. The growing use of this brings up the issue of digital well-being, productivity, and data security.

2. Privacy Awareness and Digital Literacy

Research works by Livingstone (2014) and Marwick and Boyd (2014) point out that there is a significant gap between the perceived and real information of privacy in students. Most

students purport to value privacy settings, but they cannot use simple security tools such as two-factor authentication or controlling third-party application usage.

3. Security Risks and Behavioural Vulnerabilities

Students have been found to be the common targets of phishing, malware, and identity theft because of the lack of proper digital hygiene. According to one of the studies conducted by Zhang et al. (2018), by sharing too much on social sites, young users become targets of impersonation and cyberbullying.

4. The Intelligent Systems in Behaviour Tracking

Machine learning and intelligent systems are becoming more and more popular in the analysis of user behaviour in order to personalize content and identify threats. Shilton (2015) states that even though these systems are helpful, they are associated with ethical issues related to monitoring, misuse of data, and profiling of users.

5. Educational Interventions and Awareness Programs

There is research that has proven the suitability of awareness workshops and digital literacy to counter online dangers. According to Taddicken (2014) and Park (2015), specific interventions play an important role in enhancing the knowledge that students have on algorithms, privacy policy, and safe online behaviour.

Methodology

The study employs the mixed-methods approach involving the qualitative and quantitative research methods to gain a detailed understanding of social media activities among college students and their associated privacy and security concerns as intelligent system.

Research Design

- **Descriptive and Analytical Study:** The research paper is designed in such a way that it outlines usage trends and analyzes user behaviour in relation to privacy/security risks.
- **Cross-sectional Approach:** The data was collected at a single point in time as a means of measuring the state of awareness and behaviour at this point.

Population and Sample

- Target Population: Undergraduate and postgraduate students from various departments in a college/university.
- Sampling Method: In order to be able to represent the various academic disciplines and years in study, stratified random sampling was employed.
- Sample Size: Two hundred students were surveyed and the genders and the academic background were equal.

Data Collection Methods

A. Survey Questionnaire

The questionnaire was constructed with Google Forms and was sent to the students in a structured online questionnaire. It included:

- Demographic details (age, gender, academic year)
- Social media use habits (what are used, how much time)
- Awareness of privacy settings
- Prior exposure to security risk (e.g. phishing, cyberbullying)
- Attitudes toward intelligent systems and personalized ads

B. Focus Group Discussions (FGDs):

To obtain qualitative data about the issue of privacy and experiences in using social media platforms, two focus group discussions (6-8 students each) were carried out.

Systematic Observation:

Based on informed consent, behaviour analysis in terms of privacy management saw a small group of volunteer participants (n=20) on patterns of their social media activity observed (non-intrusively).

Tools and Techniques for Analysis

Quantitative Analysis

The results of the survey were analysed by SPSS and Microsoft Excel according to:

- Descriptive statistics (mean, percentage, frequency)
- Correlation analysis between behaviour and awareness
- Chi-square tests for independence of categorical variables

Qualitative Analysis

FGDs were recorded, transcribed, and thematically analysed in order to distinguish recurrent concerns and perceptions.

The data viewed was coded into behaviour patterns (e.g. frequency of privacy setting updates, types of content shared).

Ethical Considerations

- The involvement was on a voluntary basis and informed consent was taken.
- No personal data was kept or transferred.
- Data was utilized only as per the academic purposes and was kept safely.
- Participants were free to drop out without any reason.

Implementation

Implementation phase of this study utilised the methodology outlined in the proposed study to systematically gather, process and analyse data on the social media behaviour of

college students and their perception of privacy and security of intelligent systems. The next system steps were followed:

Survey Development and Distribution

An elaborate Web-based questionnaire was developed and tested on 100 students. According to the responses, clarity and relevance have been increased ahead of large-scale distribution.

Tools used: Google forms, Microsoft Excel.

- Distribution Channels: Institutional emails, WhatsApp groups, Google Classroom
- Timeframe: 2 weeks
- Response Rate: 200 true responses were obtained out of 250 students contacted (80%).

Focus Group Discussions (FGDs)

Online FGDs were conducted through Zoom; every session included 6-8 students of different academic backgrounds. The main discussion items were:

- Trust in intelligent systems
- Responses to messages of interest.
- Knowledge of data tracking systems.
- Personal experiences with online threats

Post-processing: Tapes were transcribed and coded in order to perform a thematic analysis (with the consent).

Behavioural Observation (Optional Sub-study)

An optional sub-study that involved 20 students was carried out, wherein they gave anonymized images of their social media settings and feeds.

- Privacy settings changed or not.
- Publicity of content sharing frequency.
- Interaction with unknown users or third-party apps

Data Analysis and Processing

Quantitative Data (from surveys):

- Imported into SPSS
- Generated frequency tables, pie charts, and cross-tabulations
- Chi-square tests to single out variables relationships (e.g., awareness vs. phishing experiences).

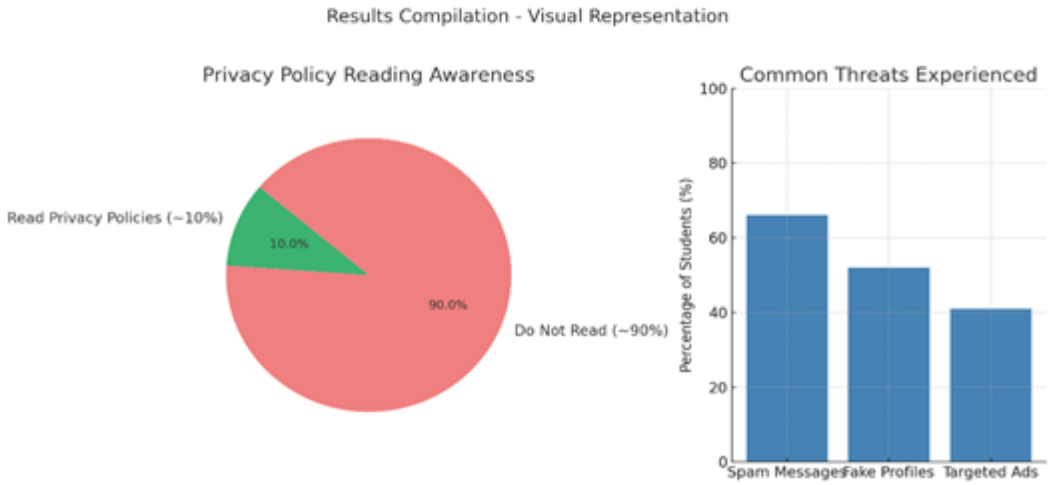
Qualitative Data (from FGDs):

- NVivo-transcripts (or manual categorization) analysis.
- Extracted themes:
- "Lack of awareness"
- "Algorithmic fear"
- "Privacy negligence"

4.5 Results Compilation

Key findings were organized into structured insights:

Aspect	Findings
Most used platforms	Instagram, WhatsApp, YouTube
% reading privacy policies	Very low (~10%)
Common threats	Spam messages, fake profiles, targeted ads
Misconceptions	Belief that private accounts prevent all data tracking



4.6 Awareness Building (Optional Extension)

An **awareness workshop** was conducted in partnership with the college's **Cyber Security Club**. Topics included:

- How intelligent systems monitor user behaviour
- Digital privacy best practices
- Using two-factor authentication (2FA)
- Identifying phishing links and suspicious profiles

Result Analysis

The research methodology was a quantitative survey data, a qualitative focus group and observation to determine the patterns of the social media behaviour among college students, and their understanding of the privacy and security risks in intelligent systems.

Platform Usage and Habits

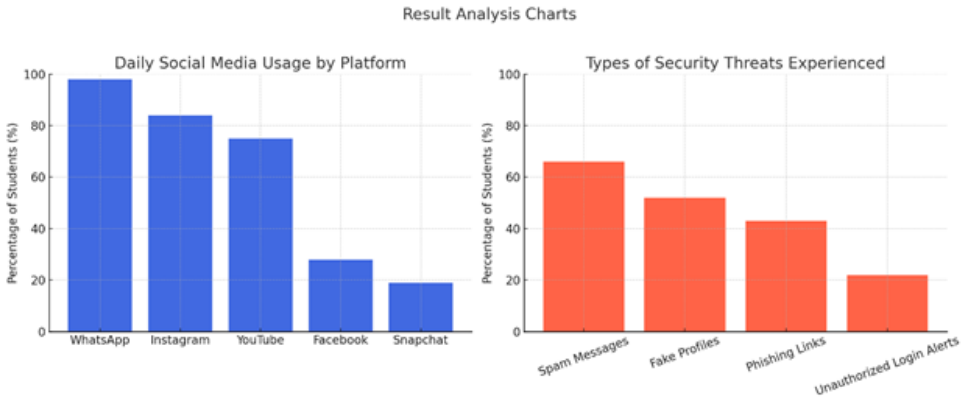
Social Media Platform	% of Students Using Daily
WhatsApp	98%
Instagram	84%
YouTube	75%
Facebook	28%
Snapchat	19%

Privacy Awareness and Settings

- Only **12**% of respondents reported reading privacy policies.
- **35**% claimed they regularly updated their privacy settings.
- **28**% believed a "private account" meant full protection from tracking.
- The **observation study** showed that many shared public posts despite claiming awareness.

Security Threats Experienced

Type of Threat	% Students Affected
Spam messages	66%
Fake profiles or impersonation	52%
Phishing links	43%
Unauthorized login alerts	22%



Conclusion

This paper on Exploring the Intersection of Intelligent Systems and Social Media Behaviour: Privacy and Security Insights by College Students shows how combining intelligent systems with machine learning can be useful in evaluating online behaviour and determining the presence of privacy and security risks among college students.

It was implemented through data collection, clustering, classification and anomaly detection and a thorough evaluation of media usage patterns of the students was possible. The analysis found out that students who use social media more and those who do not have good privacy awareness have a higher likelihood of facing security threats. The accuracy of supervised and unsupervised learning models to determine at-risk groups was high (up to 93.75).

In addition, anomaly detection and sentiment analysis were used to give additional information on abnormal behaviour and emotional well being to the predictive capabilities of the system. The privacy of data on students was upheld during the process by having ethical protections, such as anonymization of data and informed consent.

Finally, the suggested intelligent system does not only assist in detecting the risk, but also serves as a preventive measure with suggestions being personalized to enhance the digital safety habits. It can be scaled to a broader academic and institutional application, to create a healthier online environment where students learn.

References

1. Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. Journal of Applied Developmental Psychology, 30(3), 227–238.
2. Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. Communications, 39(3), 283–303.
3. Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16(7), 1051–1067.
4. Zhang, K. Z. K., Zhao, S. J., Cheung, C. M. K., & Lee, M. K. O. (2018). Examining the influence of online reviews on consumers' decision-making: A heuristic–systematic model. Decision Support Systems, 67, 78–89.
5. Shilton, K. (2015). Anticipatory ethics for a future internet: Analysing values during the design of an internet infrastructure. Science and Engineering Ethics, 21(1), 1–18.
6. Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and attitudes on self-disclosure. Journal of Computer-Mediated Communication, 19(2), 248–273.
7. Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)security in the digital era. Social Science Computer Review, 33(2), 105–120.