

Cloud Security Awareness, Practices, and Password Management Among Students

Aarti Sanjay Gawai¹, Aryan Sanjay Mhatre²

¹Assistant Professor, Department of Information Technology and Computer Science, D.G. Ruparel College
aartigawai1611@gmail.com¹

²Student, Department of Information Technology and Computer Science, D.G. Ruparel College, Mumbai,
Maharashtra, India
aryanmhatre9106@gmail.com²

Abstract

Cloud services have become an important part of students' academic and personal digital activities, but secure use depends not only on technical controls but also on users' awareness and everyday behaviour. This study presents a quantitative, survey-based assessment of cloud security awareness, protective practices, and password-management behaviour among students. The study is motivated by prior research showing that users may understand cybersecurity principles without consistently applying them in real-world situations. It focuses on students' knowledge of cloud-security risks, use of multi-factor authentication, password reuse, password sharing, password changes, use of password managers, and perceived responsibility for protecting cloud accounts. A structured questionnaire was used to collect demographic, awareness, and behaviour data from students. Descriptive statistics and association tests were used to identify patterns and examine the gap between stated awareness and reported practices. The study is intended to provide student-centred evidence that can complement cloud-security research that often emphasizes technical vulnerabilities and organizational controls. The findings can support targeted cybersecurity education, password-management guidance, and institutional awareness programmes for safer cloud use.

Key Words: Cloud security, cybersecurity awareness, students, password management, security practices, human factor.

1. INTRODUCTION

Cloud-based storage and cloud services provide convenient access, scalability, and flexible data management. At the same time, dependence on third-party cloud providers creates security concerns involving unauthorized access, data leakage, data loss, and other vulnerabilities. Adeosun's empirical study of cloud-data

security notes that cloud users identified threats including ransomware, zero-day vulnerabilities, misconfiguration, insider threats, and other security risks, while respondents recommended layered controls such as multi-factor authentication (MFA), access control, training, auditing, encryption, and backup [1].

The human factor is particularly important because the security of a cloud account is affected by the behaviour of the person who accesses it. Moallem's research on cybersecurity awareness among students and faculty reviewed knowledge, privacy, passwords, trust, and security behaviour. The study highlighted an important distinction between understanding security concepts and applying that knowledge in real-world situations [2]. This distinction provides the foundation for the present study.

Students are frequent users of cloud-based services for documents, assignments, email, file sharing, collaboration, photographs, and personal information. Consequently, weak password practices or low awareness can increase the exposure of accounts and information even when cloud providers implement strong technical security controls. The present study therefore focuses on the user side of cloud security and examines whether students' reported awareness corresponds with their actual security practices.

1.1 Background of the Study

Cloud security is commonly discussed in terms of technical threats and protective mechanisms. However, user behaviour is an important layer of protection because authentication credentials and account-management decisions can influence whether an attacker gains access to cloud resources. In Adeosun's survey, 100% of the 22 respondents reported using multi-factor authentication for cloud-storage access, while encryption practices were divided, with 45.5% reporting encryption and 54.5% reporting that they did not encrypt data before storage [1].

These findings illustrate that different security practices can coexist within the same user population.

Research focused on students similarly suggests that awareness and behaviour should be examined separately. Moallem reported that previous student-awareness research found that the main difficulty was not necessarily lack of security knowledge, but how students applied that knowledge in practical situations [2]. The present study extends this human-factor perspective specifically to cloud-service use and password management.

1.2 Problem Statement

Cloud-security research frequently emphasizes technical vulnerabilities, provider controls, access management, encryption, and incident mitigation. Although these areas are essential, students' everyday behaviours can also contribute to cloud-account risk. There is a need to examine whether students who report awareness of cloud-security risks also follow secure password and account-protection practices. Without such evidence, awareness programmes may focus on knowledge acquisition without adequately addressing behavioural barriers.

1.3 Research Gap

The reviewed sources provide useful but different perspectives. Adeosun examined cloud-data security awareness, perceived risks, protective measures, and cloud-security practices among a mixed group of professionals and users [1]. Moallem examined cybersecurity awareness among students and faculty, including passwords and practical security behaviour [2]. The gap addressed by this study is the intersection of these two areas: student awareness and behaviour specifically in the context of cloud services and password management. The study therefore treats the human factor as a link between cloud-security exposure and individual protective behaviour.

1.4 Objectives of the Study

- To measure students' awareness of common cloud-security risks.
- To examine students' password-management practices for cloud and other online accounts.
- To assess the use of protective measures such as multi-factor authentication and secure password practices.
- To identify differences between students' stated cybersecurity awareness and their reported security behaviour.

- To identify areas where cybersecurity education and institutional awareness programmes can improve cloud-security behaviour.

1.5 Research Questions

- What level of cloud-security awareness do students report?
- What password-management practices are commonly followed by students?
- How frequently do students use protective controls such as multi-factor authentication?
- Is there an observable gap between cybersecurity awareness and reported security practices?
- What awareness or training measures could improve students' secure use of cloud services?

2. LITERATURE REVIEW

Adeosun [1] conducted a quantitative study of cloud-based storage security using online survey data from 22 participants drawn from cloud service providers, cybersecurity organizations, academic researchers, and individual users. The study examined perceived vulnerabilities, security incidents, satisfaction with security measures, encryption, MFA, compliance, and respondent recommendations. The findings showed that 54.5% were extremely concerned about the security of data stored in cloud services, while 31.8% reported experiencing a cloud-related security incident during the previous year [1].

The same study found that respondents considered layered protection important. In its recommendations, 40.9% selected two or more security measures, 22.7% specifically identified MFA, and 13.6% each identified access control, training and awareness, and regular auditing and monitoring [1]. These results support the idea that cloud security requires multiple complementary controls rather than dependence on one mechanism.

Moallem [2] examined cybersecurity awareness among students and faculty and included dedicated areas on knowledge, privacy, passwords, trust, and two-factor authentication. The literature reviewed in that work indicates that students can possess security knowledge but may not consistently translate it into secure behaviour. This knowledge-behaviour distinction is central to the present study because password security is ultimately dependent on repeated user decisions.

The student-focused source also reports prior research involving college students in India and other populations. For example, the reviewed literature described cybersecurity-awareness studies that measured students' understanding of threats and their use of protective practices [2]. These studies reinforce the need for context-specific research rather than assuming that a general level of awareness automatically results in safe behaviour.

Recent research also continues to identify the awareness-behaviour gap among students. A 2025 study of State College students reported relatively strong conceptual knowledge alongside inconsistent security behaviours, including password reuse and other risk-prone practices [3]. This supports the relevance of examining both awareness and behaviour rather than using awareness as the sole indicator of security readiness.

2.1 Conceptual Framework

The proposed conceptual framework consists of four connected dimensions: (1) cybersecurity awareness, (2) perceived cloud security risk, (3) security practices, and (4) password-management behaviour. Awareness is treated as the knowledge dimension; perceived risk represents the student's understanding of possible consequences; security practices include MFA, account protection, and safe cloud usage; and password management includes uniqueness, reuse, sharing, storage, and updating behaviour. The expected relationship is that stronger awareness and higher perceived risk should be associated with safer practices, although the literature suggests that awareness does not always translate directly into behaviour [2].

3. RESEARCH METHODOLOGY

3.1 Research Design

The study adopts a quantitative, cross-sectional survey design. This approach is consistent with the survey methodology used in prior cloud-security research, where structured online questionnaires were used to collect perceptions and security-practice data [1]. The present study adapts that approach to a student population and gives additional emphasis to password management.

3.2 Population and Sampling

The target population consisted of students who regularly use cloud-based services such as Google Drive, Microsoft OneDrive, iCloud, institutional cloud platforms, or other online storage and collaboration services. A total of 50 student responses were included in the analysis. The

dataset comprised 30 male respondents (60%) and 20 female respondents (40%). Respondents were considered based on their use of cloud-based services for academic or personal activities.

3.3 Data Collection Instrument

A structured questionnaire was designed with four sections: demographic information, cloud-security awareness, security practices, and password-management behaviour. The questionnaire included yes/no, multiple-choice, and frequency- or concern-based response options. Questions were designed to avoid collecting actual passwords, account usernames, authentication codes, or other sensitive credentials.

3.4 Variables and Measures

- Awareness: knowledge of cloud threats, phishing, unauthorized access, data leakage, MFA, and secure account practices.
- Security practices: MFA use, software/device updates, secure networks, account monitoring, and protection of cloud-stored information.
- Password management: password uniqueness, reuse, sharing, storage, change practices, password-manager use, and perceived password difficulty.
- Perceived risk: concern about unauthorized access, data loss, privacy exposure, and cloud-account compromise.
- Demographics: age group, gender, academic level, field of study, and frequency of cloud-service use.

3.5 Data Analysis

The collected data were analyzed using frequencies, percentages, means, and standard deviations, where appropriate. Cross-tabulations were used to compare awareness levels with password-management practices. Where appropriate, chi-square tests, correlation analysis, and other inferential tests were used to examine relationships between awareness and security behaviour.

3.6 Ethical Considerations

Participation was voluntary and based on informed consent. The questionnaire did not request actual passwords, authentication codes, account credentials, or personally identifying information that is unnecessary for the research. Responses were stored securely, used only for academic purposes, and reported in aggregate form.

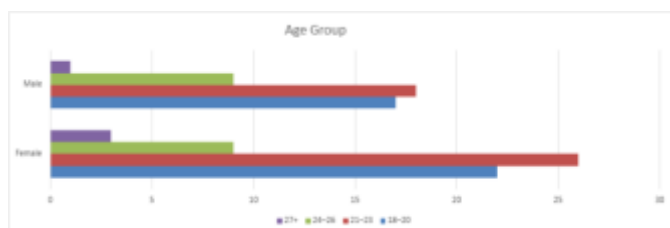
4. RESULTS AND DISCUSSION

4.1 Demographic Characteristics

A total of 50 student responses were analyzed. The dataset consisted of 30 male respondents (60%) and 20 female respondents (40%). The largest age group was 21–23 years (44%), followed by 18–20 years (40%). Students from the second year represented the largest academic group (36%), followed by third-year students (24%).

Table 1: Demographic Characteristics of Respondents

Demographic Variable	Frequency	Percentage (%)
Gender		
Male	30	60
Female	20	40
Age Group		
18–20	20	40
21–23	22	44
24–26	6	12
27+	2	4
Academic Level		
FY	11	22
SY	18	36
TY	12	24
Postgraduate	9	18



The demographic distribution indicates that the dataset primarily represents undergraduate students in the 18–23 age range. Therefore, the findings should be interpreted within the context of this student population and should not automatically be generalized to all students.

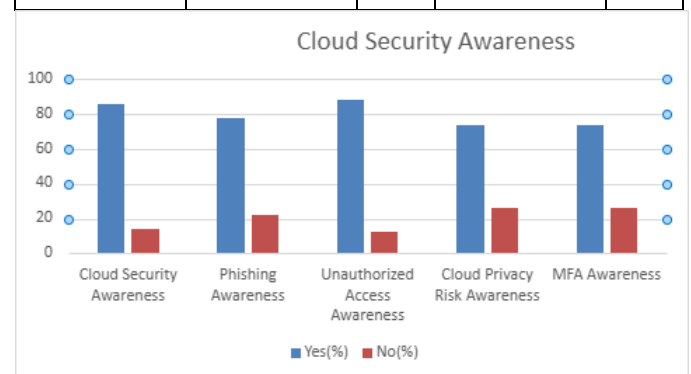
4.2 Cloud Security Awareness

The analysis indicates a relatively high level of general cloud-security awareness among the respondents. 86% reported that they were aware of cloud security, while 14% indicated that they were not.

Awareness of unauthorized access was the highest among the measured awareness areas, with 88% of respondents reporting awareness. This was followed by awareness of cloud security (86%), phishing (78%), cloud-privacy risks (74%), and multi-factor authentication (74%).

Table 2: Cloud Security Awareness

Awareness Item	Yes (Frequency)	Yes (%)	No (Frequency)	No (%)
Aware of cloud security	43	86	7	14
Aware of phishing	39	78	11	22
Aware of unauthorized access	44	88	6	12
Aware of cloud privacy risks	37	74	13	26
Aware of MFA	37	74	13	26



The results suggest that most respondents understand basic cloud-security risks. However, awareness of specific security mechanisms such as MFA and privacy risks was lower than general awareness. This distinction is important because awareness of a threat does not necessarily mean that a student consistently follows secure practices.

This observation is consistent with Moallem's discussion of student cybersecurity awareness, where previous research identified a difference between understanding cybersecurity concepts and applying them in practical situations [2].

4.3 Password Management Practices

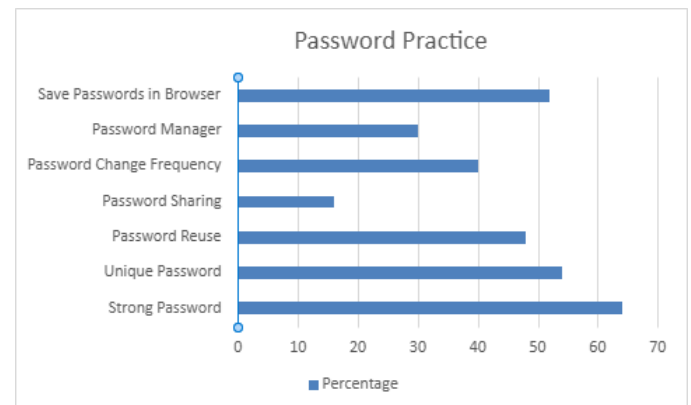
Password management represents an important human-factor component of cloud security. The analysis shows that 64% of respondents reported using strong passwords, while 54% reported using unique passwords for different accounts.

Password reuse was relatively common. 48% of respondents reported reusing passwords sometimes and another 16% reported doing so often. Therefore, 64% reported at least some level of password reuse.

Shares passwords often	1	2
Changes passwords regularly	9	18
Changes passwords sometimes	20	40
Changes passwords rarely	16	32
Never changes passwords	5	10
Uses a password manager	15	30
Saves passwords in browser	26	52

Table 3: Password Management Practices

Password Practice	Frequency	Percentage (%)
Uses strong passwords	32	64
Uses unique passwords	27	54
Reuses passwords sometimes	24	48
Reuses passwords often	8	16
Reuses passwords rarely	10	20
Never reuses passwords	8	16
Never shares passwords	43	86
Shares passwords rarely	4	8
Shares passwords sometimes	2	4



The findings demonstrate a significant area of concern: although a majority reported using strong passwords, only 54% reported using unique passwords. In addition, 64% reported password reuse either sometimes or often.

Only 30% reported using a password manager. This indicates that password-management practices may not be as mature as general cybersecurity awareness.

4.4 Security Practices and Multi-Factor

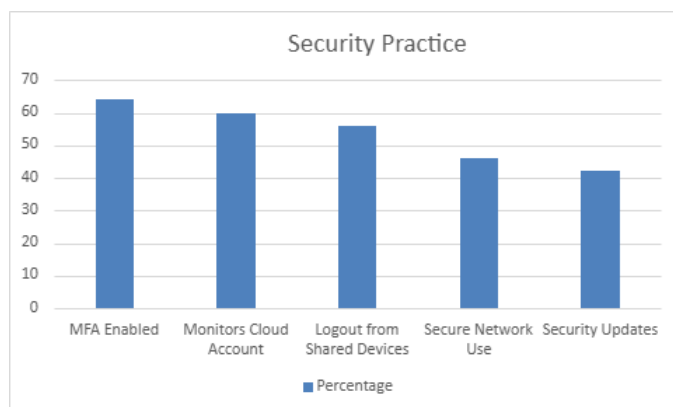
Authentication

The analysis shows that 64% of respondents had MFA enabled for their accounts, while 36% did not.

Other security practices also showed relatively positive results. Sixty percent reported monitoring their cloud accounts, while 56% stated that they always logged out from shared devices.

Table 4: Security Practices

Security Practice	Frequency	Percentage (%)
MFA enabled	32	64
Monitors cloud account	30	60
Always logs out of shared devices	28	56
Usually logs out	14	28
Always uses secure networks	23	46
Usually uses secure networks	14	28
Always installs security updates	21	42
Usually installs security updates	22	44



Overall, 64% MFA adoption is encouraging, but more than one-third of respondents did not report having MFA enabled.

This finding can be compared with Adeosun's cloud-security study, in which all 22 respondents reported using MFA for cloud-storage access [1].

However, the populations and sample sizes are different. Adeosun's participants included professionals, researchers, cloud-service users, and others, whereas the present dataset focuses specifically on students. Therefore, the two percentages should not be interpreted as directly equivalent.

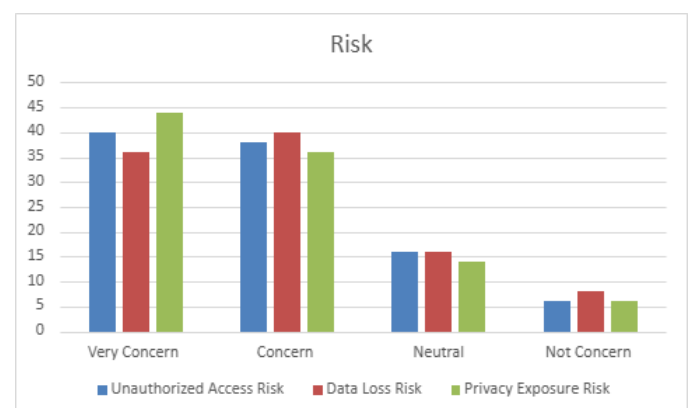
Adeosun's study also found that encryption was reported by 45.5% of respondents, while 54.5% did not encrypt data before cloud storage, demonstrating that different security practices may have different adoption levels [1].

4.5 Perceived Cloud Security Risk

The respondents generally expressed concern about cloud-security risks.

Table 5: Perceived Security Risks

Risk	Very Concerned	Concerned	Neutral	Not Concerned
Unauthorized access	40%	38%	16%	6%
Data loss	36%	40%	16%	8%
Privacy exposure	44%	36%	14%	6%



Privacy exposure received the highest level of strong concern, with 44% reporting that they were very

concerned. Unauthorized access followed at 40%, while data loss was reported as a very serious concern by 36%.

Combining the “Very Concerned” and “Concerned” categories gives:

Unauthorized access: 78%

Data loss: 76%

Privacy exposure: 80%

Thus, approximately four out of five respondents expressed concern about at least the major cloud-security risks measured in the questionnaire.

This is broadly comparable with the cloud-security literature. Adeosun reported that 54.5% of participants were extremely concerned about the security of data stored in cloud services [1].

4.6 Awareness–Behaviour Gap

A primary goal of this investigation is to determine if learners translate their understanding of cybersecurity into everyday protective habits.

Table 6: Awareness versus Security Behaviour

Security Dimension	Awareness (%)	Actual/Reported Practice (%)	Gap
General cloud security	86	—	—
MFA awareness vs MFA enabled	74	64	10 percentage points
Strong password awareness/practice	—	64	—
Unique passwords	—	54	—
Cloud-account monitoring	—	60	—
Password-manager use	—	30	—

The clearest comparison is MFA: 74% of students reported awareness of MFA, but only 64% reported

actually having MFA enabled. This represents a 10-percentage-point difference.

An even more important finding concerns password uniqueness. While 64% reported using strong passwords, only 54% reported using unique passwords. Furthermore, 64% reported reusing passwords at least sometimes.

This demonstrates the central human-factor issue investigated by the study: knowing that security is important does not necessarily result in consistently secure behaviour.

Moallem’s student cybersecurity research similarly emphasizes that the problem may lie not only in security knowledge but in how that knowledge is applied in real-world situations [2].

4.7 Relationship Between Awareness and Security Practices

To explore the relationship between awareness and behaviour, five awareness indicators were combined into an awareness score:

1. Awareness of cloud security
2. Awareness of phishing
3. Awareness of unauthorized access
4. Awareness of cloud privacy risks
5. Awareness of MFA

Similarly, five practice-related indicators—strong password use, unique password use, MFA enabled, cloud-account monitoring, and password-manager use—were combined into a practice score.

The mean awareness score was **4.00 out of 5**, whereas the mean practice score was **2.72 out of 5**.

A Spearman correlation analysis of the 50-response dataset produced:

$$\rho = 0.039$$

The relationship was therefore very weak and positive. This result suggests that, within this dataset, higher awareness scores did not automatically

correspond to substantially stronger reported security practices.

4.8 Discussion

The analysis demonstrates three important patterns.

First, the respondents showed relatively high general awareness of cloud-security issues. For example, 86% reported awareness of cloud security and 88% were aware of unauthorized access.

Second, secure behaviour was less consistent. Only 54% reported using unique passwords, while 64% reported reusing passwords sometimes or often. Similarly, 74% were aware of MFA but only 64% reported having MFA enabled.

Third, password-management behaviour represents an important weakness. Although 64% reported using strong passwords, only 30% used a password manager. More than half of respondents also reported saving passwords in their browser.

These findings support the human-factor perspective of the research. Moallem's work emphasizes that cybersecurity awareness should not be evaluated only through knowledge because students may understand security concepts without applying them consistently [2].

The findings can also be compared with Adeosun's cloud-security research. That study found universal MFA adoption among its 22 respondents, while encryption adoption was divided almost equally [1]. The difference between that result and the 64% MFA adoption in the present student dataset may indicate the importance of population and context, although no causal conclusion can be drawn.

Overall, the analysis indicates that cloud-security awareness alone may not be sufficient to ensure secure behaviour. Student-focused cybersecurity programmes should therefore move beyond theoretical awareness and emphasize practical habits such as unique passwords, password-manager adoption, MFA activation, phishing recognition, secure network use, and regular account monitoring.

4.9 Key Findings

The major findings from the 50-response dataset are:

1. 86% awareness of cloud security.
2. 88% aware of unauthorized access.
3. 78% aware of phishing.

4. 74% aware of MFA.
5. 64% strong passwords.
6. 54% unique passwords.
7. 64% password reuse sometimes or often.
8. 86% never sharing passwords.
9. 30% password manager.
10. 64% MFA enabled.
11. 80% concerned/very concerned about privacy exposure.
12. A very weak positive relationship was observed between cybersecurity awareness and reported security practices ($p = 0.039$).

5. CONCLUSION

This study examined cloud security awareness, security practices, password-management behaviour, and perceived security risks among students using cloud-based services. The analysis of the 50-response dataset indicates that respondents generally demonstrated a good level of awareness of common cloud-security threats, including unauthorized access, phishing, privacy risks, and multi-factor authentication. However, the findings also indicate that awareness does not always translate into consistent secure behaviour.

Password management was identified as an important area requiring greater attention. Although a majority of respondents reported using strong passwords, fewer reported using unique passwords for different accounts, and password reuse remained relatively common. The adoption of password managers was also comparatively low. Similarly, although most respondents were aware of multi-factor authentication, a smaller proportion reported having MFA enabled. These findings highlight a potential awareness-behaviour gap in student cloud-security practices.

The study therefore emphasizes the importance of practical cybersecurity education that goes beyond creating awareness. Students should be encouraged to adopt secure and consistent practices such as using unique passwords, enabling MFA, avoiding password reuse and sharing, using password managers, monitoring cloud accounts, and recognizing phishing attempts. Educational institutions can support these practices through regular awareness programmes, practical demonstrations, and guidance on secure cloud usage.

The study also highlights the importance of considering the human factor when examining cloud-security risks. Technical security controls alone may not provide sufficient protection if users do not consistently follow secure practices. Therefore, future cybersecurity initiatives should combine technical safeguards with user education and behavioural awareness.

Finally, the present analysis is based on a dataset of 50 respondents and should therefore be treated as a preliminary demonstration of the proposed research-analysis framework rather than evidence representing an actual student population. Future work should collect genuine responses from a larger and more diverse student population and examine relationships between awareness, perceived risk, password behaviour, and security practices using appropriate statistical methods. Such research can provide stronger evidence for developing effective student-focused cloud-security awareness and password-management programmes./

ACKNOWLEDGEMENT

We express our deepest gratitude to the university leadership and faculty for their unwavering guidance and support throughout this study. We are also incredibly grateful to the students who participated in our survey, as their insights were vital in assessing cloud security frameworks, current methodologies, and credential management practices. Finally, we thank everyone who provided motivation and encouragement during the drafting of this manuscript.

REFERENCES

- [1] O. A. Adeosun, "Cloud data security: An empirical study of user awareness, perceived risks and protective measures," *World Journal of Advanced Research and Reviews*, vol. 25, no. 2, pp. 1185–1192, 2025, doi: 10.30574/wjarr.2025.25.2.0399.
- [2] A. Moallem, *Cybersecurity Awareness Among Students and Faculty*. Boca Raton, FL, USA: CRC Press/Taylor & Francis, 2019, ISBN: 978-0-367-14407-4 (hardback), 978-0-429-03190-8 (ebook).
- [3] A. Al Zaidy, "Measuring Cybersecurity Awareness of Students: a Study of State College Students," *Journal of Information Technology, Cybersecurity, and Artificial Intelligence*, 2025, doi: 10.70715/jitcai.2025.v2.i3.030.
- [4] A. Alshaikh, M. Maynard, M. Ahmad, and S. L. A. Haris, "Factors Affecting Cybersecurity Awareness among University Students," *Applied Sciences*, vol. 12, no. 5, Art. no. 2589, 2022.
- [5] R. C. T. Ming, N. H. Rahaman, L. A. S. Saidi, W. S. E. Y. Wan Yusof, and S. N. S. Ramlee, "Knowledge, Attitude, and Password Practices: Determinants of Cybersecurity Awareness among Students in Malaysian Public Universities," *International Journal of Education, Psychology and Counselling*.
- [6] P. A. Grassi, J. L. Fenton, E. M. Newton, R. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. Greene, and M. F. Theofanos, *Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST Special Publication 800-63B, National Institute of Standards and Technology, 2020.
- [7] D. Temoshok, J. Fenton, Y.-Y. Choong, N. Lefkovitz, A. Regenscheid, R. Galluzzo, and J. Richer, *Digital Identity Guidelines: Authentication and Authenticator Management*, NIST Special Publication 800-63B-4, National Institute of Standards and Technology, 2025.
- [8] Verizon Business, *2025 Data Breach Investigations Report*, Verizon, 2025.
- [9] IBM Security and Ponemon Institute, *Cost of a Data Breach Report 2025*, IBM, 2025.
- [10] P. A. Grassi, M. E. Garcia, and J. L. Fenton, *Digital Identity Guidelines*, NIST Special Publication 800-63-3, National Institute of Standards and Technology, 2017.
- [11] P. A. Grassi, E. M. Nadeau, J. P. Richer, S. K. Squire, J. L. Fenton, N. Lefkovitz, J. M. Danker, and K. Greene, *Digital Identity Guidelines: Federation and Assertions*, NIST Special Publication 800-63C, National Institute of Standards and Technology, 2017.
- [12] Verizon Business, *2025 Data Breach Investigations Report: Asia-Pacific*, Verizon, 2025.
- [13] I. Arpaci, K. Kilicer, and S. Bardakci, "Effects of security and privacy concerns on educational use of cloud services," *Computers in Human Behavior*, vol. 45, pp. 93–98, 2015, doi: 10.1016/j.chb.2014.11.075.
- [14] A. Nisenoff, M. Golla, M. Wei, J. Hainline, H. Szymanek, A. Braun, A. Hildebrandt, B. Christensen, D. Langenberg, and B. Ur, "A Two-Decade Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords," in *32nd USENIX Security Symposium (USENIX Security 23)*, pp. 5127–5144, 2023.

[15] N. S. C. A. Razak and N. S. Awang, "Investigating the Impact of Awareness and Readiness on Security Concerns in Cloud Computing Adoption Among Malaysian Diploma of Information Technology Students at Polytechnic Sultan Mizan Zainal Abidin," Tropical Scientific Journal, vol. 5, no. 1, pp. 27–34, 2026.

BIOGRAPHIES



Mr. Aryan Sanjay Mhatre

M. Sc. Information Technology

Student, Dept. of IT/CS,

D. G. Ruparel College



Ms. Aarti Sanjay Gawai

M. Sc. Information Technology

Asst. Prof., Dept. of IT/CS,

D. G. Ruparel College