

Cloud Security and Privacy in Social Media Platforms

Pankaj Deepak Kulaye¹, Aarti Sanjay Gawai²

¹ Student, Department of Information Technology and Computer Science, D.G Ruparel College of Arts, Science and Commerce, Mumbai, Maharashtra, India

² Assistant Professor, Department of Information Technology and Computer Science, D.G. Ruparel College of Arts, Science and Commerce, Mumbai, Maharashtra, India

¹pankajkulaye31@gmail.com, ²aartigawai1611@gmail.com

Abstract - The current era of social media platforms extensively relies on cloud computing technology for data storage, processing, and service provisioning. While cloud technology supports high scalability and flexible service provisioning, it also poses various security and privacy threats. Data leakage, insecure application programming interfaces (APIs), account hijacking, cloud misconfiguration, unauthorized access, and denial-of-service attacks are some of the security issues that may impact users and service providers. This paper provides a literature review of cloud security and privacy in social media platforms. The paper analyzes major threats posed by the cloud environment to social media, their impact, and the security measures that can be leveraged to mitigate the risks. Encryption, multi-factor authentication, access control, application programming interface (API) security, monitoring, and security auditing are some of the common security measures that have been widely implemented. In addition, the paper also reviews the emerging approaches such as artificial intelligence, machine learning, privacy-preserving technologies, federated learning, and adaptive security. Overall, the paper concludes that existing and emerging security measures can be combined to enhance the security, privacy, and reliability of social media platforms hosted on the cloud.

Key Words: Cloud Security, Social Media, Cloud Computing, Data Privacy, Cybersecurity, Data Protection.

1. INTRODUCTION

Social media has seen a tremendous increase in usage in recent years, facilitating frequent communication and interaction among millions of social media users. As social media platforms continue to experience a steady increase in terms of users and data volume, the platforms increasingly rely on cloud technology for data storage, application hosting, and service provisioning. Cloud technology enables high scalability and demand-driven service provisioning; however, it also poses various security and privacy threats. With the extensive volume of data being hosted and processed in the cloud, social media and other online platforms have become more vulnerable to data leakage, application programming interface (API) insecurity, account hijacking, and denial-of-service attacks

among other security issues. The focus of cloud security in social media is on the security and protection of users' data, accounts, applications, application programming interfaces (APIs), and cloud infrastructure from cyber-attacks and unauthorized access. Some of the major security concerns in the context of cloud-based social media include data leakage, insecure application programming interfaces (APIs), account hijacking, cloud misconfiguration, unauthorized access, and denial-of-service attacks among others. Additionally, privacy is a related and critical aspect of cloud security in social media since the platforms contain a wealth of personal information of the users including photographs, videos, and private messages. Lack of adequate security and privacy measures in social media clouds can result in damage to the reputation of the organization, financial losses, and compromised user data. Therefore, encryption, authentication, access control, monitoring and auditing, and other related mechanisms are critical in enhancing cloud security and privacy of social media. The increased adoption and utilization of social media have led to the need to process and store a huge volume of data in the cloud. Specifically, figure 1 below shows the growth of social media users from 2019 to 2025.

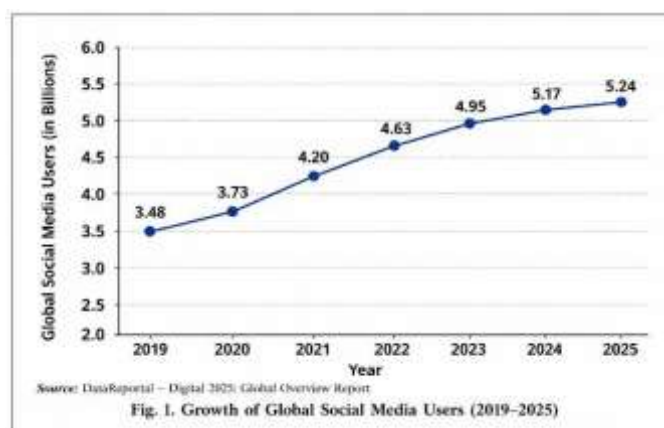


Fig. 1: Growth of the global social media user base (2019–2025)

Source: DataReportal, Digital 2025: Global Overview Report [15].

In addition to the increased volume of data, the changing dynamics and associated threats in the cloud environment necessitate the frequent evaluation and enhancement of security measures for cloud-based social media. In addition to traditional security measures, recent studies have focused on leveraging emerging technologies to enhance social media

cloud security. The paper will conduct a literature review of the existing and emerging security measures that can be used to enhance the security, privacy, and reliability of cloud-based social media. Figure 2 below provides the conceptual framework of the study.

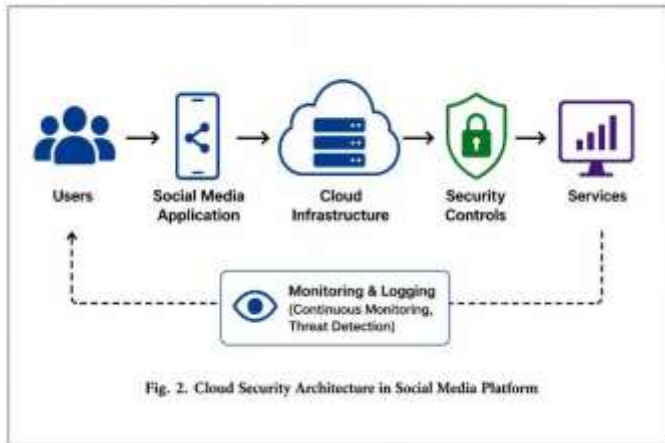


Fig. 2. Cloud Security Architecture in Social Media Platform

Fig. 2: Conceptual view of cloud-based social media platforms and security controls

Source: Author's own representation

2. LITERATURE REVIEW

With the increasing adoption of cloud technology in social media platforms, researchers have focused on addressing the numerous data privacy and protection issues associated with the adoption of the cloud in social media. The papers reviewed below address the issue from different perspectives; some focus on threats identification and analysis while others focus on the security measures and approaches that can be used to detect and mitigate the vulnerabilities. While different papers have focused on different aspects of the issue, it is evident that the security of data, applications, and cloud infrastructure in social media is inseparable from the manner in which the data and applications are managed.

Yadav et al. [1] have conducted a comprehensive review of security and privacy issues of cloud-based online social media. Their analysis focuses on addressing the range of threats that can compromise the information of the users and social networking services. A key observation from the review is that a significant volume of personal information is hosted and processed in social media, thus calling for the need to consider robust security and privacy safeguards. Sharadha [2] addresses specific security issues faced by social media in the cloud including insecure interfaces and APIs, data loss and leakage, shared technology weakness, and hijacked services. The review identifies that the weakness in the cloud infrastructure and related issues can result in compromising the confidentiality of social media information.

Bhatt [3] focuses on the mechanisms that can be used in social media to protect information being passed through the cloud. Vajjhala [4] addresses the cloud security models applicable in

the social network context, with a focus on the role played by various cloud security models in addressing the security challenges associated with the use of the cloud in social networks. Gawai et al. [5] have reviewed the impact of cloud security on social media to expound further on the threats posed by the cloud to social media and the countermeasures. In addition to revealing the threats posed by the cloud to social media including misconfigured cloud storage and hijacked accounts, the paper also reviews various countermeasures including encryption, multi-factor authentication, monitoring, security auditing, and access control. Recently, researchers have focused on examining the role played by artificial intelligence and machine learning in cloud security to mitigate the threats. Alzoubi et al. [6] have reviewed the application of machine learning and deep learning algorithms in the cloud security landscape. In a similar context and focus, Albshaier et al. [7] have addressed the application of federated learning in cloud and edge security with a focus on limitations and opportunities for privacy-aware applications. Rahdari et al. [8] have also reviewed the privacy and security issues in distributed cloud computing with a focus on distributed cloud computing and federated learning. The recent literature reviews offer more insight into the cloud security landscape in the context of social media by reviewing both traditional and emerging security measures. A number of authors have also reviewed the security and privacy of big data for cloud-based social networking services [9], cloud computing threats and controls [10], and cloud computing security issues [11].

3. MAJOR CLOUD SECURITY THREATS IN SOCIAL MEDIA PLATFORMS

Social media platforms highly rely on cloud infrastructure for the storage of data and service provisioning for millions of users. As a result, the platforms are exposed to a number of cloud-related security threats, which can compromise the privacy and security of the users. Based on the review literature, this section expounds on the common cloud-related security threats in the context of social media. The threats include data leakage and unauthorized exposure, insecure interfaces and APIs, hijacked accounts, cloud misconfigurations, unauthorized access, and denial-of-service attacks as illustrated in figure 3 below.

3.1 Data Leakage and Unauthorized Exposure

Social media platforms contain a wealth of personal information about the users. As a result, any form of unauthorized exposure of the information could result in adverse consequences such as loss of trust and damage to the reputation of the organization. Data leakage can occur due to inadequate control measures and/or misconfigured cloud storage. In addition, compromised accounts can also result in unauthorized exposure of data and information. Enhanced data encryption, proper access control, secure storage, and frequent

audits and monitoring of the social media systems can offer some protection against the threats.

3.2 Insecure APIs and Interfaces

Application programming interfaces (APIs) enable communication between different applications and the cloud in social media. In social media, APIs support features such as logins, messages, and content sharing. As a result, insecure APIs pose a great security threat to the system and the privacy and security of the data and information being processed and stored in the cloud. Poor authentication mechanisms, inappropriate authorization and access control, poor input validation, and misconfigured APIs can compromise the security of the APIs. Enforcing proper security measures such as strong authentication and authorization, enhanced input validation, monitoring, rate limiting, and security auditing can enhance the security of the APIs.

3.3 Account Hijacking and Identity-Based Attacks

In general, account hijacking occurs when an unauthorized entity gains access to a legitimate account and utilizes the account to conduct malicious activities. The hijacked account can be used to access private information such as messages and images or to gain access to other cloud services by exploiting the credentials of the account. In the case of social media, user accounts such as logins and passwords can be compromised by brute force and/or social engineering techniques, thereby posing a great threat to the privacy and security of the information. Where social media services are integrated with other cloud services such as online storage, the hijacked account can pose a more significant threat. Strong authentication measures such as multi-factor authentication and strong passwords, as well as frequent monitoring and detection of suspicious activities, can offer some protection against account hijacking and related identity-based attacks.

3.4 Cloud Misconfiguration

Cloud misconfiguration occurs when there are weaknesses in the cloud infrastructure, which could be easily exploited by an attacker to alter or wipe data or gain unauthorized access to the system. In the case of social media, misconfigured cloud resources and policies can create vulnerabilities and weaknesses in the system, thus compromising the privacy and integrity of data. Poor and/or unauthorized access control and isolation of cloud resources and services can also pose a great threat to the system integrity and confidentiality of the data. Frequent monitoring and auditing of the cloud policies, access control, and isolation of cloud resources and services can enhance the security and privacy of the social media platform.

3.5 Shared Infrastructure and Unauthorized Access

Cloud services are based on a shared infrastructure where multiple users share the same set of resources including

processors, storage, and virtual machines. In this case, appropriate resource isolation, access control, and authentication are critical in ensuring the security and privacy of the data and services since the unauthorized access or hijacking of resources could result in detrimental effects such as data tampering and deletion. Similar to cloud misconfiguration, unauthorized access occurs when an entity accesses another entity's information despite the lack of authorization. This can occur when the entity exploits weak access control policies and/or uses forged credentials to access the target data. Least privilege access control, proper authentication measures, resource isolation, and frequent audits and monitoring can enhance the protection of the social media cloud infrastructure against unauthorized access.

3.6 Denial-of-Service (DoS) Attacks

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks involve sending a huge amount of traffic to a server or network via a botnet. The objective of such an attack is to overwhelm the system causing it to crash or slow down significantly thus making it inaccessible to legitimate users. DoS and DDoS attacks are some of the most damaging attacks since they could be launched against social media platforms, which have become increasingly depended on in the current era of social media. The attacks can cause the platforms to be inaccessible, thus frustrating users and potentially damaging the reputation of the social media organization. Implementing traffic filtering, rate limiting, and protection through cloud infrastructure can provide some protection against DoS and DDoS attacks.

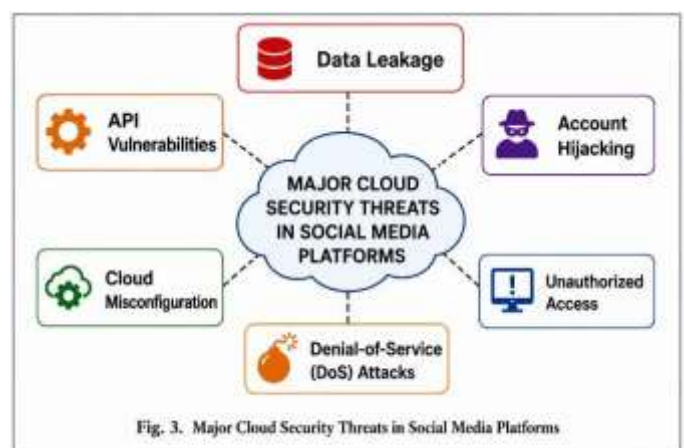


Fig. 3: Major cloud security threats in social media platforms

Source: Author's own representation

4. IMPACT OF CLOUD SECURITY AND PRIVACY ISSUES

Security and privacy issues may have a significant impact on social media based on the cloud. A security incident affecting a social media platform can expose personal information, allow modification of data, disrupt services, and decrease trust in the platform. Since social media platforms deal with a significant

amount of personal and generated data, the impact of the incident may go beyond the technical issues of trust, reliability, reputation, and even the business model.

4.1 Privacy and Confidentiality

As social media systems store and process personal information of a user on a frequent basis, privacy becomes one of the key concerns. The leakage of data or its unauthorized access can lead to its exposure and the loss of control of the information. Such an incident can also increase the risk of identity theft, fraud, targeting, and the misuse of data. Confidentiality measures such as encryption, authentication mechanisms, access control, and the corresponding procedures can ensure the privacy of the data.

4.2 Integrity and Unauthorized Modification

In addition to the confidentiality of data, its integrity is also of great importance, as any unauthorized modification can lead to adverse consequences. At first, an attacker may get unauthorized access to the user account, API, databases, or any other cloud resources. As a result, the information may be changed, deleted, or modified, thus reducing the reliability of the information and the services provided by social media. The use of authentication, tight permissions, activity monitoring, and security audits can help mitigate such issues.

4.3 Availability and Service Reliability

Social media users expect a high level of reliability and continuous operation of services. Denial-of-service attacks and the issues related to cloud infrastructure may limit the responsiveness of social media or temporarily shut down its operation. Such incidents may impact not only the user experience related to social media but also its reputation. Proper traffic management, monitoring procedures, backup systems, and the appropriate response mechanisms can help ensure service reliability and availability.

4.4 User Trust and Platform Reputation

Social media users expect their information to be protected and the services to remain available and reliable. The occurrence of a security incident, which may involve the unauthorized exposure of personal information, may affect the trust of the users in a platform. In particular, the trust level can decrease due to the adverse experience or the feeling that the information was not sufficiently protected. Thus, the reputation of a platform and its level of adoption may be impacted, which may be especially challenging for specific types of users. Therefore, it is essential to ensure not only the technical aspects of cloud security but also address the factors affecting user trust.

4.5 Legal, Regulatory, and Financial Consequences

The violation of data protection regulations, privacy rules, and other standards can have adverse consequences for the business model of social media based on the cloud. Notably, the unauthorized disclosure of information or its improper treatment may result in investigations, lawsuits, penalties, and additional expenses. Besides, the costs associated with incident response and the technical improvements to the infrastructure in terms of security and privacy should be taken into account. In addition, reputation risk factors should also be mitigated to avoid additional expenses.

5. SECURITY MECHANISMS AND CHALLENGES

There is a set of security mechanisms that can be employed to protect the social media platform. Since multiple elements, including user accounts, APIs, applications, cloud storage, and extensive personal information, should be protected, relying on individual components is not sufficient. Common measures include encrypting data, implementing authentication mechanisms and access control to protect the data and account, performing monitoring, protecting social media APIs, and conducting regular security auditing [12]. In addition, the mechanisms should align with the definitions of cloud service and deployment models [13]. Fig. 4 presents the key security mechanisms outlined in this section.

5.1 Data Encryption

Data encryption mechanisms transform information into a different representation that only the entities with the secret key can process or retrieve. Encrypting the information on the cloud infrastructure can protect it from being accessed and processed by unauthorized entities. Similarly, the encryption of data in transit allows its protection while it is transferred between systems and users. Therefore, the mechanisms can protect numerous types of information held by social media, including personal details, messages, photos, and videos. However, the success of such security measures also depends on the management of encryption keys, access control, and general protection.

5.2 Multi-Factor Authentication

Multi-factor authentication (MFA) is the use of two or more authentication factors to ensure that the system responds to valid user requests and denies access to unauthorized entities. In particular, a user can enter the password and a temporary code, which will be sent to their account, or provide a biometric sample. MFA can increase the security level as compared to single-factor authentication mechanisms. Being used in social media, the multi-factor authentication can protect numerous resources, including user data and cloud applications, from being compromised. In particular, hijacked accounts present a significant risk factor as an attacker can gain access to the sensitive information of a user and their associated cloud

services. Thus, relying on MFA can reduce the risk of such incidents.

5.3 Access Control and Identity Management

Access control mechanisms protect information and only allow its retrieval by authorized entities. In particular, identity and access management can secure various resources of a social media platform and ensure that only the rightful owner can modify or delete data. The principle of least privilege ensures that the user interacts with the information or systems they need. Applying the principle is especially important in the case of social media based on the cloud as it relies on the data of numerous users. If an unauthorized entity accesses one of their accounts, the loss of information can be significant. Besides, the principle of least privilege, when applied to applications and their interaction with the cloud, can limit the impact of compromise.

5.4 Security Monitoring and Anomaly Detection

The continuous detection of security-related incidents can significantly improve the protection of a social media platform as early identification of suspicious activity can help reduce the scope of an incident. In particular, monitoring can reveal the login attempts, denied access requests, API activity, and attempts to reach critical data and resources. Detection mechanisms can also flag suspicious activity, such as multiple failed login attempts, or identify anomalies that may indicate potential intrusions. Thus, having the tools to detect incidents can provide more time for the security teams to respond to the problem.

5.5 API Security and Security Auditing

The Application Programming Interface (API) provides an open connection between the social media and the cloud, so its protection is of great importance. Having effective protection mechanisms on the API makes it more difficult for an attacker to compromise the social media. Such mechanisms include authentication, authorization, input validation, rate-limiting, and security testing. In addition, the presence of tools to continually detect potential security issues can help secure the API and the system in general. Besides, regular security auditing can be viewed as a separate procedure to ensure that no vulnerabilities and weak points exist. Notably, social media based on the cloud requires regular and continuous auditing to ensure the stability of its protection.

5.6 Remaining Challenges

The outlined mechanisms provide substantial protection but do not guarantee that no security incident will ever happen. In fact, cloud environments are continuously evolving as new users, applications, APIs, and services are introduced. At the same time, attackers are also adapting and looking for ways to compromise systems. Therefore, it is essential to constantly update the mechanisms and rely on both the detection of

adverse activity and the prevention of unauthorized activities. Moreover, the application of protection tools should be efficient and should not impact the user privacy. Newer technologies, such as artificial intelligence and machine learning, can support the platform by identifying and responding to the issues in an automated manner, but their implementation and continuous use present additional challenges. In addition, such technologies should not impact privacy or provide false positives and negatives.

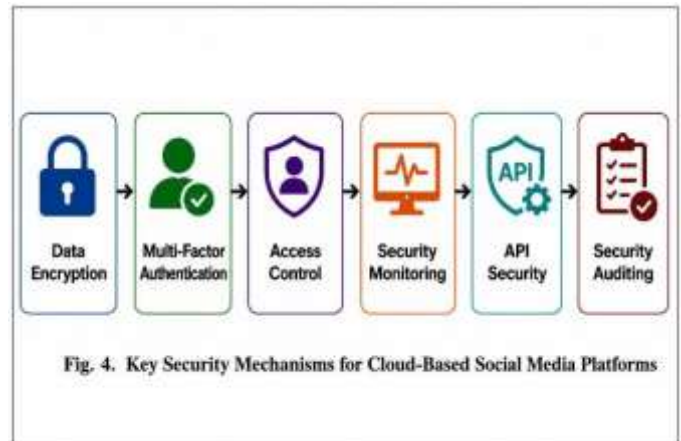


Fig. 4: Key security mechanisms for cloud-based social media platforms
Source: Author's own representation

6. FUTURE DIRECTIONS

The security of social media based on the cloud environment is continuously evolving. In particular, the increasing amount of data, services, and threats require the implementation of continuous monitoring and rapid response mechanisms. The latest research directions emphasize the need for continuous auditing, the use of artificial intelligence and machine learning to detect new threats, and the introduction of mechanisms to ensure user privacy. At the same time, the traditional sets of security controls, such as encryption, authentication, and access control, should not be replaced but rather complemented with newer technologies.

6.1 Artificial Intelligence and Machine Learning for Threat Detection

Artificial intelligence (AI) and machine learning (ML) can be a powerful tool for detecting threats and responding to incidents in the cloud environment of social media. In particular, ML algorithms can learn the behavior patterns of users, unauthorized attempts to access data, and other anomalies, thus rapidly detecting threats. The use of such tools is especially useful for continuous auditing, as they can detect patterns that would not be possible for the security team. Modern research emphasizes the importance of cloud security and the application of AI threat detection and ML techniques [6]. However, the application of such methods raises additional privacy and reliability concerns.

6.2 Zero Trust Security Architecture

Zero Trust is a concept that involves continuous verification as well as limited access [14]. Applying such an approach to social media based on the cloud environment can limit the impact of individual compromised accounts by adhering to the least-privilege principle. In particular, when using the concept of Zero Trust in the social media, an attacker will not be able to gain access to all the information and features they would be able to see if they took over an ordinary account. In addition to the general improvement of security, the approach can also significantly reduce the impact of a security incident, such as unauthorized data exposure or interference with the functioning of applications. The implementation of continuous verification and reduced privileges can provide better overall security for social media.

6.3 Privacy-Preserving Technologies

The future security of social media should incorporate technologies to ensure the privacy of personal information while allowing it to be used for processing and analytics. In particular, such technologies can ensure that the data is not exposed, allowing users to remain in control of the information. Applying differential privacy, access control mechanisms, and data protection analytics can improve the security level of a social media platform. The concepts of privacy-preserving analytics and distributed cloud security can also limit the amount of personal information that can be processed by a single system, thus further improving the level of protection.

6.4 Adaptive Security and Automated Response

The cloud is continuously evolving as new users, applications, APIs, and services are introduced or modified. Thus, the mechanisms to detect suspicious activity should also rapidly adapt to new threats. In addition to the continuous auditing, adaptive mechanisms can identify changes in the typical behavior pattern of the user or suspicious activity that might indicate a threat. In addition to detection, the mechanisms can also be automated to respond to a threat or even eliminate it before it impacts the operation of the entire system. Technologies, such as AI and ML, can automatically detect an incident, assess its scope, and take appropriate actions to mitigate it.

6.5 Federated and Distributed Learning

Federated learning is a concept that allows developing machine learning models without the need to gather all the data on one platform, such as the social media or cloud infrastructure. Thus, the data of users can remain on an individual account and not be transferred or processed by the social media. The concept limits the exposure of the data to a single entity, thus improving the level of security. Recent research has shown that federated learning can be employed in cloud and edge security to enhance personal data protection [7], [8]. However, the researchers have also identified concerns, including model security,

communication overhead, computational costs, and attacks on the federated learning pipeline. Federated learning is a promising technology, but many of the issues should be resolved before it can be applied.

6.6 Stronger Cloud–Platform Security Collaboration

The security of social media involves multiple entities, including user accounts, applications, APIs, cloud resources, and third-party services and analytics providers. Thus, the collaboration between the cloud platform provider and the social media company can improve the security level. In particular, both sides should have comprehensive auditing and response mechanisms to address and mitigate the potential threats. The proper allocation of responsibilities can also assist in identifying potential issues before they evolve into adverse consequences.

7. CONCLUSION

Cloud storage and processing present numerous benefits for the implementation of social media. However, relying on a single cloud infrastructure comes with significant risks and challenges. In particular, the loss of personal information, insecure APIs, account hijacking, misconfigurations, unauthorized access, and denial-of-service attacks pose significant threats to the operation of a social media platform. The review has shown that the application of encryption, multi-factor authentication, access control, API protection, security monitoring, and regular security auditing can help address the issues to a considerable extent. However, a set of measures is required to ensure the security of social media based on the cloud, and the mechanisms should continuously be updated and maintained. Addressing the challenges from all sides, including the cloud provider, will ensure better security and continuous protection.

The review has also demonstrated that emerging concepts, technologies, and standards, such as artificial intelligence and machine learning, can support the security aspects of a social media platform. In addition, the Zero Trust concept and federated learning provide additional protection. These technologies can be implemented alongside the traditional aspects of cloud security, such as access control, authentication, and encryption, to ensure robust and continuous protection for a social media platform.

REFERENCES

- [1] U. S. Yadav, B. B. Gupta, D. Peraković, F. J. García-Peñalvo, and I. Cvitić, "Security and Privacy of Cloud-Based Online Social Media: A Survey," in *Sustainable Management of Manufacturing Systems in Industry 4.0*, Springer, 2022, pp. 213–236, doi: 10.1007/978-3-030-90462-3_14.
- [2] K. Sharadha, "Cloud Security Issues and Impact on Social Media," *International Journal of Computer Applications*, vol. 2, pp. 26–28, 2015.
- [3] C. M. Bhatt, "Data Protection and Security Issues in Social Media," in *Cloud Computing Systems and Applications in Healthcare*, IGI Global, 2017, pp. 135–162, doi: 10.4018/978-1-5225-1002-4.ch008.

- [4] N. R. Vajjhala, "An Exploratory Analysis of Cloud Security Models in Social Networks," in *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)*, Salem, India, 2023, pp. 935–941, doi: 10.1109/ICPCSN58827.2023.00159.
- [5] A. S. Gawai, S. Chindam, and A. Jogdankar, "Impact of Cloud Security in Social Media," *International Research Journal of Engineering and Technology (IRJET)*, vol. 12, no. 3, pp. 272–276, Mar. 2025.
- [6] Y. I. Alzoubi, A. Mishra, and A. E. Topcu, "Research trends in deep learning and machine learning for cloud computing security," *Artificial Intelligence Review*, vol. 57, Art. no. 132, 2024, doi: 10.1007/s10462-024-10776-5.
- [7] L. Albshaier, S. Almarri, and A. Albuali, "Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities," *Electronics*, vol. 14, no. 5, Art. no. 1019, 2025, doi: 10.3390/electronics14051019.
- [8] A. Rahdari, E. Keshavarz, E. Nowroozi, R. Taheri, M. Hajizadeh, M. Mohammadi, S. Sinaei, and T. Bauschert, "A Survey on Privacy and Security in Distributed Cloud Computing: Exploring Federated Learning and Beyond," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 3710–3744, 2025, doi: 10.1109/OJCOMS.2025.3560034.
- [9] C. Stergiou, K. E. Psannis, T. Xifilidis, A. P. Plageras, and B. B. Gupta, "Security and privacy of big data for social networking services in cloud," in *2018 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2018, pp. 438–443, doi: 10.1109/INFOCOMW.2018.8406831.
- [10] F. Sabahi, "Cloud computing security threats and responses," in *2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, 2011, pp. 245–249.
- [11] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernández, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, Art. no. 5, 2013.
- [12] T. Grance and W. Jansen, "Guidelines on Security and Privacy in Public Cloud Computing," NIST Special Publication 800-144, National Institute of Standards and Technology, 2011, doi: 10.6028/NIST.SP.800-144.
- [13] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, National Institute of Standards and Technology, 2011, doi: 10.6028/NIST.SP.800-145.
- [14] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.
- [15] DataReportal, Digital 2025: Global Overview Report, 2025.

BIOGRAPHIES



Mr. Pankaj Deepak Kulaye

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