Cloud Connect: A Social Cloud Data Sharing Platform Using MERN Stack

Ashutosh Sharma, Prem Prakash Agrawal, Yashovardhan Awasthi
Department of Computer Science and Engineering, Sharda University, Greater Noida, India
17ashutoshsharma@gmail.com, premalwar@gmail.com, yashovardhanawasthi@gmail.com

ABSTRACT

With the arrival of the digital age, it has become easy to post moments online, but it commonly comes at the cost of privacy and control over personal data. Cloud Connect addresses this deficiency by offering a secure, user-centred alternative to mainstream social networks. Developed on the MERN stack and deployed on the AWS cloud platform, the site enables users to upload and store images or videos in a protected zone and share access with only specially selected followers. For greater privacy, all media and direct message content is encrypted with AES, while interactive features such as likes, comments, notifications, and encrypted conversations preserve the social media experience. Besides, a joined-up analytics dashboard provides valuable insights into audience behaviour and engagement trends, and it puts users in better touch with their content. With the convergence of cloud computing, next-generation web technology, and strong encryption, Cloud Connect proves that strong data privacy and social interaction can be successful online.

KEYWORDS: *Cloud computing, user-controlled access, social media, privacy, selective content sharing, AES encryption, MERN stack, AWS cloud, secure messaging, data security.*

1. Introduction

The rapid expansion of social media and the internet has transformed how people connect and exchange information worldwide [1]. From posting images to broadcasting in real-time, the web sites have facilitated ease and immediacy in communicating. Easiness is at the expense of forfeiting control and privacy. Content is stored on centralized servers where individuals have minimal control over who is granted access to it or how it is handled, and this raises issues concerning data abuse, privacy infringement, and unclear digital content ownership. Cloud Connect solves such problems.

It's cloud-based web-sharing social software based on the MERN stack on AWS cloud infrastructure [2,12]. The site provides individuals with the ability to securely upload, store, and share multimedia, with a selective model that makes only pre-approved followers able to see selected material. Besides secure cloud storage, Cloud Connect also possesses likes, comments, notifications, and end-to- end encrypted messages combining social media connectability with strong encryption security.

1.1 Rationale for the Study

Cloud Connect's vision emerges from increasing divergence between user needs and the workings of modern social networking sites. On the one hand, they need easy sharing and interaction; on the other, complete control over their own information[3]. And yet, the majority of sites currently exist to deliver maximum visibility and interactions at the cost of privacy. Targeted advertising, algorithmic visibility, and data profiteering have transferred control from the user to corporate domination.

Additional instances of cyberattacks, misuse of content, and surveillance online have further increase the awareness of data privacy. People and companies are becoming more interested in where their information is stored, who will be accessing it, and what protections are being taken. Cloud Connect meets all such concerns head-on with a secure platform for mind sharing, end-to-end encrypted messaging, and access controls based on the user.

1.2 Gap in Research

In spite of the plurality of spaces, there is a vast vacuum in current online existence. Social media platforms like Facebook [12], Instagram [13], and Snapchat are good at being engaging but have missing or vague privacy controls. People might feel that they are chatting in a closed circle, but changing algorithms, policy updates, and surreptitious permissions amplify their audience without permission. Content regulation is subdued, and the "personal" and "public" distinction is easily lost.

At the same time, cloud storage applications such as Google Drive[14], Dropbox [15], and OneDrive [16] offer protected data security and access control but none of social networking's socializing and community features. This is a begrudging trade-off: take advantage of secure storage at the cost of socializing or enjoy dynamic social websites at the cost of privacy.

Cloud Connect fills this gap by providing one portal that combines the social interconnectivity of social networks with the strength of cloud computing [17,18,19]. It is a perfectly proportionate solution where the users remain connected without giving up anything on their security due to selective sharing, end-to-end AES encryption, AWS-supported scale, and real-time interaction.

2. Literature Review

The last two decades have seen the digital communications space characterized by an uninterrupted stream of technologies all aimed at uniting the world even more [4]. From the initial networking sites of Friendster and Orkut to the interactive, multimedia-focused arenas of Instagram, Facebook, and TikTok, focus has been invariably on increasing reach, engagement, and retention. Though such sites have managed to create worldwide communities, they have also given rise to new issues specifically, those of data privacy, authorship of content, and selective sharing [20,21].

On the flip side, cloud storage platforms like Google Drive, Dropbox, and OneDrive have also proved to be safe and stable destinations for storage and sharing of information. They excel at scalability, encryption, and access control. They fall short in providing the interactive elements that allow users to linger on social websites. There is little room for spontaneous interaction, community building, or storytelling ,the heart of contemporary digital life.

2.1 Social Networking Platforms and Privacy Constraints

Facebook, Instagram, and Snapchat are social media giants with an ad model based on engagement. Although they do offer "Close Friends" lists or private profiles, these are typically hidden in nested settings and subject to constant policy shifts that could weaken their impact [23,24]. Ownership of the content is still a key concern once it's posted, media becomes the property of a wider database owned by the site and is susceptible to

being parsed for data, processed by an algorithm, or accessed by improper third parties. A 2022 survey by the Pew Research Center found that 81% of social media users are worried that corporations will exploit their personal information, yet they use it on a daily basis since they do not have suitable, privacy-focused alternatives [6,7]. Plans to incorporate enhanced privacy elements in current social websites clash with their models of business, and there is a conflict of structure between corporate interests and user security.

2.2 Cloud Storage Platforms and Their Engagement Gap

Concurrently, cloud services such as Google Drive, Dropbox, and Microsoft OneDrive have the secure storage and controlled access cornered. They enable users to explicitly define who is allowed to read and write a file, and they store and protect content in transit and on disk with encryption. But they're transactional, not relational designed to offer files, not enable rich, sustained interaction between humans [8,9,10].

They can only share a link to a folder and not dynamic interaction of likes, comments, live chat, or recommendations. Consequently, cloud platforms address security requirements but cannot support the requirement for community and interactivity that customers today have embraced on their virtual interfaces.

2.3 Hybrid Models and Their Limitations

A variety of hybrid solutions have sought to fill this gap between social exchange and secure storage. Software programs such as Flickr and SmugMug target groups of photographers and offer a mix of storage and social exchange integration. They have less management than enterprise cloud storage solutions, but they do not offer end- to-end encryption of sensitive material. Emergent decentralised networks like Mastodon and blockchain networks offer user independence and resistance to censorship at the expense of simplicity and recognisability in their pursuit of decentralisation ,rendering them inaccessible to the general user [11,12,13].

Moreover, hybrids rarely put selective sharing on a per-post or per-file basis first and let users choose exactly who can see their stuff. Rarely do they also include tight encryption methods such as AES for static and dynamic content and thereby have an open vulnerability in their security systems.

2.4 Explaining the Research Gap

We can observe from this review that the contemporary ecosystem imposes an artificial decision upon users: Enjoy the social media interactivity at the cost of privacy and control, or Enjoy the convenience of cloud storage without the benefits of an engaged, vibrant community [22]. This difference offers the research space for a product which combines the social feel of human contact with the uncompromising security of contemporary cloud technology. That type of product would have to bring selective sharing, end-to-end encryption, real-time communication, and scalability into being without burdening the user with onerous configurations.

2.5 How Cloud Connect Fills This Gap

Cloud Connect is best situated to be able to fill this gap. Connecting AWS cloud storage for stability, MERN stack coding for responsiveness and speed, and AES encryption for

impenetrable security, it's the best of both worlds without taking on their pitfalls. Compared to plain social media, users have complete control over who views their posts. Compared to plain cloud storage, the site includes likes, comments, stories, real-time alerts, and a custom analytics dashboard that actively engages users. By doing so, Cloud Connect not only solves the age-old conflict between social conversation and privacy but also establishes a template for the future of internet conversation, one in which users own their data, determine their audience, and still experience the richness of an active online community[25].

3. Proposed System

3.1 System Overview

Proposed system Cloud Connect is a web-based social cloud-sharing system with the objective of reconciling the social interaction of social networking and security and control of secure cloud storage. In essence, the system gives users control over who can view their uploaded material, a selling point widely promoted but rarely adhered to by mass-market services. Once the user uploads pictures or videos, they are safely stored in AWS cloud storage and encrypted so they are not accessible to unauthorised viewers. Not all of their followers gain automatic access; the user can even pick and choose which of their followers can view each piece of content.

This selective-sharing model never presents personal or intimate moments before the wrong crowds. The model uses the Advanced Encryption Standard (AES) to encrypt media and messages, two-factor authentication (2FA) to protect accounts, and role-based access control to implement strict security. Adding these features, along with an intuitive, interactive interface, Cloud Connect provides social networking benefits without compromising user privacy.

3.2 Architecture Design

Cloud Connect is a multi-layered and modular architecture for providing flexibility and sustainability: Frontend Layer (ReactJS) – Offers an interactive and responsive interface to surf, upload, and interact with content. The UI offers media upload windows, follower choice boxes, content streams, and chat windows.

Backend Layer (Node.js + Express.js) – Performs all the business logic, i.e., authentication, encryption/decryption operations, and content access control.

Database Layer (MySQL/MongoDB) – Stores metadata such as user profiles, followers list, access management, and analytics data.

Cloud Storage Layer (AWS S3) – Stores encrypted multimedia content and offers high availability, redundancy, and elastic performance.

Security Layer (AES + 2FA) – Offers end- to-end encryption of uploaded content and direct messages, and offers authorized login and access to data alone.

3.3 Module Descriptions

User Access & Access Control – Allows secure login with 2FA and maintains user-based permissions history for all uploaded media.

Media Upload & Selective Sharing – Allows media file uploads, choosing followers to view selectively, and securely storing the files in AWS S3.

Encrypted Messaging – Allows direct messaging between users with end-to-end AES encryption.

Real-Time Notifications – Informs users when they receive new content access, messages, likes, or comments.

Analytics Dashboard – Displays audience engagement, content visibility, and activity trends reports.

Admin Panel – Supports content moderation, platform administration, and user administration.

3.4 Data Flow / Workflow

Upload: User selects media files and specifies specific followers who need to be given access.
Encryption: Files are encrypted locally with AES prior to being uploaded to AWS S3.
Storage: AWS S3 stores encrypted files and file permission is stored in the database.
Access Request: If a selected follower wants to view the content, his/her identity and access rights are verified by the system.
Decryption: If permission, decryption is performed client-side and displays securely.

3.5 Technology Stack Justification

MERN stack has been utilized because of its efficiency, scalability, and flexibility. ReactJS has provided responsive UI performance, while Node.js and Express.js produce asynchronous requests with optimal efficiency. MongoDB/MySQL has stored user data and access records efficiently and quickly. AWS S3 has offered secure and scalable cloud storage space. AES encryption has been employed because of its widely documented strength and effectiveness in safeguarding large multimedia content.

4. Objectives

Final goal of Cloud Connect is to create and deliver a next-gen social cloud-sharing solution that balances the social media interactivity with privacy and reliability of secure storage in the cloud. Project goal is to provide users with the choice of their own data by not deciding to be private or socially engaged. Below are well-crafted objectives to direct the research and development effort:

4.1 Make Sharing Content Truly Selective

In order to offer a content-sharing site in which the user can easily establish, with precision, who can see their photos, videos, and other items. A strong contrast to today's vague and too liberal social media privacy settings, Cloud Connect will utilize a straightforward and simple follower chooser so that personal moments remain private.

4.2 Develop Secure and Scalable Cloud Storage

To leverage Amazon Web Services (AWS) capability to store user-uploaded multimedia

files securely in highly available and highly scalable setup. This goal will position the users to be able to upload many multimedia files without compromising their performance or exhausting capacity and still maintain redundancy as well as automatic backup functionality.

4.3 Do End-to-End Encryption for Privacy

To secure stored data and real-time communications with Advanced Encryption Standard (AES). Protecting information prior to departure from the user's computer, Cloud Connect makes sure that if a server is compromised, information will not be readable and secure. It is a safe solution because it makes sure that the sender and intended recipients are the only ones who know how to access shared data.

4.4 Support Rich, Real-Time Social Interactions

To include likes, comments, notifications, and end-to-end encrypted one-on-one messages ,all enabled by embracing socket-based real-time communication. It is to bring the social juice users have come to know and love on platforms like Instagram but to a privacy-conscious and controlled setting.

4.5 Deliver Personalised Analytical Insights

To develop an effective, responsive, and beautiful UI for ReactJS, optimized to run for desktop, tablet, and smartphone operating systems. Simplicity, minimalism, and usability will be the guiding philosophies, such that user-friendliness is never compromised at the expense of the security feature.

4.6 Provide Personalised Analytical Insights

To provide users with actionable real-time data in the form of expert-level analytics dashboard. The dashboard will show engagement rate on posts, follower action, reach, and trend in audience ,so users can more easily see how their posts are performing and adjust sharing activity accordingly.

4.7 Provide Platform Security, Reliability, and Readiness for Growth

To incorporate strong security features such as two-factor authentication (2FA), daily security scan, vulnerability test, and disaster recovery. Scalability will be introduced in infrastructure to make the platform support increasing numbers of users without ever degrading speed or security.

By doing all this, Cloud Connect will redefine sharing on the web ,showing the world what is possible with a social space in social media without sacrificing ownership and control of one's own data. The project will not only be an experiment in privacy-first online communities but as an incubator for future innovations in safe, user-sourced social networking.

5. Results and Discussion

Cloud Connect design and implementation offered an efficiently running web-based social cloud-sharing system that combined the privacy of secure cloud storage and social networking interactivity. Usability, security, and performance were tested for the system

and the results show that the objectives emphasized in Section 3 were successfully met.

5.1 Functional Achievements

Selective Sharing in Action – Photos and films can be uploaded to AWS cloud storage and shared with only selected followers. Test cases assured unauthorized users were unable to see or download these files even when they were getting explicit file links because of AES encryption and access controls.

Secure Messaging: The encryption-based instant messaging using AES maintained the confidentiality of message content. Even in a test scenario where network traffic was intercepted, the encrypted messages couldn't be decrypted unless the decryption key was in place.

Real-Time Interaction: Communication via Socket-Enabled features such as comments, likes, and notifications functions smoothly, resulting in an interactive user experience on par with mainstream websites.

Analytics Dashboard: All the users can see detailed reports such as post reach, engagement rate, and follower trend insights, which will help them make informed decisions for sharing content intelligently.

5.2 Performance Measurement

Load testing was done in order to verify system response against varying user loads:
Response Time: Even during 500 simultaneous user sessions, the mean API response time was less than 1.5 seconds.
Scalability: AWS S3 cloud infrastructure dynamically scaled to meet rising storage demands without any loss of performance.
Encryption Overhead: AES encryption incurred negligible processing overhead (about 0.3 seconds per file), within usability limits.

5.3 Security Assessment

Access Control Verification: Penetration test scenarios ensured that only the explicitly allowed followers were able to access uploaded files.
2FA Guard: Account intrusions were blocked in brute-force attack simulations, with the two-factor authentication control added as another layer of defense on top.
Data Privacy: Direct S3 object URLs or not, files were still requested to validate themselves via tokens, showing the integrity of the system's multi-layered security environment.

5.4 User Feedback and Usability

A limited number of beta testers (university classmates and professors) used the site and gave feedback:

Positive Feedback: Users appreciated the simple follower selection process, the ease of use of the upload interface, and per-file access control.

Suggested Changes: Testers suggested the addition of AI-driven content tagging to facilitate organisation, and scheduling of sharing of content.

5.5 Discussion

The findings indicate that Cloud Connect not only achieves its technical goal but also plugs a huge gaping hole in the modern digital world. By utilizing the selective- sharing accuracy of cloud storage and the interactive features of social networking, the system resolves the Privacy Paradox described in Section 1.2.
To the end user, the site is open and friendly but with tighter privacy controls than mass market rivals. From a technical perspective, the usage of MERN stack + AWS + AES encryption was acceptable on both scalability and security fronts at the expense of a loss of performance, which was not significant. This blending of usability and safety is one of the aspects of Cloud Connect that differentiates it from other cloud only storage programs as well as with traditional social networking sites.

6. Conclusion

In a time when social connectivity is generally traded in for personal privacy, Cloud Connect shows that the two are not necessarily at odds. This endeavor sought to solve a cornerstone problem of the online world ,the lack of a platform that allows effective social interaction without compromising content ownership and user control. By integrating the MERN stack, AWS cloud infrastructure, and AES encryption, we were able to produce a web application that is scalable, secure, and user-friendly while bridging the gap between social media's collaborative nature and the privacy-first policy of secure cloud storage.

The selective sharing mechanism, under which the audience can grant the ability to view something to specific followers, turned out to be the most important aspect of the platform, giving the fine-grained control that the mainstream platforms lack. The performance testing, security testing, and user testing all guaranteed that Cloud Connect not only fulfills its technical objectives but also delivers an intuitive, fast, and reliable user experience.

On a broader scale, Cloud Connect is not just a technical achievement; it is a statement of the kind of direction that digital platforms can go, towards systems that respect the agency of users, protect personal information, and also allow meaningful engagement. The effort itself is a proof-of-concept for a privacy-conscious, socially conscious platform that can inspire further innovation in the field.

References

[1] A. Smith, “Privacy and Information Sharing,” *Pew Research Center*, Jan. 2016. [Online]. Available: https://www.pewresearch.org/internet/2016 /01/14/privacy-and-information-sharing/
[2] M. Jackson, “The Privacy Paradox in the Digital Age,” *Journal of Information Security*, vol. 12, no. 3, pp. 45–58, 2021.
[3] Singh, R., Suyal, H., Shivhare, A., & Malviya, L. (2024, November). A stochastic hill climbing approach for power efficiency in cloud-based systems. In 2024 International Conference on Cybernation and Computation (CYBERCOM) (pp. 46-51). IEEE.
[4] Amazon Web Services, “Amazon Simple Storage Service (Amazon S3) Developer Guide,” AWS, 2024. [Online]. Available: https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html
[5] MongoDB Inc.,“Introduction to MongoDB,” MongoDB Documentation, 2024. [Online]. Available: https://www.mongodb.com/docs/manual/in troduction/
[6] Node.js Foundation, “About Node.js,” Node.js, 2024. [Online]. Available: https://nodejs.org/en/about/
[7] ReactJS, “Getting Started – React,” React Developer Documentation, 2024. [Online]. Available: https://react.dev/learn
[8] National Institute of Standards and Technology (NIST), “Advanced Encryption Standard

(AES)," *Federal Information Processing Standards Publication*, FIPS PUB 197, Nov. 2001.
[9] T. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed., Pearson Education, 2023.
[10] P. Kumar and S. Sharma, "Cloud Computing Security: A Survey," *International Journal of Computer Applications*, vol. 182, no. 42, pp. 1–7, Jan.
2019.
[11] S. Gupta, R. Mishra, and K. Jain, "Selective Content Sharing in Cloud Environments," in *Proc. Int. Conf. Cloud Computing and Security*, 2020, pp. 243–252.
[12] Facebook Inc., "Privacy Settings & Tools," Facebook Help Center, 2024. [Online]. Available: https://www.facebook.com/privacy/explan ation
[13] Instagram, "Privacy and Security Help," Instagram Help Center, 2024. [Online]. Available: https://help.instagram.com/196883487377 501
[14] Google, "Google Drive Security and Privacy," Google Drive Help, 2024. [Online]. Available: https://support.google.com/drive/answer/2 450387
[15] Dropbox, "Dropbox Security White Paper," Dropbox Help Center, 2024. [Online]. Available: https://help.dropbox.com/security
[16] Microsoft, "OneDrive Security, Privacy, and Compliance," Microsoft OneDrive, 2024. [Online]. Available: https://www.microsoft.com/en- us/microsoft-365/onedrive/security
[17] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, Jan. 2011.
[18] Kaspersky Labs, "Social Media Privacy Risks and How to Protect Yourself," Kaspersky Resource Center, 2023. [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/social-media- privacy
[19] J. Anderson and P. Rainie, "Americans' Attitudes About Privacy, Security, and Surveillance," *Pew Research Center*, Nov. 20 [Online]. Available:
https://www.pewresearch.org/internet/2019/11/15
[20] M. Armbrust et al., "A View of Cloud Computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010.
[21] M. Rosenblum, "The Case for Cloud- Native Applications," *IEEE Internet Computing*, vol. 18, no. 3, pp. 89–93, May -June 2014.
[22] Suyal, H., Singh, A., & Shrivastava, G. (2025). Privacy Preserving Efficient Worker Selection in the Cloud-Based Crowdsourcing Platform. Internet Technology Letters, 8(5), e70092.
[23] S. Wang, "User-Centric Access Control in Social Networks," *ACM Transactions on Internet Technology*, vol. 20, no. 2, pp. 1–25, 2020.
[24] C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, nos. 3–4, pp. 211–407, 2014.
[25] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," Cloud Security Alliance, 2023. [Online]. Available: https://cloudsecurityalliance.org/
[26] J. K. Kuan and H. Park, "Security and Performance Evaluation of Encrypted Multimedia Sharing Systems," *IEEE Access*, vol. 8, pp. 54132–54145, 2020.