*Journal of Advances and Scholarly Researches in Allied Education*
*Vol. 21, Issue No. 5, July-2024, ISSN 2230-7540*

# Enhancing Privacy on Online Social Networs: A comparative study of encryption techniques

**Vaishnavi Agrawal***

Studdent, Class 11th, Welham Girls School, Dehradun, Uttrakhand, India

Email: vaish075navi@gmail.com

***Abstract - The ability to connect with people all over the world and share private information has made online social networks (OSNs) indispensable to contemporary communication. Because of the serious privacy and security concerns that come with their fast growth, protecting user data is of the utmost importance. In order to improve OSN privacy, this study examines several encryption techniques. It discusses symmetric encryption (ECC and RSA) and synthetic encryption (AES) as well as hybrid methods that combine the two types of encryption. Using examples from well-known sites such as LinkedIn, Facebook, and Twitter, the research assesses the efficacy and practicality of various strategies. Key management, performance implications, and user experience maintenance are some of the challenges that are addressed while adopting comprehensive encryption. To further improve privacy protection in OSNs, the paper delves into upcoming developments in encryption technology, such as decentralized encryption approaches and algorithms that are resistant to quantum computing. In order to better understand how to improve OSN security, this article will provide a thorough examination of encryption's function in protecting user privacy.***

***Keywords: Online Social Network, Privacy, Encryption Techniques***

----------X----------

## INTRODUCTION

Online social networks (OSNs) have completely altered the ways in which people all over the world communicate, exchange information, and remain connected. Photos, videos, location data, private messages, and even more delicate details like names and birthdays have been collected by social media platforms like Instagram, Facebook, LinkedIn, and Twitter. Privacy and security are valid issues that arise from this massive data collecting. The need of protecting user privacy is growing in relation to the adoption of OSNs. Identity theft, unlawful data mining by other parties, and malevolent hackers attempting to profit from personal information are all sources of concern. Concerns over business or government monitoring and unauthorized access further highlight the need for strong privacy safeguards.

Striking a balance between users' right to privacy and the collaborative and open character of OSNs is never easy. The potential dangers and the degree to which users' data is exposed are often underestimated when users provide personal information. This emphasizes how important it is for OSNs to have robust privacy policies in place to protect user information. This study's overarching goal is to evaluate and contrast several OSN privacy-enhancing encryption techniques. The study's overarching goal is to determine which encryption methods are most successful in practical settings by comparing and contrasting symmetric, asymmetric, and hybrid encryption, as well as other commonly used OSNs.

### Encryption

Encryption is a method for protecting sensitive information by changing it into ciphertext. The decryption key is a secret code that only authorized parties with it may use to decode the original plaintext material. To put it simply, encryption makes data unintelligible to anybody who does not possess the correct decryption key. This effectively stops hackers from gaining access to and making use of compromised material. When data or communications are encrypted, not only is sensitive information protected, but the original data or communications are also guaranteed to stay untouched, which guarantees authenticity and integrity.

The simplest example of original information, or plain text, would be "Hello, world!" To the untrained eye, the ciphertext may seem like 7*#0+gvU2x, completely disconnected from the original plaintext. On the other hand, decryption is a simple logical operation; whomever receives the encrypted data and also has the key may easily convert it back into plaintext. As a defence mechanism, attackers have been attempting to deduce such keys using brute force attacks for many years. The processing power available to cybercriminals is becoming greater all

the time, which means that they may occasionally exploit flaws. There are two times when data must be encrypted: first, while it is "at rest," as in a database, and second, when it is "in transit," as in being accessed or sent between parties. The mathematical formulae used to convert data from plaintext to ciphertext are known as encryption algorithms. The key will be used by an algorithm to make predictable changes to the data. By simply reusing the key, the encrypted data may be decrypted from its seemingly random appearance. These are some of the most popular encryption algorithms: Blowfish, AES, RC4, RC5, RC6, DES, and Twofish. Historically used mainly by governments for clandestine activities, encryption is now an essential tool for organisations to safeguard their data and maintain user privacy.

- **Types of Encryption**

Each of the several forms of encryption has its own unique advantages and applications.

**Symmetric Encryption -** In this straightforward encryption system, the cypher and decryption processes share a single secret key. While public key encryption has been around the longest and is most well-known, it has one major limitation: in order to decode data, both parties must posses the key that was used to encrypt it. Included in the family of symmetric encryption algorithms are AES-128, AES-192, and AES-256. For large data transfers, symmetric encryption is the way to go since it's simpler and runs quicker.

**Asymmetric cryptography-** Asymmetric encryption, closely connected to public key cryptography, is a modern technique for encrypting and decrypting data using two distinct but related keys. An encrypted key and an open key are both in use. Data encryption relies on the public key, whereas decryption is accomplished by use of the private key (and inversely). Given that the public key is freely shareable online, its security is unnecessary.

One far more robust solution for protecting data in transit over the internet is asymmetric encryption. With the use of SSL or TLS certificates, websites are protected. You can get the public key from a digital certificate by sending a request to a web server; the private key remains secret.

**Data Encryption Standard (DES)-** The Data Encryption Standard (DES) was an older, symmetric key encryption technology. For DES to function, the sender and the receiver need to possess the same private key, since it is used for both encryption and decryption purposes. AES, which is more secure, has replaced DES. In 1977, the United States government implemented it as a mandatory standard for encrypting sensitive federal computer records. A case might be made that DES was the spark that ignited the contemporary encryption and cryptography business.

**Triple Data Encryption Protocol (3DES)-** As part of the Triple Data Encryption Standard, the DES algorithm was executed three times using three different keys. The single DES algorithm was progressively seen to be too vulnerable to brute force assaults, and the more robust AES was still being considered, therefore 3DES was mostly considered as a temporary fix.

**RSA-** An algorithm known as Rivest-Shamir-Adleman (RSA) forms the backbone of a cryptosystem, which is a collection of cryptographic algorithms used for certain security-related missions or services. As a result, browsers and VPNs are able to employ public key encryption while connecting to websites. Because it is asymmetric, RSA encrypts data using a pair of keys, one public and one private. The private key is used for encryption while decryption is being done using the public key, and vice versa.

**Advanced Encryption Standard (AES)-** One cypher that the United States government uses to secure sensitive data is the Advanced Encryption Standard, which was developed in 1997 by the National Institute of Standards and Technology (NIST) to replace the Data Encryption Standard. When using AES to encrypt and decode a message block, you may choose between three alternative key lengths: 128 bits, 192 bits, or 256 bits. When it comes to applications like databases and hard drives, AES is the go-to for safeguarding data when it's at rest.

**Cloud Encryption-** When you use cloud encryption, your data is encrypted using algorithms before being sent to the cloud. This is a feature that cloud storage companies provide. Customers of cloud storage providers should be well-versed in the provider's encryption rules and processes, as well as satisfied with the degree of security they provide.

Several cloud providers limit encryption to a subset of database fields, including passwords and account numbers, due to the increased bandwidth consumption that comes with encryption. This is often insufficient for some groups. As a result, they choose a BYOE approach, where they bring their own encryption software and handle their own encryption keys, to guarantee a degree of cloud computing security they are satisfied with.

Encryption as a Service (EaaS) is an alternative model that has evolved as a straightforward, pay-as-you-go service that cloud providers provide. With EaaS, clients are able to manage their own encryption in a shared environment.

**End to End Encryption-** Only the two users engaged in the conversation can decipher the messages sent and received using end-to-end encryption (E2EE). It is impossible for any other party, even a telco or ISP, to decipher the communications. From a security standpoint, most people consider E2EE to be the best option for private and secure internet communication. An example of an E2EE service in action is the popular messaging app WhatsApp, which boasts that its

users' communications are safe because of special "locks."

- **The Advantages of Using Encryption**

**Confidentiality and safety-** One way to stop data leaks is via encryption. If a device is encrypted, it will remain safe even if a hostile attacker acquires network access. This will make the attacker's efforts to consume the data ineffective. With encryption, only the receiver or owner of the data can decipher the message or data. As a result, malicious actors are unable to decipher and access confidential information.

**Regulations -** In line with industry rules and government legislation, organisations may secure data and preserve privacy by encrypting it. Particularly in the healthcare and banking sectors, there are clear regulations on data protection. As an example, the Gramm-Leach-Bliley Act mandates that banks inform their clients about the sharing and protection of their data. Financial institutions may comply with this statute with the use of encryption.

**Safe web surfing -** Users are also protected while using encryption when they are online. At one point in the early days of the internet, criminals discovered techniques to intercept and steal HTTP traffic that was not encrypted. Enterprises, publishers, and e-commerce providers were able to give consumers with a safe experience when the standard for encrypting online material using the safe Socket Layer protocol (SSL) developed. This standard was later superseded by the Transport Layer Security protocol. Customers feel more secure making online purchases or providing financial information when websites utilise encryption.

**Sensitive information is protected by encryption-** From online video conversations and e-commerce to social media, encryption is and will be a fundamental security component. Encryption is a standard practice for everything that may be kept or transferred. A user's or organization's ability to keep sensitive information secure from prying eyes depends on how well they stay abreast of encryption standards.

- **Difficulties with Encryption**

Even if attackers are aware that data or devices are encrypted, they will nevertheless attack. They think that if they try hard enough, they may succeed. Because even the most advanced tools could crack weak passwords at some point, this fact encouraged attackers to stay trying for a long time.

The sophistication of brute force assaults has grown in recent years, with the goal of decryption key discovery via the use of thousands—if not millions—of guesses. Organisations are becoming more resilient to brute force assaults with the aid of most recent encryption technologies and multi-factor authentication (MFA).

**LITERATURE OF REVIEW**

**Jain et al. (2021)** Online social networks (OSNs) have seen meteoric rise in popularity in recent years, thanks to rapidly developing technology. The capacity of OSNs to facilitate communication between users and their loved ones, acquaintances, and coworkers is a driving force behind this trend. The information that is posted on social networks and in the media may travel at a rapid pace, practically instantly, making it a tempting target for attackers. It is necessary to query about the secrecy and certainty of OSNs from several angles. When users submit personally identifiable information (PII) such as images, videos, or audio files, a plethora of security and privacy concerns arise. The perpetrator may use the divulged data for illicit ends. When children are specifically targeted, the hazards are magnified. This paper provides a comprehensive overview of various security and privacy problems, as well as current solutions, in order to solve these issues and ensure the safety of social network members. Through the use of cited data, we have also covered OSN assaults on a variety of OSN online applications. This is on top of the many defensive measures for OSN security that we have already covered. The poll concludes by outlining pertinent security principles, current concerns, and obstacles with building confidence in online social networks.

**Makarenko et al. (2020)** The implementation and commercialization of Wireless Sensor Network (WSN) technologies are heavily dependent on the security of the Internet of Things (IoT). Due to the inherent low power and resource limitations of IoT devices, it is crucial to pick a suitable encryption technique in order to secure communication in WSN. Therefore, to help choose the best method for a given application, we evaluate and contrast several symmetric block-based cryptographic algorithms in this work and provide comments on their capabilities. We choose AES, CLEFIA, DES, Triple DES, IDEA, PRESENT, SEA, SPECK, TEA, XTEA, and TWOFISH, among others, with varying block and key lengths. Power and memory use, throughput, and energy consumption are the metrics used to compare the algorithms. We use the Cooja simulator with z1 motes to do the comparison, and you can find the code in our GitHub repository.

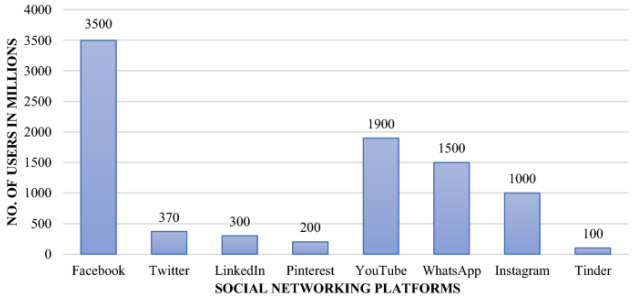
**Loren et al. (2019)** Modern communication systems place a premium on security, and cryptography is among the most secure technology available. Symmetric algorithms use just one key, whereas asymmetric algorithms use two keys; these two categories define the two main kinds of cryptography algorithms. But security concerns, key size, and latency make it hard to choose the best algorithms for different uses. Multiple forms of assaults, including brute force, man-in-the-middle, and cycle attacks, persist as threads in cryptographic systems. This study provides a thread-and performance-based comparison of several cryptographic

algorithms, highlighting which algorithms are best suited to certain kinds of applications.

**Azeez et al. (2018)** Due to the sensitive and confidential nature of certain data, such as health and financial records, individuals whose information must remain private have unfortunately faced significant risks. Encryption methods are employed to ensure the complete security of data during transmission and prevent unauthorized parties from accessing sensitive information. The primary function of encryption techniques is to secure data in transit against unauthorized access. Experts in banking, healthcare, and defense have developed various algorithms over the years to protect sensitive data, each varying in terms of speed, accuracy, reliability, and response time in data security applications. This study focuses on comparing the Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), and Data Encryption Standard (DES) algorithms to determine their effectiveness based on these metrics. The comparative evaluation aims to identify the most trustworthy, functional, and reliable encryption algorithm. The implementation of the system was carried out using C#. Experimental findings indicate that AES encryption is the fastest among the three algorithms, while RSA encryption consumes the most time. According to the assessment criteria used, AES emerges as the most efficient algorithm among the three. This report presents only a subset of the comprehensive findings gathered during the study.

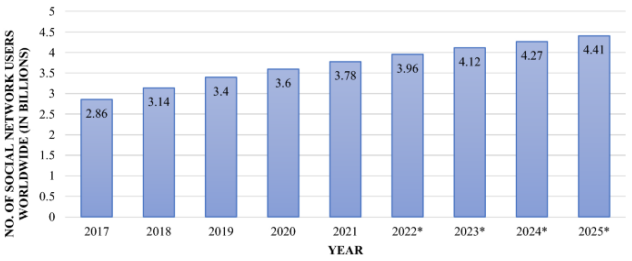
## DATA PERTAINING TO SOCIAL MEDIA AND INTERNET NETWORKS

The number of people using the internet is close to 4 billion. As of December 30, 2020, out of the entire population on the internet, the following numbers reflect the percentage of active users: 2.7 billion on Facebook per month, 330 million on Twitter, and 320 million on Pinterest. The number of users on various social networking sites is shown in Figure 3. Zephoria reports that the number of people who use Facebook on a monthly basis has increased by 16% over the previous year. On the dot, seven new profiles are generated. On a daily basis, users submitted 350 million images. Approximately 510,000 comments, 298,000 status updates, and 136,000 picture uploads occur every 60 seconds on Facebook. There is a significant likelihood of security issues due to the large volume of data posted to Facebook. Malicious material may be included in multimedia files or used with shortened URLs, allowing anybody to submit it. Approximately 83 million of these accounts are false, and they may belong to either real users or researchers and testers. Each day, hackers get access to around 1 lakh websites.



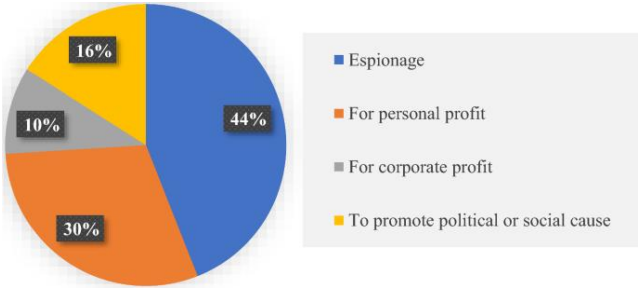

**Graph 1: Users number on different social networking platforms**

Graph 2 shows that the amount of data and information available on social networking sites has grown exponentially due to the sites' popularity. This has led to several cyber-crimes, such as data interception, privacy spying, copyright infringement, and information fraudulence, and has also raised the risk of information leakage. Some social media platforms, like Twitter, do not explicitly prohibit users from sharing personal information. However, skilled cybercriminals may still deduce sensitive data from users' online postings and profiles. Cybercriminals may be able to get our email addresses and passwords from the personal information we divulge online. To ensure that the scope of the research is manageable, we have reduced the list of networks taking popularity into consideration. So, it follows that the selected social networks use cutting-edge security measures. As a result, cutting-edge methods would be used in any assaults on these networks. The study is applicable to various social networks in a transitive sense.



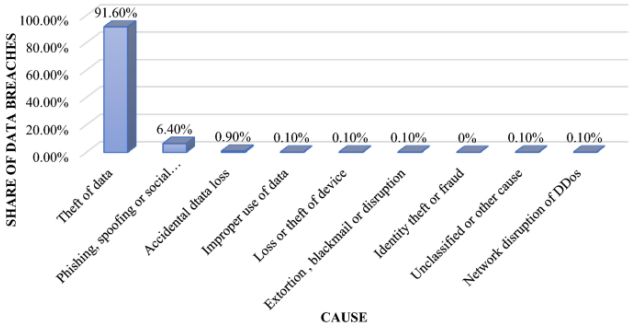

**Graph 2: Users Number (year-wise) on social media worldwide**

Graph 3 insights show the ranking of the most prohibited hacking techniques. This is in line with the results of a January 2021 study of American people. Approximately 44% of those who took the survey agreed that the harshest penalties should be reserved for cybercrime.




**Graph 3: Most punishable types of hacking in 2023**

Graph 4 shows the most susceptible methods for data breaches globally in 2021, arranged by the percentage of identities compromised. Identity theft or impersonation was the consequence of 91.6% of data breaches, as stated in the most current study.




**Graph 4: In year 2023 Leading cause of data breaches worldwide**

**EFFECTS, BOTH POSITIVE AND BAD, OF SOCIAL MEDIA SITES AS SEEN THROUGH THE EYES OF THEIR USERS**

When it comes to working together and seeing the world, social media has completely transformed people's perspectives. Social media platforms like Facebook and Twitter have made it easier for millions of people to keep in touch with loved ones far away because of their widespread use and low entry barriers. Social networks, like many technology breakthroughs, have both positive and bad aspects. We outline some of the benefits and drawbacks of social media based on the opinions of the researchers highlighted below.

- **Critical success elements of OSN**

1. Maintaining social relationships, selling products and platforms, participating in rescue efforts, and finding a similar group of individuals with whom to interact and share ideas are all good aspects that encourage users to build and utilise environments.

2. Keeping in touch with friends and family Keeping up with the lives of those we care about has never been easier than with social networking platforms. A person's social connections, including friendships, may benefit from this.

3. Advertising medium Professionals may connect with like-minded individuals and showcase their job expertise on career-focused social networks like LinkedIn or Plaxo. You may find greater work chances with their assistance. Social media advertising allows marketers to reach a wider demographic and influence their purchasing decision.

4. Efforts to rescue With the help of social media, rescue and recovery operations are able to get back on their feet after catastrophes. During these pivotal moments, when the traditional social order has crumbled, they bring people together. In order to help families find one other again, social media platforms make it easy to post bulletins. Using the tools made available by vital service providers via social media websites, the general population may be kept informed. It is easier for government officials to comprehend the situation and make educated judgements when they have access to real-time local information on social media.

5. Determining shared communities People with similar interests may easily locate one other via social networking sites. These communities allow people to express themselves freely, which in turn fosters a more accepting culture.

- **Causes of OSN's negative effects-**

1. Many studies have found, based on security parameters, that regular users encounter a number of problems while using social network platforms. For example, One kind of cyberbullying is the ease with which predators may locate potential victims. Ongoing concern among social media users pertains to the anonymity offered by these platforms. When someone was bullied, it was always done in person. But the best part is that anybody may now bully someone online without facing any consequences.

2. Despite the fact that making an account on a social networking site does not cost anything, the majority of their revenue comes from the adverts that appear on such sites. The exploitation of private information. Social media users' permission is not required before data is collected and sold to relationship brokers. In addition, enemies may use various attack methods to steal sensitive information about their targets from these websites.

3. Isolation: although social media has undoubtedly facilitated communication between users, it has also served to discourage face-to-face encounters. When compared to visiting or calling a friend in person, following their written remarks is far more convenient.

4. In terms of overall addiction, statistics show that social media use is much more problematic than cigarette and alcohol use. For many, going a whole day without checking their social media accounts might leave them feeling numb and down.

5. A comprehensive and methodical analysis of existing and future security risks and challenges is provided in this report. In particular, this research covers all the time-honored dangers that afflict the vast majority of social media users as well as the vast majority of the cutting-edge dangers that teens and young children face today. Sharing information on the safety and security of the social network is the main goal of this article. Readers will be introduced to every conceivable aspect of online social networks and the challenges surrounding them. Our findings shed light on the most pressing unresolved problems and open questions on how to make social media platforms more trustworthy.

6. Section "Statistics of online social network and media" details several pervasive social media dangers in the remainder organised paper. A discussion of the "Positive and negative effects of online social networks based on users perspective" explains why many are worried about the safety of social media. The section under "Various threats on online social network and media" delves into the remedies proposed by different scholars, then Some security-guidelines for users are included in the "Reasons behind online social media security issues" part, while the "Solutions for various threats" section confers answers to some open issues and challenges in online social media.

## INTERNET SOCIAL NETWORKS AND MEDIA FACE A NUMBER OF THREATS

Because of our technologically advanced culture and the widespread availability of the internet, we have expanded our means of communication to include the virtual realm. The following are examples of assaults that users have noticed when social networks first emerged.

As seen in Figure 1, we have classified threats as either conventional, modern, or targeted. Traditional dangers include those that users have encountered since the social network's inception. Both targeted assaults, in which an individual user is specifically targeted for malicious purposes, and modern threats, in which sophisticated methods are used to breach user accounts, are possible for any user to perpetrate.

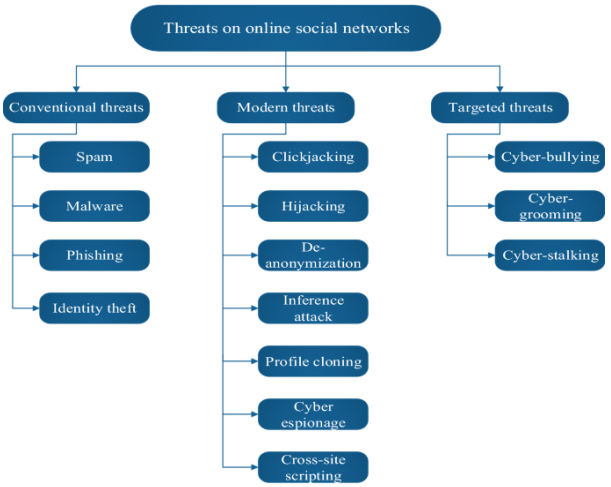



**Figure 1: Threat's Classification**

## REASONS OF SOCIAL MEDIA SAFETY VIOLATIONS IN THE DIGITAL SPHERE

Worldwide, social media is rapidly becoming one of the most distinctive, unstructured, and uncontrolled datasets in the modern world [88]. Millions of individuals use social media every day to share images, videos, and other forms of multimedia with their friends. Because of this, digital risk monitoring is being developed [89]. New security requirements introduced by the rise of web-based media placed customers (representatives, clients, and partners) squarely in the path of the attacker. Attackers now see social media as a new digital milestone because of how easy it is to target victims there. It has been one of the most significant threats to the authority's security. As seen in Figure 8, there are three reasons why attackers might affect social media:

**(a) The sheer number of individuals using social media:** assaults may quickly become viral because to the large number of people using these platforms for a variety of reasons. An attacker may broadcast malware that targets everyone or a specific group using hashtags, clickbait, and popular subjects. Physically, this is a huge obstacle for security professionals to overcome.

**(b) An adversary can take advantage of social media's trustworthy nature:** On sometimes, people may accept a friend request from someone they don't know only because they have common connections with the requester. Without giving any thought to the possibility of a security breach, they readily access the link that their friends have shared. With more than a third of social media users accepting friend requests from strangers, it's safe to say that online platforms are ideal for winning over a target's trust.

**(c) Complete anonymity from the security team:** Facebook, Twitter, and Instagram account for the vast majority of internet users. Security teams lack the capabilities to expand their visibility beyond a certain border into the social media realm, where workers are very susceptible to penetration, making

it incredibly difficult to monitor such a large population.

## COMPARATIVE EVALUATION

This section contrasted our survey, which examined various threat analyses and their defensive strategies, with other cutting-edge methods and surveys to highlight the innovations shown in Table 1.

| Encryption Technique | Type | Key Features | Advantages | Disadvantages | Common Algorithms | Use Case in OSNs |
|---|---|---|---|---|---|---|
| Symmetric Encryption | Private Key | Single key for encryption and decryption | Fast and efficient | Key distribution problem; less secure for large networks | AES, DES, 3DES | Securing stored user data, encrypting messages |
| Asymmetric Encryption | Public Key | Pair of keys (public and private) | Enhanced security, no need for key distribution | Slower than symmetric encryption, computationally intensive | RSA, ECC | Secure key exchange, encrypting private communications |
| Hybrid Encryption | Combination | Uses both symmetric and asymmetric encryption | Combines the speed of symmetric encryption with the security of asymmetric encryption | Complexity in implementation | RSA + AES, ECC + AES | Securing data transmission, end-to-end encryption |
| Homomorphic Encryption | Public Key | Allows computation on encrypted data without decryption | Enables secure data processing and privacy-preserving computations | Computationally expensive, slower than traditional methods | Paillier, BGV, GSW | Secure data analytics, privacy-preserving computations |
| Elliptic Curve Cryptography (ECC) | Public Key | Uses elliptic curves for key generation | Strong security with smaller key sizes, efficient | Complex implementation, patent issues (historically) | ECDSA, ECDH | Secure key exchange, digital signatures |
| Attribute-Based Encryption (ABE) | Public Key | Access control mechanism based on attributes | Flexible access control, fine-grained data sharing | High computational overhead, complex key management | CP-ABE, KP-ABE | Secure data sharing, fine-grained access control |
| End-to-End Encryption (E2EE) | Combination | Encrypts data on sender's side and decrypts it on receiver's side | High level of privacy, secure communications | Key management can be challenging, not effective if endpoints are compromised | Signal Protocol | Secure messaging, private communications |

## CONCLUSION

Online social networks are becoming an essential component of the widely connected world. Social networks are now able to interact with people on a regular basis because to this paradigm change. Due to the rise in social media use, it is necessary to educate consumers about the risks, assaults, and privacy concerns associated with these platforms. Technology has advanced, and social media now exists in many different ways. People may relate to one another in a variety of ways. Netizens have unparalleled access to professional websites, discussion forums, multimedia sharing networks, and much more. Regrettably, users' ignorance of security and privacy risks might result in a variety of cyberattacks via social media. Despite the fact that academics has developed creative approaches to handle the security precautions related to social media security, these approaches lack practicality and real-world application. As a result, it is essential that security vulnerabilities in social networks be reviewed often and iteratively in order to stay up with technological advancements. In order to defend social network users from a variety of assaults, we used a variety of models, frameworks, and encryption approaches to address various situations relating to online social network risks in this study. To make our survey more clear, we have included many solutions and compared analyses of other surveys. Many of these privacy-related problems haven't been fixed yet, however. Apart from implementing defensive measures, parents also need to keep a close eye on their children while they use online resources like OSNs. In general, researchers have a big part to play in OSN defence against these threats, but certain problems still need to be addressed using a combination of frameworks, hybrid approaches, and threat detection technologies.

## REFERENCES

1. Al-Saggaf, Y., & Islam, M. Z. (2015). Data mining and privacy of social media users: Implications of the data mining of Facebook profiles. Journal of Information, Communication and Ethics in Society, 13(1), 39-59.

2. Ali, A., & Abid, F. (2018). Enhancing privacy in online social networks using a user-centric approach. IEEE Access, 6, 20991-21005.

3. Bansal, C., Bhattacharya, S., & Murtuza, A. (2019). Privacy-preserving frameworks for social media analytics. Social Network Analysis and Mining, 9(1), 1-13.

4. Bhagat, K., & Aggarwal, A. (2021). A survey on privacy-preserving techniques in social networks. International Journal of Advanced Computer Science and Applications, 12(5), 155-161.

5. Chen, C., & Zhou, X. (2020). Secure and efficient data sharing in social networks: A survey. Computers & Security, 89, 101672.

6. Choi, J., & Shin, D. H. (2017). Privacy in social media: Comparing the experiences of older and younger users. Computers in Human Behavior, 69, 294-303.

7. Fan, W., & Liu, J. (2022). Privacy preservation in social network data publishing: A survey. IEEE Transactions on Knowledge and Data Engineering, 34(4), 1420-1437.

8. Gao, H., & Liu, X. (2018). Efficient and secure data sharing in social networks using homomorphic encryption. Journal of Network and Computer Applications, 107, 108-117.

9. Hasan, H. R., & Salah, K. (2019). Blockchain-based proof of delivery of physical assets with single and multiple transporters. IEEE Access, 7, 37026-37035.

10. Jiang, L., & Shao, J. (2016). A survey on privacy protection for users in social networks. Security and Communication Networks, 9(18), 5267-5288.

11. Johnson, A. M., & Torres, E. (2021). Privacy-enhancing technologies for social networks: A review. Information Systems Frontiers, 23(4), 899-913.

12. Kaur, P., & Singh, M. (2020). A comprehensive survey of privacy-preserving techniques for social networks. Journal of King Saud University-Computer and Information Sciences, 32(1), 21-37.

13. Li, H., & Li, J. (2017). Privacy-preserving data aggregation in social networks: A comprehensive survey. ACM Computing Surveys (CSUR), 50(2), 1-36.

14. Liu, D., & Li, X. (2019). A survey on secure data sharing in social networks. Journal of Communications and Information Networks, 4(3), 47-57.

15. Martinez, G., & Tejedor, M. (2018). Attribute-based encryption schemes in social networks: A survey. Computers & Security, 77, 29-47.

16. Mitra, S., & Pati, B. (2021). Security and privacy in online social networks: A review. Journal of Information Security and Applications, 58, 102702.

17. Mohammadi, M., & Abbasinezhad-Mood, D. (2018). Secure and efficient data transmission in social networks using hybrid encryption. Journal of Systems Architecture, 88, 1-9.

18. Nguyen, T. T., & Tran, V. T. (2020). Privacy-aware data sharing in online social networks using attribute-based encryption. IEEE Transactions on Dependable and Secure Computing, 17(5), 1082-1096.

19. Patil, P. P., & Kalbande, D. R. (2016). Privacy preservation in social network data publishing: A survey. Journal of Engineering Science and Technology Review, 9(5), 82-89.

20. Qiu, J., & Yang, Z. (2019). Privacy-preserving social network analysis: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), 1145-1173.

21. Rao, M., & Reddy, P. (2017). A comprehensive review of privacy-preserving mechanisms in social networks. International Journal of Communication Networks and Information Security, 9(3), 462-468.

22. Sharma, A., & Gupta, P. (2022). Enhancing security and privacy in online social networks through advanced cryptographic techniques. Journal of Information Security and Applications, 60, 102859.

23. Singh, K., & Kaur, H. (2021). Comparative study of encryption techniques in online social networks. International Journal of Advanced Research in Computer Science, 12(2), 34-42.

24. Wang, Y., & Chen, X. (2017). Privacy-preserving techniques for online social networks: A comprehensive survey. Journal of Network and Computer Applications, 86, 33-47.

25. Xu, J., & Zhou, H. (2020). End-to-end encryption in social networks: A review and perspective. IEEE Access, 8, 45632-45647.

26. Zhang, Y., & Han, Y. (2019). Blockchain-based privacy preservation for big data in social networks. IEEE Access, 7, 103241-103250.

27. Zhao, S., & Wang, S. (2023). Advances in privacy-preserving techniques for social networks: A review. ACM Transactions on Internet Technology (TOIT), 23(3), 1-27.

**Corresponding Author**

**Vaishnavi Agrawal***

Studdent, Class 11th, Welham Girls School, Dehradun, Uttrakhand, India

Email: vaish075navi@gmail.com