SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: XXXX-XXXX

Mitigating Social Media Cybercrime: Revolutionising with AES Encryption and Generative AI

Poh Soon JosephNg[1,2,*], Zhuang Cheik EricMok[1], Koo Yuen Phan[3], Jianhua Sun[4], and Zhiming Wei[4]

[1] Faculty of Data Science and Information Technology, INTI International University, Nilai 71800, Negeri Sembilan, Malaysia
[2] Institute of Computer Science and Digital Innovation, UCSI University, Kuala Lumpur 56000, Malaysia
[3] Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, 31900 Kampar, Perak, Malaysia
[4] Jiangsu Vocational College of Medicine, Jiangsu, China

ARTICLE INFO

Article history:
Received 15 August 2023
Received in revised form 29 December 2023
Accepted 3 March 2024
Available online 9 June 2024

Keywords:
AES Encryption techniques; cybercrime; secure communication; personal social media platforms; profitability; implementation; effectiveness; Generative AI; economic growth; resilient infrastructure; user experience

ABSTRACT

This research investigates the effective implementation of AES encryption techniques, combined with Generative AI, to ensure secure communication on personal social media platforms. The research aims to propose strategies for improving encryption implementation, enhancing usability for easy adoption, and exploring the potential for increased profitability while maintaining security. The research methodology includes a mixed mode to collect data on encryption practices, challenges, and perceptions in social media platforms. The research concludes that the findings will offer valuable insights into the effectiveness, usability, and potential impact of AES encryption techniques, powered by Generative AI, on secure communication while assessing the potential economic benefits and growth of enhanced encryption implementation. The results of this research will contribute to developing robust encryption strategies, user-centered design principles, and cost-effective encryption solutions, ultimately strengthening the security of user communications on personal social media platforms to mitigate cybercrime.

1. Introduction

A crucial step in ensuring data confidentiality and secure transmission is encryption. AES, a popular symmetric encryption algorithm, is essential for protecting sensitive data. The adoption of AES encryption by major technology companies like Google, Microsoft, and Amazon reflects the rising demand for effective encryption solutions [1]. Using AES encryption can improve operations, branding, and financial performance. It fosters secure communication, increases organizational efficiency, and safeguards sensitive data. AES encryption establishes credibility and trust by demonstrating a dedication to customer privacy and data security [2]. Companies need to be aware of the advantages and restrictions of AES encryption. Organizations should address the evolving

* *Corresponding author.*
E-mail address: joseph.ng@newinti.edu.my

https://doi.org/10.37934/araset.46.2.124154

cybersecurity risks, encryption vulnerabilities, and potential abuse by malicious actors while improving data security and regulatory compliance [3].

Keeping up with encryption developments, investing in reliable encryption software, and implementing extensive security measures are crucial for reducing potential threats [4]. Organizations can navigate the digital landscape, safeguard their data, and improve their security by embracing encryption and addressing related threats [5]. The literature highlights the use of AES encryption for secure communication, user satisfaction, and organizational profitability, emphasizing the importance of encryption across a variety of domains [6].

Encryption has long been a fundamental aspect of safeguarding data, however, the integration of cutting-edge advancements such as Generative Artificial Intelligence (AI) presents intriguing prospects for enhancing encryption methodologies in the foreseeable future. Generative artificial intelligence (AI), a prominent subfield within the broader domain of artificial intelligence, enables the production of new data that closely resembles existing datasets employed in the training process. By leveraging the capabilities of Generative AI in the field of encryption, the possibility of advancing the development of increasingly complex and efficient encryption algorithms emerges, consequently enhancing the overall security of personal social media platforms [33-35]. The inclusion of education on encryption in user awareness programs can also empower individuals to better understand and utilize encryption features, further strengthening the security and privacy of their communications on social media platforms.

1.1 Background Studies

End-to-end encryption is used by messaging apps like WhatsApp, Signal, and Telegram to protect user data, enhancing security and privacy [6]. Although social media platforms use encryption to protect private communications, there are possible flaws that could jeopardize data security. Even with message content encryption, metadata like communication information and duration still pose privacy risks [7]. Partnerships between technology companies and government surveillance programs raise concerns about privacy and security. Concerns about user privacy and the integrity of the encryption system are raised by government pressure on technology companies to build backdoors into encryption systems for law enforcement purposes [8].

1.2 Problem Statement

This research investigates the importance of network security and the risks associated with user data on social media platforms. Given the widespread usage and potential risks, it is crucial to address new threats and implement robust security controls to safeguard user data and privacy [8]. The importance of this research lies in the need to protect user data and privacy on social media platforms. The risks include privacy breaches, social engineering attacks, data breaches, and other vulnerabilities. By understanding these threats and exploring creative security solutions, social media platforms can ensure a safer user environment. While end-to-end encryption has been implemented, there are still issues with key management, law enforcement backdoors, and platform dependability that limit social media security [9]. Cryptography plays a crucial role in boosting the security of social media platforms and overcoming these constraints.

Efficient key generation, distribution, and storage mechanisms are required to protect the keys and reduce the risk of unauthorized access. User-controlled key management systems can increase trust and security [11]. Current encryption solutions in social media platforms face challenges related

to the protection of metadata, confidence in key management, implementation flaws, and security usability [10].

The disregard for metadata in encryption can expose potential weaknesses in security. Centralized key management may raise trust and privacy concerns for users. Protocol implementation errors and complicated encryption procedures can negatively impact user adoption and usability [12].

To address the limitations, social media platforms should focus on improving metadata protection, implementing user-controlled key management systems, and addressing protocol implementation errors. Efficient encryption techniques and user-friendly encryption procedures can enhance security and user adoption.

1.3 Research Objectives

RO1: To propose strategies to improve the implementation of encryption techniques in personal social media platforms.

RO2: To investigate ways to enhance the user experience of encryption techniques, the focus is on identifying user-centered techniques that can simplify the encryption process in personal social media platforms.

RO3: To propose encryption to reduce operational costs in personal social media platforms.

The security and privacy of user communications on social media platforms are crucially ensured by encryption, which turns sensitive information into a coded format that can only be decoded with the right decryption key. The incorporation of strong encryption techniques in these platforms offers several important benefits.

Encryption, in the first place, vastly improves communication security by shielding user data from unauthorized access and interception. This is especially important for personal social media platforms where users share sensitive information and have private conversations. Robust encryption methods guarantee the privacy and security of user communications while preventing security lapses.

The usability of encryption implementation is improved second. Although security is crucial, user experience shouldn't be sacrificed. Platforms can make encryption simple and practical for users by streamlining encryption procedures and incorporating user-friendly features. Lowering adoption barriers encourages more users to use encryption to protect their communications. User-friendly encryption implementation enhances user satisfaction, engagement, and long-term platform retention.

Finally, cost-effectiveness is a crucial factor for personal social media platforms. Although implementing encryption might require upfront costs like infrastructure upgrades and staff training, it has long-term advantages. Effective encryption techniques can reduce the financial risks, legal repercussions, and reputational harm brought on by data breaches. Platforms can save money by avoiding expensive data breach incidents and their consequences. Prioritizing encryption also helps platforms avoid fines and penalties by aligning with regulatory compliance requirements.

1.4 Research Hypothesis

RH1: By implementing encryption techniques in personal social media platforms, the security of user communications can be improved.

RH2: By implementing user-friendly simplified encryption techniques in personal social media platforms, users would find it easier to adopt and utilize encryption.

RH3: By implementing encryption techniques in personal social media platforms, the overall profitability can be increased through cost reduction while maintaining an elevated level of security.

This research study delves into the complex world of implementing encryption techniques within social media platforms to improve security, usability, and profitability. Three carefully crafted hypotheses targeting a different aspect of the research objectives are presented in the research framework. The focus of Hypothesis 1 is on the enhancement of security through encryption. Encryption plays a crucial role in bolstering the protection of user data and communications in today's constantly changing digital environment, where privacy breaches and data theft pose a serious threat. Personal social media platforms can erect substantial barriers against unauthorized access by deftly implementing robust encryption techniques, guaranteeing the sanctity of user information, and maintaining its confidentiality and integrity.

Hypothesis 2, in turn, pivots towards user-friendly design principles, seeking to streamline the adoption of encryption. The success of any security measure hinges on the extent of user acceptance and adoption. Encryption techniques that embody simplicity, ease of comprehension, and seamless integration into the platform's interface are poised to garner wider acceptance among users. By prioritizing user-centric design principles, personal social media platforms can galvanize the widespread adoption of encryption, thus bolstering security measures and shielding user privacy.

The third and final hypothesis, which forms the basis of the research framework, sets out to investigate cost optimization while maintaining the effectiveness of security measures. There are always expenses associated with implementing encryption techniques, from infrastructure upgrades to software development and maintenance. Nevertheless, personal social media platforms can balance security and cost-effectiveness by carefully choosing cost-effective encryption solutions and optimizing resource allocation. This hypothesis looks for methods and tools that reduce costs while maintaining the system's integrity and the encryption paradigm's effectiveness.

Figure 1 shows the research framework's visual representation captures the complex interactions between the three hypotheses and their symbiotic relationship with the overarching research objectives. It offers a comprehensive analysis of the complex dance of user interactions within the system, with hypotheses 1, 2, and 3 acting as guiding lights to improve the safety, usability, and financial success of social media platforms.

This study significantly advances knowledge about using encryption in personal social media platforms by carefully examining and dissecting the connections between these hypotheses. It sheds light on how crucial it is to address user experience, security concerns, and cost-effectiveness as crucial cogs in the machinery that drives these platforms' overall performance and profitability.

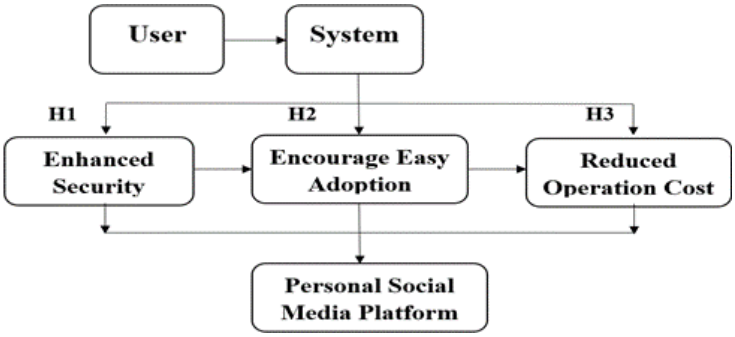

Fig. 1. Research framework diagram

1.5 Value Creation

This research significantly contributes to various aspects of personal social media platforms, driving advancements in the field. Integrating state-of-the-art Generative AI into encryption methodologies amplifies security measures and safeguards user data and communications, thereby significantly mitigating the likelihood of data breaches and infringements on privacy. The emphasis on user-friendly design principles for encryption adoption improves the overall user experience, making it easier for individuals to adopt encryption measures and promoting their widespread use. Additionally, the research explores strategies for cost reduction without compromising security, enabling platforms to optimize resource allocation and maximize profitability. By prioritizing security, usability, and cost-effectiveness, social media platforms can gain a competitive edge in the market and attract and retain users who value data privacy and security. Moreover, the research contributes to establishing industry best practices in encryption implementation, providing guidance for platform developers and managers to make informed decisions about security strategies. In conjunction with these outcomes, the integration of Generative AI synergistically contributes to establishing a more secure, user-centric, and financially advantageous milieu for both platforms and their users. This symbiotic relationship fosters a perpetual cycle of enhancement and progress within personal social media platforms.

1.6 Scope

This study investigates the use of encryption methods to increase the safety of personal social media platforms. Its goal is to address the shortcomings of the current encryption techniques used in social media apps and investigate different strategies to secure user communications. The study uses a practical sampling technique to ensure the representation of social media users who might be vulnerable to security risks. Users' data and privacy are seriously threatened by personal social media platforms that lack reliable encryption because they are open to surveillance and cyberattacks. Platforms can significantly improve the security and integrity of user communications by incorporating encryption, such as the Advanced Encryption Standard (AES). Data protection and robust security features are two of AES's most well-known strengths. In addition to conventional encryption methods, such as the Advanced Encryption Standard (AES), this study also explores the potential integration of state-of-the-art solutions, such as Generative Artificial Intelligence (AI), to further augment encryption techniques in the foreseeable future.

Secondly, AES encryption improves performance by quickly encrypting and decrypting user communications. This guarantees that the encryption procedures have minimal impact on the social media platform's speed and usability, giving users a seamless experience. The use of AES encryption also promotes trust among users and other stakeholders. Users are more likely to trust the platform and stick around when they believe their data and communications are secure. The satisfaction, engagement, and retention of users are all influenced by this feeling of trust. The use of AES encryption demonstrates to stakeholders a commitment to data security and privacy, which can improve the platform's reputation and credibility. As a result, the platform may draw more users, advertisers, and potential business partners, which will ultimately help it grow and succeed.

In conclusion, using encryption methods, particularly AES, integrating Generative Artificial Intelligence, in personal social media platforms is essential for enhancing data security, boosting performance, and fostering user and stakeholder confidence. Platforms can reduce security risks, protect user data, and foster a more secure environment for social media communication by addressing the shortcomings of current encryption techniques.

2. Literature Review

The Advanced Encryption Standard (AES) and modern cryptography sections go in-depth on the complexities of encryption and the necessity of using better techniques and protocols. Encryption is a key step in ensuring the confidentiality and integrity of data during transmission and storage. Stronger encryption methods are essential for successfully fending off these threats as technology advances and cyber threats become more sophisticated. AES, a widely used symmetric encryption algorithm, is crucial in protecting sensitive data. It was specifically created to provide a higher level of security while guaranteeing effectiveness in data encryption and decryption. The section emphasizes AES's importance in various contexts, including manual encryption techniques, social media platform encryption technologies, and existing AES-related literature.

Organizations face challenges when implementing new encryption techniques or upgrading existing ones, including the change management process. This project requires addressing a wide range of issues, including technical issues, compatibility with current systems, user education, and training needs, and potential resistance to change. Understanding and successfully navigating these complexities are essential components for the effective application of encryption. A summary of the lessons learned from the chosen papers concludes this section. It clarifies the complex nature of AES and highlights how important it is to protect private data. The studies in the literature that have been reviewed have offered insightful viewpoints on various aspects of AES, including its design, implementation, performance, and security. These details add up to a thorough understanding of AES and its importance within the context of contemporary cryptography.

Breakthrough developments have been made in the quickly developing generative artificial intelligence (AI) field, unleashing transformative applications in various fields. Notably, generative artificial intelligence (generative AI) uses the capabilities of neural networks, most notably Generative Adversarial Networks (GANs), to create new data samples that are strikingly like existing datasets. The limits of creativity have been pushed by these neural networks' extraordinary skill in tasks like image synthesis and natural language processing [33].

A world of opportunities opens when Generative AI and AES encryption come together, promising to strengthen data security on private social media platforms. AES encryption is made more effective by the skillful integration of Generative AI, which enables the generation and analysis of potential attack patterns and vulnerabilities. The AI algorithms facilitate the identification of weaknesses in the encryption scheme through clever simulations of realistic attack scenarios, fostering the development of stronger encryption methodologies [34].

To further strengthen data, Generative AI demonstrates its skill at producing impenetrable cryptographic keys, an unbreakable foundation for encryption. AI models demonstrate the ability to develop new keys that prevent even the most audacious brute-force attacks by leveraging existing encryption key patterns. The AI-driven encryption system's dynamism and adaptability reveal a potent force that relentlessly combats new threats and attacks and transforms into a flexible, futuristic solution [35].

This symbiotic combination of Generative AI and AES encryption charts a favorable trajectory for data security in private social media platforms, unfurling a variety of advanced encryption methods and flexible security measures that can skilfully address the constantly changing cybersecurity challenges. The fusion of Generative AI and encryption technologies is poised to take a commanding role in ensuring secure communications and protecting user data in the digital era as researchers delve deeper into their respective frontiers [33,34].

Upon conducting an in-depth exploration of the extant literature, it becomes evident that encryption undeniably assumes a crucial role in enhancing levels of security. Nevertheless, it is

evident that many challenges and potential vulnerabilities continue to exist, thereby demanding additional scrutiny. An area of interest that warrants further investigation is the integration of Generative AI and encryption methodologies, presenting a promising avenue for enhancing data security and introducing innovative approaches to address security and privacy issues on personal social media platforms.

Finally, this section highlights the potential future direction of incorporating generative artificial intelligence (AI) to strengthen data security further and provide a thorough review of modern cryptography and the significance of AES. Personal social media platforms can guarantee secure communications, safeguard sensitive information, and increase user confidence in the constantly changing digital environment by consistently improving encryption techniques and leveraging the power of Generative AI.

Figure 2 shows how existing social media platforms can use encryption to secure data transmission in a social media environment, ultimately, helping to secure social media platforms. Incorporating encryption methods into social media platforms is crucial for securing data transmission and enhancing the platform's overall security. Encryption is crucial because it accomplishes several goals, including protecting user data, guaranteeing privacy and confidentiality, maintaining data integrity, fostering user confidence and trust, and complying with data protection laws. Social media platforms can thwart unauthorized access, data breaches, and identity theft by encrypting sensitive user data and communications. This assists in protecting the sacredness of user privacy, maintaining the secrecy of conversations, and discouraging unauthorized surveillance. Additionally, encryption protocols offer tools for spotting any unauthorized or tampered changes to data, guaranteeing its integrity throughout transmission. Users' trust and confidence are boosted using encryption techniques, which promotes increased user engagement, brand loyalty, and the development of a positive platform reputation. Additionally, encryption helps platforms comply with data protection laws by reducing legal risks and potential fines. In short, encryption is essential for creating a secure environment on social media platforms, encouraging user trust, and reducing the risks of data breaches and privacy violations.

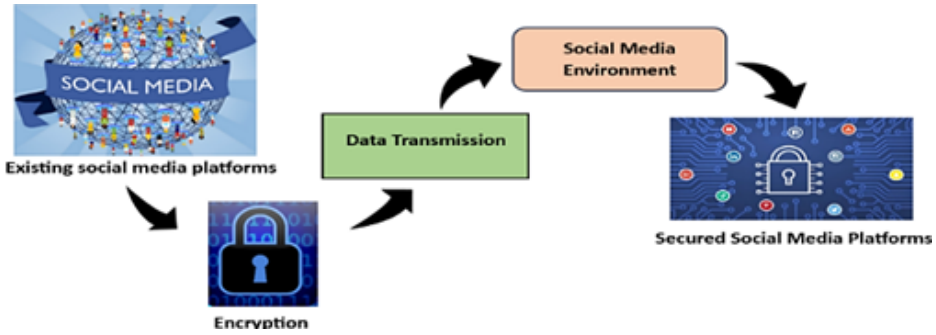

Fig. 2. Overview flowchart

2.1 Background Studies

Cryptographic methodologies and cryptographic keys play an indispensable role in preserving sensitive information and preventing unauthorized access, particularly within the contemporary digital environment, distinguished by the incessant proliferation of data breaches and apprehensions regarding privacy. Ongoing endeavors to augment encryption methodologies and techniques have been documented in the literature [13-15]. The Advanced Encryption Standard (AES), which was conceived as a successor to the Data Encryption Standard (DES) by the National Institute of Standards and Technology (NIST), has garnered significant acclaim for its formidable security capabilities. The

cryptographic system in question employs symmetric key algorithms and functions on data blocks of a predetermined size. It provides a range of key lengths, namely 128-bit, 192-bit, and 256-bit, to accommodate diverse security requirements [16].

Extensive testing and validation have been conducted to assess AES encryption's formidable strength and reliability, thereby solidifying its status as a trusted solution for protecting sensitive information [16]. The Advanced Encryption Standard (AES) is renowned for its many advantageous features, encompassing robust encryption capabilities, expedient processing velocity, and seamless compatibility across various platforms. In the realm of symmetric encryption algorithms, decryption in the absence of the requisite cryptographic keys presents an exceedingly formidable challenge. The robustness of AES encryption is firmly established through extensive scholarly inquiry and meticulous examination [16].

The Advanced Encryption Standard (AES) has gained considerable recognition in information security due to its exceptional security capabilities. As a result, its impact has expanded to encompass social media platforms. In the contemporary global landscape characterized by extensive interconnectivity, wherein interpersonal communication and the transmission of data flourish within digital platforms, the utilization of AES encryption assumes a paramount significance. Implementing robust security measures guarantees the preservation of confidentiality and integrity in the realm of private messaging, voice/video communication, and file transfers within social media platforms. Implementing AES encryption enables social media platforms to enhance user privacy and security, thereby fostering trust and confidence among their vast user population. [17-19].

An exemplary advantage inherent in the utilization of Advanced Encryption Standard (AES) encryption resides in its inherent flexibility, thereby affording the user the capacity to meticulously tailor the encryption strength in accordance with the precise security requirements at hand. Different platforms have the prerogative to exercise their autonomy in selecting key lengths, ranging from 128-bit to 256-bit, to conform to their distinct security exigencies. This enables social media platforms to customize their encryption strategies and provide their users with optimal security.

By deploying AES encryption, social media platforms possess the capacity to cultivate user trust and instill confidence, thereby efficaciously mitigating escalating apprehensions about data privacy and security. Utilizing AES's robust cryptographic algorithms guarantees the utmost confidentiality and safeguarding of users' highly sensitive information, effectively mitigating the risk of unauthorized access. Establishing trust among users fosters a cognitive disposition that promotes sustained engagement and utilization of the platform.

In summary, AES encryption functions as a formidable instrumentality in fortifying the confidentiality and integrity of delicate information within the realm of social media platforms. The preferred choice for safeguarding private communications is attributed to its potent encryption capabilities, demonstrated reliability, and remarkable flexibility in key lengths. Through the adoption and implementation of AES encryption, social media platforms have the potential to enhance user privacy, bolster security measures, and foster a reliable and dependable atmosphere within their user community.

2.2 Current Process

Snapchat's emphasis on safeguarding user privacy through the implementation of self-destructing messages affords users a discernible advantage in maintaining their personal information confidentiality. Nonetheless, the absence of end-to-end encryption across all modes of communication gives rise to substantial apprehensions pertaining to security and privacy. End-to-end encryption is an encryption technique of utmost security that guarantees exclusive access to the

content of messages solely to the sender and the designated recipient, thereby shielding them from any form of unauthorized access or interception [20].

In the absence of end-to-end encryption, Snapchat can gain access to and oversee user communications, potentially jeopardizing the confidentiality of said interactions. This situation elicits apprehensions regarding the platform's dedication to safeguarding privacy and the possibility of unsanctioned intrusion by external entities.

It is imperative for users to possess an awareness that although self-destructing messages may provide transient advantages in terms of privacy, the underlying platform retains the capability to access and exert authority over user communications. The inclusion of end-to-end encryption is of utmost importance to optimize privacy and security within personal social media platforms. End-to-end encryption ensures that the content of messages can only be accessed by the sender and the intended recipient, thereby offering an enhanced level of security against unauthorized access or interception. Through end-to-end encryption, platforms can augment user privacy, fortify the security of sensitive information, and exhibit their unwavering dedication to preserving the integrity of user communications.

Incorporating end-to-end encryption, in conjunction with the Advanced Encryption Standard (AES), can significantly augment the levels of security and privacy afforded to individual users on social media platforms. End-to-end encryption guarantees that the content of a message remains exclusively accessible to the sender and recipient, even in the event of interception. Encryption occurs exclusively at the originating device, while decryption is restricted to the intended recipient's device. This ensures continuous encryption during transmission and mitigates the potential for unauthorized access or interception.

The Advanced Encryption Standard (AES) is a highly regarded symmetric encryption algorithm renowned for its exceptional resilience and robust security measures. The system employs a confidential and integrity-preserving mechanism using a secret key for encryption and decryption. The Advanced Encryption Standard (AES) has been widely adopted and is regarded as a preeminent encryption algorithm. The amalgamation of end-to-end encryption and Advanced Encryption Standard (AES) can yield advantageous outcomes for personal social media platforms, as it allows for the utilization of the respective strengths inherent in each encryption technique. Using end-to-end encryption guarantees the preservation of user communications in a confidential and impervious manner while implementing the Advanced Encryption Standard (AES) furnishes a robust mechanism for safeguarding data through encryption. This amalgamation presents a comprehensive and robust security solution, assuring users that their messages and personal information are protected from unauthorized access.

The incorporation of end-to-end encryption in conjunction with the Advanced Encryption Standard (AES) effectively mitigates apprehensions about possible susceptibilities or deficiencies in either cryptographic technique. Implementing this additional security measure provides an augmented level of safeguarding against various security vulnerabilities, including but not limited to eavesdropping, data breaches, and unauthorized data access. In a comprehensive analysis, the integration of end-to-end encryption utilizing the Advanced Encryption Standard (AES) within personal social media platforms presents a highly resilient and efficacious approach to augmenting the levels of security and privacy. This feature's implementation enhances user confidence, bolsters the platform's standing in safeguarding user data, and fosters a more secure and reliable digital milieu.

2.3 Technology Innovation

The Advanced Encryption Standard (AES) is critical in safeguarding the confidentiality and integrity of sensitive data transmitted through social media platforms, owing to its resilient encryption algorithm. Exploring hybrid encryption methods as potential alternatives to AES is a growing trend. However, it is crucial to acknowledge that this shift in focus does not undermine the effectiveness or security of AES. The Advanced Encryption Standard (AES) continues to be extensively employed and enjoys high confidence within the encryption domain [18].

The growth of hybrid encryption methodologies within social media is propelled by the overarching aim of fortifying security measures by amalgamating diverse encryption techniques. Acknowledging the dynamic nature of threats in the digital realm highlights the imperative for implementing progressively robust security protocols. Nevertheless, it is imperative to recognize that extensively established encryption solutions, such as the Advanced Encryption Standard (AES), persistently remain indispensable in ensuring the efficient preservation of user data security [19].

While it is acknowledged that forthcoming encryption technologies exhibit potential, it is of utmost importance to accord precedence to established solutions such as AES to safeguard the confidentiality and integrity of user data on social media platforms. With the increasing adoption of AES encryption and its proven efficacy, there is a growing recognition of the significance of leveraging novel technologies to mitigate evolving threats in dynamic contexts. Ongoing research and analysis are being conducted to explore alternative encryption methods and hybrid approaches, to augment security and privacy measures, specifically within the domain of social media.

The process of transitioning from AES to novel encryption technologies necessitates a thorough assessment of cutting-edge security measures, performance benchmarks that have been optimized, and smooth integration with pre-existing systems. The primary aim of this study is to employ robust encryption techniques for safeguarding user data amidst the dynamic and constantly evolving technological environment.

In summary, it is noteworthy that hybrid approaches to social media encryption have gained considerable attention. However, it is imperative to acknowledge that the Advanced Encryption Standard (AES) continues to be a highly reliable encryption algorithm in social media security. The investigation into alternative encryption methodologies and the utilization of hybrid strategies demonstrates a dedication to augmenting security in response to the ever-evolving landscape of threats. The Advanced Encryption Standard (AES) functions as a yardstick for evaluating the efficacy of encryption. Ongoing endeavors are being made to integrate novel technologies while guaranteeing the uninterrupted safeguarding of user data on social media platforms.

2.4 Framework Literature

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm that has gained widespread recognition and adoption. It is renowned for its robust design, firmly grounded in intricate mathematical principles. Employing a symmetric key for data encryption and decryption establishes a reliable and efficient solution for organizations that are in pursuit of safeguarding sensitive information [16].

Integrating AES encryption in the storage and transmission of sensitive data presents numerous notable advantages. First and foremost, it is imperative to note that AES encryption ensures the preservation of data confidentiality by utilizing a transformative process that renders the information in an illegible format, necessitating the possession of the appropriate decryption key for successful

decipherment. This measure enhances the safeguarding of systems from unauthorized access and mitigates the potential vulnerabilities that could lead to data breaches [16].

Additionally, implementing AES encryption enhances data integrity by providing robust mechanisms that effectively detect any unauthorized modifications or tampering of the encrypted data. This practice guarantees the maintenance of data integrity during both storage and transmission, thereby upholding its reliability and trustworthiness.

In addition, it is worth noting that the utilization of AES encryption plays a substantial role in enhancing overall privacy and security within digital transactions and communication systems. Through AES encryption, organizations can establish secure channels for data exchange, effectively preventing interception and unauthorized surveillance. This practice cultivates a sense of confidence and reliance among users and customers, who can be assured that their data is safeguarded, and their privacy is upheld.

The extensive implementation of AES encryption has firmly established its status as a prevailing standard across various industries and sectors. The trust of organizations seeking to safeguard sensitive data has been garnered by this software due to its substantiated security features and proficient encryption capabilities. Consequently, it has enhanced confidence in digital transactions and communication systems, enabling secure and reliable interactions between users and organizations.

In summary, it is evident that AES encryption exhibits a commendable degree of security owing to its resilient architectural framework and intricate mathematical foundations. The incorporation of this technology into the data storage and transmission systems of organizations has yielded substantial enhancements in privacy and security, thereby fostering confidence in digital transactions and communication. The utilization of AES encryption presents a dependable and proficient resolution for protecting sensitive data, guaranteeing the preservation of confidentiality, integrity, and privacy. Table 1 shows a framework literature summary.

Table 1
Framework Literature Summary

Framework	Problem Statement	Objective	Methodology	Contribution	Limitation	Perspective
AES (Advanced Encryption Standard)	AES Addressing Limitations and Enhancing Security [19].	Safeguarding Sensitive Data with Resilience [19].	Multi-Round Symmetric Encryption with Substitution, Permutation, and Mixing Operations [19].	Unleashing the Power of Strong Cryptographic Design and Analysis. Embracing an Esteemed Encryption Standard for Seamless Integration Across Diverse Systems. Empowering Data Security and Privacy Through Unparalleled Encryption Measures.	Overcoming Block Size Limitations [19].	Theoretical Advancements, Managerial Adoption, and Societal Impact [19].
DES (Data Encryption Standard)	Secure and Efficient Algorithm for Modern Platforms [16].	Developing a Robust Symmetric Encryption Algorithm [16].	DES involves permutation, substitution, and key generation [16].	Unleashing the Power of DES Algorithmic Design. DES Fortifies Secure Communication and Storage. DES Empowers Privacy and Data Security.	The Demise of DES Algorithm in Modern Cryptography [16].	The Historical Significance and Limitations of AES Encryption for Secure Applications [16].

Blowfish	Secure and Efficient Symmetric Key Encryption for Data Protection and Integrity [24].	Empowering Rapid and Secure Symmetric Key Encryption for Safeguarding Sensitive Data [24].	Robust Encryption using Feistel Network and Key-dependent S-Box Substitution [24].	AES Encryption's Secure and Efficient Symmetric Algorithm. AES Encryption is the Ultimate Confidentiality, Integrity, and Availability Solution. AES Encryption Empowering Trust in Diverse Applications.	Inherent Vulnerabilities and Security Concerns of AES Encryption [24].	A Comprehensive Perspective on Cryptography's Theoretical, Managerial, and Societal Impact [24].
RSA (Rivest-Shamir-Adleman)	A Powerful Public-Key Cryptographic Algorithm [25].	Asymmetric Key Cryptography for Confidentiality, Integrity, and Authentication [25].	Secure Communication through Key Pair Generation and Modulo Exponentiation [25].	Unleashing the Power of Public-Key Cryptography. Safeguarding Data Transmission and Enriching Society. Enhancing Privacy, Security, and Online Interactions.	Efficiency, Scalability, and Security Challenges in AES Encryption: Unveiling Computational Complexity and Vulnerability [25].	Significance, Impact, and Secure Communication [25].

2.4.1 AES (Advanced Encryption Standard) framework

The AES (Advanced Encryption Standard) is an innovative encryption methodology that effectively mitigates the limitations inherent in current encryption techniques, with the ultimate objective of enhancing security to unprecedented levels. The primary aim of the Advanced Encryption Standard (AES) is to establish a robust and impregnable stronghold for the protection of highly sensitive data, thereby guaranteeing its utmost confidentiality, integrity, and availability. The AES algorithm employs a sophisticated methodology incorporating multi-round symmetric encryption, complemented by intricate operations including substitution, permutation, and mixing. The iterative procedure employed in this cryptographic process converts plaintext into ciphertext and vice versa, enhancing the encryption mechanism's intricacy and resilience. The inherent potency of AES resides in its resilient cryptographic architecture and meticulous scrutiny, thereby establishing it as a revered encryption paradigm that has garnered extensive adoption across heterogeneous systems. The Advanced Encryption Standard (AES) is renowned for its robust encryption techniques, safeguarding data integrity and confidentiality. By employing AES, organizations can enhance their data security measures, thereby fostering a heightened level of trust in safeguarding sensitive information. Although AES has certain limitations, such as constraints on block size, it provides a range of operational modes tailored to accommodate diverse data sizes, thereby effectively addressing this drawback. From a comprehensive standpoint that encompasses theoretical advancements, managerial adoption, and societal impact, the Advanced Encryption Standard (AES) represents a significant advancement in the field of encryption, ensuring the confidentiality and integrity of sensitive information across various applications [19].

2.4.2 DES (Data Encryption Standard) framework

The Data Encryption Standard (DES) is a cryptographic framework designed to address the need for a robust and efficient encryption algorithm in modern computing environments. The primary objective of this study is to develop a resilient symmetric encryption algorithm that effectively

enhances the confidentiality and integrity of data. The Data Encryption Standard (DES) encompasses a range of methodologies, including permutation, substitution, and key generation, to deliver robust encryption and decryption functionalities. The significance of this technology resides in its algorithmic design, which enables the secure transmission and storage of data. Nevertheless, the Data Encryption Standard (DES) exhibits certain limitations, particularly within contemporary cryptography, because its security has been compromised due to the progress made in computational capabilities. The perspective surrounding the Data Encryption Standard (DES) highlights the historical significance of the Advanced Encryption Standard (AES) as a viable substitute for DES in secure applications. The Advanced Encryption Standard (AES) is widely regarded as providing enhanced security and efficiency compared to the Data Encryption Standard (DES), thus establishing it as the favored option in modern cryptographic methodologies [16].

2.4.3 Blowfish framework

The Blowfish encryption algorithm, a symmetric key cryptographic technique, offers robust and expedient encryption for safeguarding confidential information. This study examines the imperative for robust encryption techniques that guarantee the preservation of data integrity and safeguard against unauthorized intrusion. Blowfish attains resilient encryption by employing a Feistel network structure alongside key-dependent S-box substitution. The solution presents a feasible alternative to AES encryption, expanding the array of choices accessible for safeguarding data confidentiality. Nevertheless, it is imperative to duly contemplate the intrinsic susceptibilities and security apprehensions linked to the Blowfish cryptographic algorithm. The efficacy of its encryption capabilities should be thoroughly assessed in relation to specific use cases, while also considering the necessity of implementing supplementary security measures. The examination of Blowfish enhances the holistic comprehension of the theoretical, managerial, and societal ramifications of cryptography. Through a comprehensive analysis of both the merits and drawbacks, scholars and professionals acquire invaluable insights to inform their decision-making process when selecting encryption algorithms and implementing encryption techniques in practical contexts. In summary, Blowfish allows users to safeguard confidential information; however, it is imperative to evaluate its susceptibilities and constraints within circumstances thoroughly. This analysis serves to augment our comprehension of the wider implications of encryption algorithms [24].

2.4.4 RSA (Rivest-Shamir-Adleman) framework

The RSA (Rivest-Shamir-Adleman) framework is widely recognized as a highly influential entity within the domain of public-key cryptographic algorithms, providing a resilient resolution to the pressing requirements of secure communication, confidentiality, integrity, and authentication. By employing strategic key pair generation and modulo exponentiation techniques, the RSA algorithm effectively traverses the complex landscape of cryptographic security. The system exploits the potential of two colossal prime numbers to generate a public key for encryption and a private key for decryption. Through adeptly leveraging the mathematical intricacies inherent in prime factorization and modular arithmetic, RSA effectively guarantees that solely the intended recipient possesses the capability to decipher the cryptic message concealed within. The extensive ramifications of the RSA algorithm are profound, as it serves to protect the intangible domain of data transmission, reinforcing the strongholds of confidentiality, integrity, and authenticity in digital communications. Nevertheless, it is imperative to comprehend the perplexing computational intricacies associated with the manipulation of immense prime numbers and maintain vigilance regarding potential

vulnerabilities that may be exploited by persistent malicious attacks. However, the resilient RSA framework confidently maintains its position as a crucial element in the captivating fabric of cryptography, consistently molding the dynamic realm of secure communication. It exerts its impact to facilitate the advancement of impenetrable communication protocols and robust cryptographic systems [25].

2.5 Change Management

The Advanced Encryption Standard (AES), a highly prevalent encryption algorithm, is widely recognized for its exceptional ability to provide robust protection for confidential information as shown in Figure 3 below. The employed methodology encompasses the utilization of block cipher encryption and decryption techniques within a Substitution-Permutation Network (SPN) framework, which integrates key expansion, substitution, and permutation operations [23]. The Advanced Encryption Standard (AES) has garnered a commendable standing due to its robust security measures, optimal operational efficiency, and seamless compatibility across a wide range of platforms. As a result, it has emerged as the encryption algorithm of choice for various critical applications within the United States government, including but not limited to data encryption, secure communication, and data storage. The consideration of migrating from AES to an alternative encryption technology necessitates careful examination of sophisticated security attributes, enhanced operational efficiency, and smooth incorporation into current systems to guarantee a flawless and safeguarded encryption procedure. By conducting a thorough assessment of these variables, organizations can effectively maintain or potentially augment the level of security offered by AES, thereby ensuring the safeguarding of sensitive information, and mitigating the risk of unauthorized access [25,26].

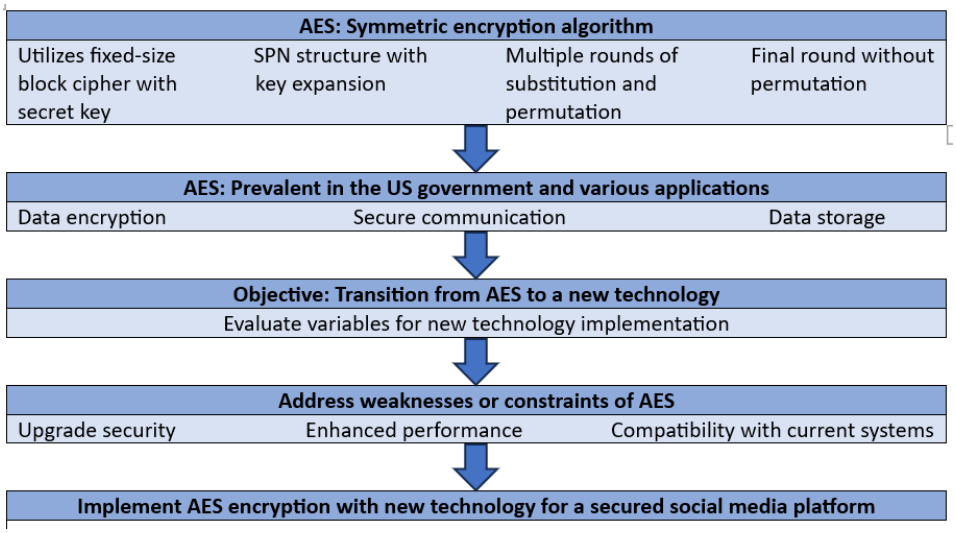

Fig. 3. Change Management Diagram

2.6 Summary of Literature

The papers chosen on modern cryptography provide a detailed analysis of the AES algorithm and its essential function in enabling secure data transmission. The foundational resource "An Introduction to modern cryptography" teaches the basic ideas that guide cryptography. The paper lays the foundation for understanding encryption algorithms like AES and their critical function in safeguarding sensitive information by laying this foundation.

The evaluation of the AES standard's development and application in "The Many Faces of AES" adopts a critical stance. This study delves into the subtleties of AES, assessing its advantages and disadvantages to offer insightful information about its effectiveness and potential weaknesses. The paper provides a deeper understanding of the algorithm's capabilities and constraints through a thorough analysis of various aspects, including design decisions and implementation details.

In particular, "A Comprehensive Review on Secure Data Transmission using AES Algorithm in Cloud Computing" focuses on the use of AES to ensure secure data transmission in cloud computing environments. This paper examines how AES can successfully address the specific issues and challenges posed by cloud computing, which calls for a tailored approach to data security. This study offers priceless insights into securing data during transmission by analyzing the effective use and practical implementation of AES in cloud environments.

These papers collectively shed light on the importance of AES in contemporary cryptography and its essential function in secure data transmission. AES is well known for its reliability and robustness and has received extensive study. For researchers and practitioners in the field of cryptography, gaining a thorough understanding of its design principles, implementation considerations, and practical applications is crucial.

Researchers can find areas for improvement and raise the security of the algorithm by carefully analyzing the strengths and weaknesses of AES. The knowledge gained from these papers aids in the development of encryption methods and ongoing research. Additionally, the information gained from these studies acts as a manual for creating stronger encryption protocols and systems.

The chosen papers offer a thorough understanding of AES and its crucial part in ensuring secure data transmission, so to sum up. They make a significant contribution to the field of cryptography by analyzing AES's strengths and weaknesses, especially in the context of cloud computing. Table 2 shows the summary of paper.

Table 2
Summary Paper Table

Paper Article	Problem Statement & Objectives	Contribution & Methods	Limitations	Perspective
An introduction to modern cryptography. In Contemporary Cryptography. Ristenpart, T., Shrimpton, T., & Shrimpton, T. (2018).	Demystifying AES Encryption: Empowering Secure Communication and Data Protection.	Unveiling the Power of AES and Modern Security Protocols.	A Comprehensive Overview with a Focus on Practical Applications.	Cryptographic Foundations, Exploring Concepts, Principles, and Applications.
The many faces of AES: A critical review of the design and implementation of the AES standard. Rogaway, P. (2020).	Critically Evaluating and Enhancing the AES Standard to Strengthen Security and Resilience.	Analyzing and enhancing the AES Standard to Strengthen Security and Deployment.	Acknowledging Implementation-Specific Weaknesses in Addressing Vulnerabilities and Security Risks.	Exploring AES Standard by Unveiling Vulnerabilities and Enhancements in Secure Systems.
A Comprehensive Review of Secure Data Transmission using AES Algorithm in Cloud Computing. Patidar, S., & Jatav, M. (2021).	A Comprehensive Review of AES Algorithm Effectiveness.	A Comprehensive Review and AES Algorithm Integration.	AES for Secure Data Transmission in Cloud Computing by Exploring Key Considerations.	A Theoretical and Managerial Perspective on AES for Secure Data Transmission.

3. Methodology

Effectively addressing research questions and obtaining profound insights depend critically on the research design. In this setting, mixed methods research stands out as a powerful strategy because it combines qualitative and quantitative techniques to explore complex phenomena and overcome the shortcomings of each technique separately. Combining these various approaches enables triangulation, which strengthens the validity and reliability of research findings [21-23]. Primary data assumes the utmost significance when it comes to data collection. Primary data is more trustworthy, accurate, and relevant than secondary data sourced from existing repositories because it is directly acquired by researchers for a particular research project [24-27]. The quality and accuracy of the data are ensured by the researcher's total control over the data collection procedure.

Additionally, using mixed-mode data collection techniques helps to strengthen research findings. Researchers can gather a wide range of perspectives and insights from study participants by using both surveys and interviews. While interviews provide in-depth qualitative insights into participants' experiences and perceptions, surveys provide an effective and statistically sound way to quickly collect large volumes of data. Additionally, the methodology and methods used to collect the data must be compatible with the goals of the study as well as the characteristics of the participants [28-30]. For instance, quantitative surveys may be more suitable when examining relationships and coming to general conclusions. Qualitative interviews, on the other hand, become the method of choice when attempting to gain profound insights into participants' subjective experiences and contexts.

3.1 Research Design

The intricate complexities of research design play a crucial role in determining the efficacy of any study, as it lays out the blueprint and method by which researchers can investigate complex phenomena. Embracing the combination of qualitative and quantitative methods, the mixed methods research design provides a robust framework for gaining an in-depth understanding of multifaceted topics [31-33]. By integrating qualitative and quantitative data, researchers can delve into subjective experiences through interviews and reveal statistical patterns through surveys, enhancing the findings with a multifaceted and nuanced perspective.

Primary data is the unrivaled focal point of this study, prevailing over secondary data. Primary data, which was intrepidly collected by researchers solely for their research endeavor, exhibits enhanced reliability and precision and is in perfect harmony with the research objectives. Researchers who have control over the process of data collection can meticulously ensure its relevance and quality. In contrast, secondary data collected for a variety of purposes may lack applicability or precision in the current research context. This study embarks on a daring mission to produce novel knowledge and uncharted insights, advancing the field's understanding to greater heights by relying solely on primary data.

Quantitative research, resolute in its pursuit of analyzing numerical data obtained from surveys, equips researchers with the ability to draw generalizable inferences and discover patterns embedded within massive datasets. In contrast to quantitative research, qualitative research delves deeply into the realm of subjective experiences and contexts through in-depth interviews, granting a profound understanding of participants' points of view. The study's foundations of validity and comprehensiveness are strengthened by the deft incorporation of triangulation and mixed-mode research, which harmonizes quantitative and qualitative methodologies. By deftly interweaving these two approaches, researchers cast a wide net, entwining a multitude of data threads that

coalesce to form an all-encompassing panorama of the research topic. In addition, convenience sampling is utilized to recruit participants based on their availability and willingness to participate in the research journey. This approach, despite its convenience, may inadvertently usher in bias.

In conclusion, the potent prowess of the mixed methods research design, the unwavering reliance on primary data, and the artful fusion of qualitative and quantitative methodologies stand tall as the research endeavor's guiding light [34-36]. The study deftly navigates the waters of diversity and in-depth investigation by employing stratified random sampling and in-depth interviews with determination. The ultimate objective is to chart a course toward a profoundly enlightening contribution to the field by unearthing knowledge of the utmost importance that future research and advancements will value and champion. Research flowchart is shown in Table 3.

Table 3
Research Flowchart

Activity/ *Phase*	Phase 1 *Quantitative Generalization*	Phase 2 *Qualitative Reasoning*
Research dimension	Phenomena Explanatory Sequential Dimension	
Research design	Random survey	Personal interview
Data collection	Online across Malaysia. 60 respondents.	Online across Malaysia. 60 respondents.
Research methods	Convenient sampling who are willing to participate and share information.	Convenient sampling who are willing to participate and share information.

3.2 Research Method Type

A mixed-method research approach will be used in this study to gather data in a single Google Sheet using both qualitative and quantitative techniques. To fully address the research objectives, using a mixed-method approach has several benefits [37]. The research develops a deeper and more comprehensive understanding of users' preferences, viewpoints, and experiences with encryption features in private social media platforms by combining qualitative and quantitative data collection techniques [38].

The research will be able to investigate the individualized perspectives and experiences of users about encryption using qualitative methods, such as interviews or open-ended survey questions. These qualitative data can offer subtle insights into the drivers, worries, and expectations of users about the implementation of data security and encryption [34]. The use of quantitative techniques, on the other hand, like closed-ended questionnaires or rating scales, will allow us to collect numerical information and spot patterns and trends across a wider sample of respondents. This quantitative information will offer insightful statistical analysis into the frequency of preferences or perceptions among users [39,40].

We can cross-validate findings, improve the reliability of the results, and triangulate data to make more firm conclusions by combining qualitative and quantitative methods. While the quantitative data can offer broader generalizability to the research findings, the qualitative data can aid in contextualizing and interpreting the quantitative findings. The combination of these approaches will also offer a more thorough and well-rounded analysis of the research topic, capturing both the diversity of individual experiences and the more general trends within the user population [41].

3.2.1 Quantitative

A quantitative approach will be used in this study to gather data. Researchers can examine relationships, patterns, and trends objectively by using quantitative research to collect numerical

data and statistically analyze it. This study uses quantitative methods to collect quantifiable data from a larger sample size and produce statistically significant findings. The use of quantitative research has several benefits, including its capacity to deliver accurate and trustworthy data, ease comparisons between various groups or variables, and establish causal relationships between variables [40]. Quantitative data also makes it possible to extrapolate results to larger populations, improving the study's external validity. In this study, quantitative methods will be used to supplement qualitative insights and provide a thorough understanding of the research topic [42].

3.3 Target Population

All users of social media platforms are included in the study's target population. The purpose of the study is to investigate how this diverse population views the use of encryption in social media and its significance. The study aims to gather a thorough and inclusive understanding of people's attitudes toward encryption features and techniques by focusing on social media users from various backgrounds, demographics, and ages. The knowledge gained from this diverse target audience will aid in the creation of encryption techniques that take social media users' needs and preferences into account, ultimately enhancing data security and user experience in the digital sphere.

3.4 Convenient Sampling

Convenient sampling was selected as the sampling technique in this study to gather information from social media users. A non-probability sampling technique called convenient sampling involves choosing participants based on their accessibility and willingness to take part in the study. It is chosen because it is practical and simple to use, enabling researchers to efficiently collect data from a variety of social media users. Convenient sampling has the benefit of saving time and money, making it a good strategy for studies with constrained time or financial resources. Additionally, it offers insightful feedback from a wide range of participants that can be used to better understand how social media users view and feel about encryption. Convenient sampling may, however, introduce some bias because participants who are more accessible or willing to participate might not be entirely representative of the target population. This limitation needs to be considered when interpreting the results. Nevertheless, practical, and useful approaches to gather pertinent data for this research include convenient sampling [43].

4. Findings and Discussion

4.1 Demographics

As shown in Figure 4, making educated decisions about implementing encryption in social media platforms requires an understanding of user demographics. Age, gender, occupation, and education all have a big impact on how users behave and what they think about security and privacy. Knowing how users are distributed by age makes it easier to adjust encryption features to satisfy the requirements of various age groups. Younger users might favor seamless encryption that happens automatically, whereas older users might prefer encryption settings that are more open and customizable. Gender-specific factors are also very important. Women may place a different value on privacy and data security than men do, and it is important to address their unique concerns and foster trust by taking these differences into account. The user base's technical knowledge and understanding of encryption can be inferred from occupation and educational levels. More robust encryption measures may be expected from experts in cybersecurity or related fields, while users

with less technical backgrounds may require clearer explanations and user-friendly interfaces. We can identify potential obstacles and opportunities for enhancing encryption strategy by examining the connections between these demographic factors and user perceptions of encryption. For instance, if a certain age group expresses more privacy concerns, we can concentrate on strengthening data protection measures to allay their concerns and increase trust in our platform. Additionally, knowing how various user groups interact with encryption can help us refine our marketing and communication strategies. For instance, increasing user engagement and encouraging encryption adoption can be achieved by highlighting the benefits of encryption techniques to users based on their demographic traits.

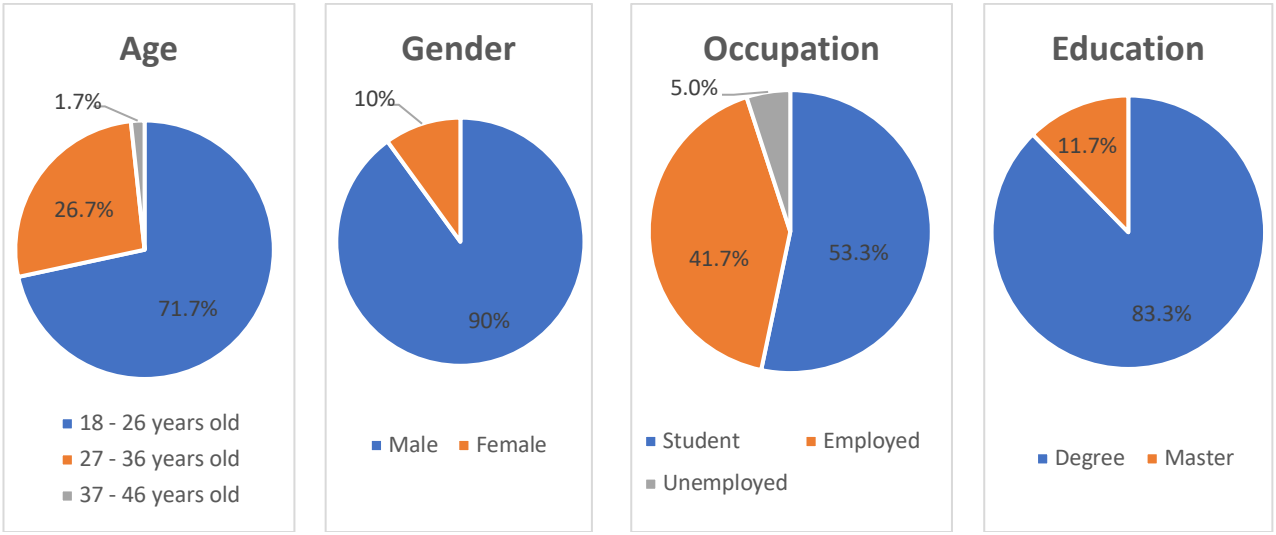

Fig. 4. Demographics section

4.2 Quantitative Results

Figure 5 shows that 70% of users agree and 15% strongly agree that encryption is important is critical to the platform's security strategy. It suggests that a sizeable percentage of users are aware of the value of encryption in protecting their data and communications on social media platforms. Due to the prioritization of strong encryption measures made possible by this insight, encryption can be the default setting when using social media. By making encryption the default, users are guaranteed that all communications and data are automatically protected without having to take any additional action on their part. The adoption of encryption is made easier by this simplified user experience, which also improves user security in general. With the help of this knowledge, marketing, and communication strategies can be adjusted to highlight the platform's default encryption setting and inspire user confidence in the platform's dedication to its security. The platform can ensure that encryption measures are still applicable, reliable, and current by continuously requesting user feedback and implementing updates based on their requirements. Overall, it is crucial to use this insight to emphasize the significance of encryption throughout social media platforms. A secure and dependable environment that appeals to users and distinguishes the platform from rivals can be created by incorporating encryption into the user experience design, marketing strategies, and customer support initiatives.

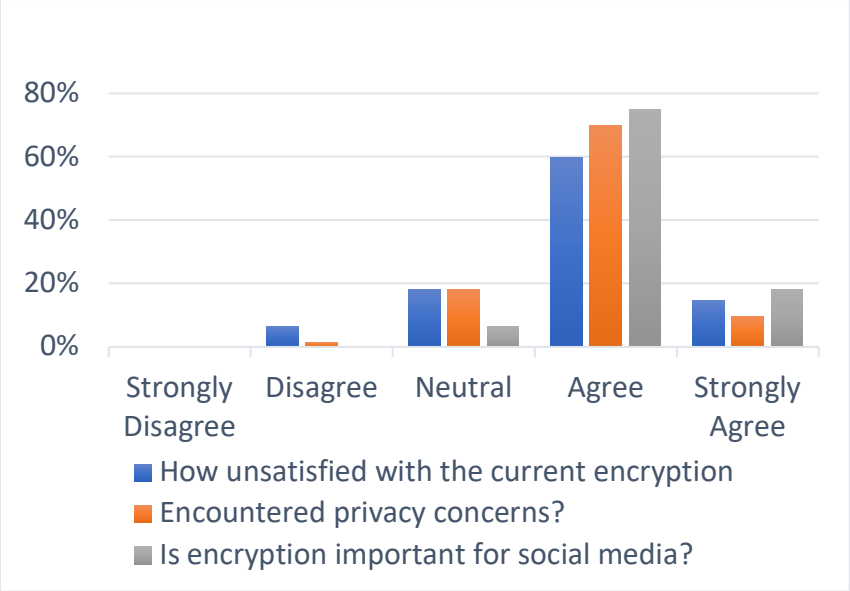

Fig. 5. Importance of encryption for security

According to the data as shown in Figure 6, 45% of users agree, and 10% strongly agree that it is important for encryption to be widely adopted and used. This result shows that a sizable portion of the user base is aware of the advantages of user-friendly encryption features. According to the data analysis, some users reject the idea that widespread encryption adoption is essential. It is crucial to consider possible causes of this viewpoint to better comprehend their viewpoint. Users' ignorance of the importance of encryption in protecting their data and communications is one potential cause. Some users might not be fully aware of the vulnerabilities and potential risks connected to insufficient encryption. Additionally, some users may perceive encryption as being complex, which would make them think that it requires extra steps or makes using the platform more difficult. Another factor might be that users who disagree might already have a high level of confidence in the platform's current security measures and might not view encryption as a top priority for them. Targeted educational initiatives and communication tactics can be used to address these issues. Users may better appreciate the value of encryption if its advantages are made clear, such as improved privacy, data protection, and secure communication. Concerns about complexity can be allayed by offering simple instructions and tutorials that show how easy it is to use encryption. Building credibility and trust can be accomplished by highlighting actual instances in which encryption has stopped data breaches or unauthorized access. Engaging with users through feedback forms and customer support channels can help us understand their unique isues and provide individualized solutions. The platform can foster a sense of partnership and strengthen its dedication to security by promptly and openly responding to user feedback. The goal is to address users' concerns and misconceptions while educating them on the value of simple adoption of encryption. This will encourage more users to do so and boost the platform's overall security for a safer and more secure user experience.

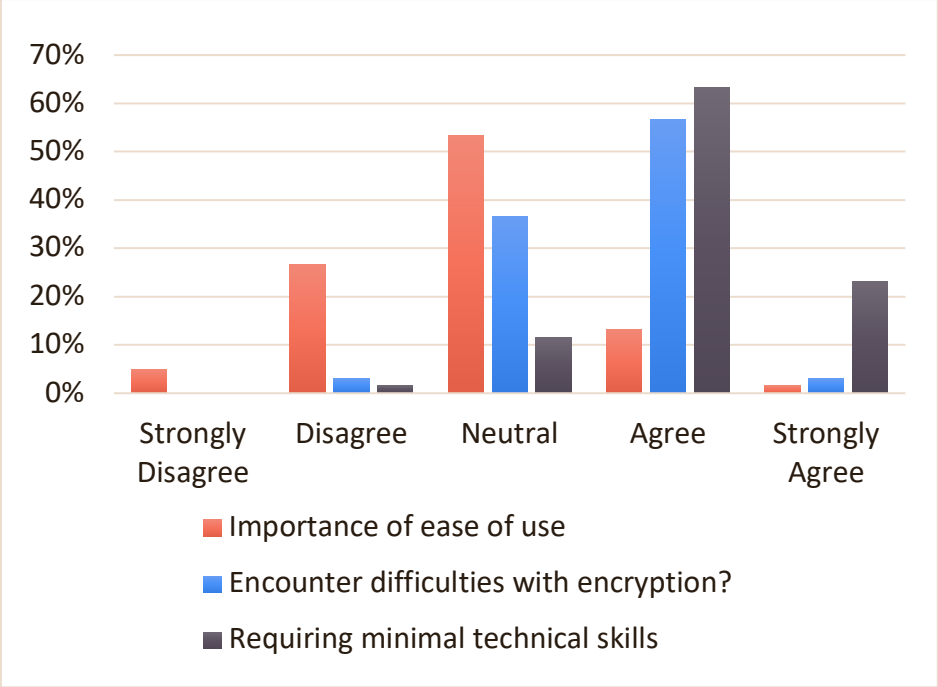

Fig. 6. Importance of easy adoption and utilization for encryption

As shown in Figure 7, users value the incorporation of robust security measures in the platform based on the data showing that a sizable portion of users agree that encryption can increase profit while reducing costs. This confidence in encryption can be a competitive advantage to draw in and keep clients. Managers must comprehend that how users feel about encryption has a direct bearing on whether they will continue to use the platform. Platforms can strategically offer paid subscription services with improved encryption features by recognizing the value users place on security. The added advantages of such services are more likely to be recognized by users who value encryption, and they may even be willing to pay for them. Implementing paid subscription services with encryption as a key selling point can boost revenue while fostering user loyalty and trust. Users' trust in the platform can be increased by making investments in cutting-edge encryption technologies and transparently communicating these security measures to them. Offering robust encryption solutions can be a key differentiator for the platform as data breaches and privacy issues continue to be major problems in the digital world. To maintain a competitive edge in the market, platforms must, however, strike a balance between offering improved security features and guaranteeing affordability. Overall, platforms can make wise decisions about the introduction of paid subscription services and can reinforce their commitment to data security by considering users' perceptions of how encryption affects revenue and customer trust.

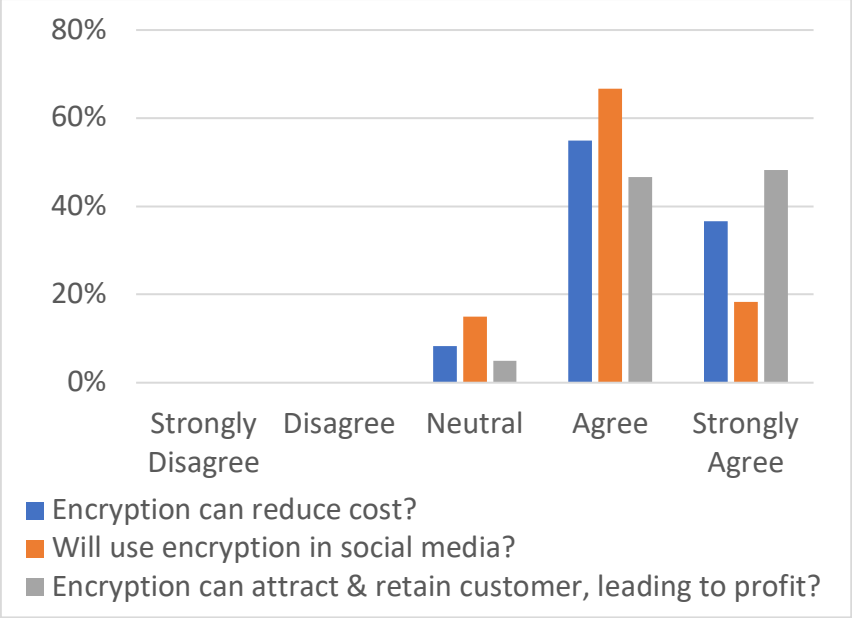

Fig. 7. Encryption can increase profit and reduce cost

4.3 Qualitative Results

It is clear from the data in Figure 8 that 19 respondents emphasized the significance of an intuitive user interface for encryption features. The need for platforms to prioritize user-friendly encryption solutions and offer straightforward instructions is made clear by this, which will help users use encryption effectively. The significance of finding a balance between user privacy and content moderation was also mentioned by 14 respondents. This shows that users are aware of the value of social media safety and privacy, as well as the necessity of content regulation and safety. For personal social media platforms to be secure and trustworthy, this balance must be struck. Additionally, 12 respondents emphasized the value of education and awareness in assisting users in comprehending and effectively utilizing encryption features. This suggests that promoting the use and advantages of encryption to users can be accomplished by offering educational materials and awareness campaigns. Platforms can enhance user experience and promote a more secure communication environment by addressing these problems and incorporating user feedback. The data concludes that when implementing encryption on private social media platforms, usability is a crucial factor to address. To help users understand and effectively use encryption, platforms should put a priority on user-friendly encryption, strike a balance between user privacy and content moderation, and spend money on education and awareness initiatives. Personal social media platforms can improve the usability of encryption features and encourage more users to adopt them for secure communication by addressing these issues and putting user-centered solutions in place.

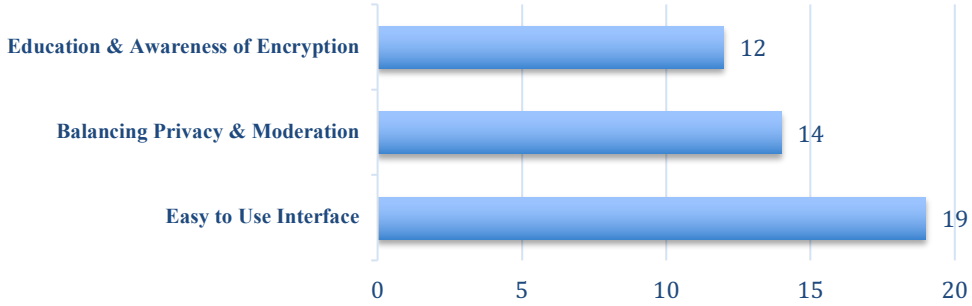

Fig. 8. User perspective and suggestions

It is clear from the data in Figure 9 that a sizeable portion of participants places a high value on encryption on private social media platforms. The graph shows that encryption is essential for safeguarding user data and fostering user confidence. There is a growing awareness and concern regarding data privacy in today's digital environment, as evidenced by the high percentage of participants who acknowledge the significance of encryption. Users value the protection of their personal information online, so platforms that prioritize data security through encryption are likely to draw and keep users. This emphasis on the value of encryption can greatly increase user confidence and customer adherence, which will ultimately increase platform profitability. Even though most participants understand the importance of encryption, a small percentage of respondents gave encryption a lower rating. This difference in opinions or the need for more information on the importance and advantages of encryption in private social media platforms could be the cause of the discrepancy in responses. In conclusion, encryption is essential for luring users to personal social media platforms and keeping them there. Encryption allows platforms to prioritize data security and user privacy, which helps to foster customer loyalty, increase trust, and increase revenue. The results from Figure 9 show how crucial encryption is in the data-driven digital world of today and emphasize the need for ongoing efforts to inform users about the benefits of encryption in private social media networks.

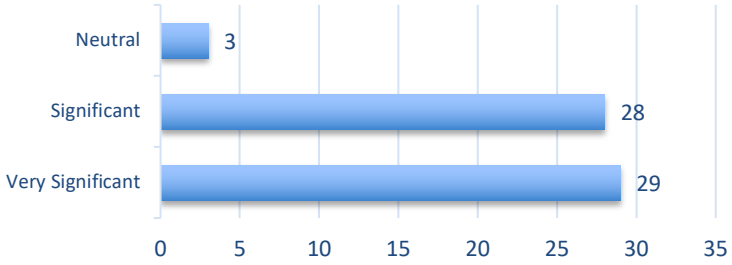

Fig. 9. Encryption role in attracting & retaining user

4.4 Value Creation

The research's four major contributions—practical, managerial, theoretical, and societal—combine to create value. The research offers helpful insights into user preferences and opinions regarding encryption features and techniques in private social media platforms, which is a practical contribution. Strong encryption algorithms like AES are overwhelmingly supported by users, highlighting their strong desire for increased privacy, and security and directing developers and managers to prioritize encryption implementation and build a safe environment for their users. The value derived from technological and procedural innovation is demonstrated by this useful

contribution, which has practical implications for the creation and application of encryption strategies [44-45].

From a managerial standpoint, the research provides insights that can direct the creation of educational initiatives and public awareness campaigns to highlight the advantages and simplicity of utilizing encryption. Managers can improve user experience and foster a secure communication environment on personal social media platforms by addressing user concerns and giving precise instructions on using encryption. This managerial contribution exemplifies how crucial it is to constantly advance encryption methods to successfully address the changing difficulties presented by cybersecurity [46].

Theoretical contributions are made by expanding our understanding of cryptography, particularly as it relates to personal social media platforms. The study examines the challenges of change management and offers a thorough analysis of modern encryption methods, emphasizing the role of AES in safeguarding sensitive data. The literature on encryption technologies and their use in protecting user data and communication on social media platforms is enriched by this theoretical contribution [47].

Next, the emphasis on data privacy awareness and concerns among users shows the contribution to society. The study shows that users respect platforms that put encryption first and are aware of the value of data security. Encryption contributes to a safer online environment by fostering user confidence and trust, as well as a sense of security and privacy for users on private social media platforms. The growing demand for secure and privacy-focused services in the digital age is in line with this societal contribution [48-49].

In conclusion, the importance of encryption in enhancing data security, boosting performance, and fostering user and stakeholder confidence on personal social media platforms is highlighted by the value created by this research through practical, managerial, theoretical, and societal contributions. A safer and more secure digital environment is promoted by the knowledge gained from this research, which has broad implications for platform developers, managers, policymakers, and users.

4.4.1 Practical contribution

The practical value of this research is found in how it affects the creation and application of encryption techniques in private social media platforms. The research directs platform developers and managers to prioritize the integration of strong security measures by emphasizing the importance of encryption, particularly advanced encryption technologies like AES. The user experience, safety, and trust can all be significantly improved by implementing such encryption techniques. Users are more likely to be loyal to a platform that prioritizes data security and privacy because they feel more trusted by it. The results highlight how important encryption is in creating a safe and reliable environment for social media communication. This useful contribution gives platform vendors the ability to proactively strengthen their offerings, which ultimately benefits both the platform and its users [50-52].

4.4.2 Managerial contribution

Numerous benefits can be obtained by implementing encryption methods, especially AES, in private social media platforms. Encryption guarantees that user communication and data security are not compromised by enhancing performance, and creating a seamless user experience. Additionally, ensuring system compatibility enables the platform to reach a larger user base. User

trust is increased, and a trustworthy reputation is fostered by adhering to data protection regulations. The platform is protected from potential financial and reputational losses thanks to encryption's role in reducing costs associated with data breaches. Additionally, more user retention is encouraged by the increased user satisfaction and loyalty brought about by secure communication. The platform gains a competitive edge in the market by incorporating cutting-edge encryption processes and technologies, drawing in more users and potential business partners. The platform's position in the market and its dedication to user data security and privacy are both strengthened by this managerial contribution [53-55].

4.4.3 Theoretical contribution

The theoretical contribution of this research lies in providing a solid foundation for future advancements in encryption technologies. By examining the perceptions and preferences of users towards encryption features in personal social media platforms, the study sheds light on the importance and effectiveness of encryption as a security measure. The empirical evidence collected from the survey showcases the value of encryption in safeguarding user data and communications. This evidence can serve as a basis for further research and development of encryption techniques to address the evolving challenges of cybersecurity in the digital age. The findings contribute to the growing body of knowledge in the field of encryption and its significance in enhancing data security and user trust in personal social media platforms [56-59].

4.4.4 Societal contribution

It is crucial to use strong encryption methods like AES in personal social media platforms because of their positive social impact. This initiative addresses growing concerns about the compromise of sensitive information and vulnerability to data breaches in the digital age by upholding privacy and data protection. By establishing a robust encryption framework, user communications and data are kept secure, potentially reducing the risks of unauthorized access. This action promotes user confidence in the platform's dedication to secure communication and data protection, which fosters user trust. Such a societal contribution improves the overall security environment and encourages responsible data handling practices, which ultimately makes the internet safer for all users [60-64].

4.4.5 Integration and Value Creation

By integrating AES encryption and Generative AI on social media platforms, the potential for value creation becomes evident. AES encryption ensures robust data security and protection, addressing users' concerns about privacy and unauthorized access [65-66]. On the other hand, Generative AI can enhance user experiences by providing personalized content, recommendations, and interactions [67]. The combination of these technologies can lead to increased user satisfaction and loyalty, as users feel more secure and engaged with personalized and relevant content. Moreover, the integration of AES encryption and Generative AI can attract new users who prioritize data security and personalized experiences. This, in turn, can lead to increased user retention and platform profitability, as users are more likely to stay and engage with the platform that prioritizes their privacy and provides valuable content [69-70]. Additionally, the integration of these technologies showcases the platform's commitment to staying at the forefront of technology advancements, which can boost the platform's reputation and credibility in the market. Overall, the integration of AES encryption and

Generative AI holds the potential for substantial value creation for both the social media platform and its users, providing a win-win scenario for all stakeholders involved.

4.5 Contribution of This Research Compared to Elliptic Curve Cryptographic

The research by Rashidi, titled "A Survey on Hardware Implementations of Elliptic Curve Cryptosystems," [71] offers a comprehensive overview of hardware implementations related to Elliptic Curve Cryptosystems (ECC). This work delves into the intricacies of ECC hardware, providing valuable insights for engineers and developers interested in deploying ECC in resource-constrained environments, like embedded systems. On the other hand, this research focuses on a different facet of encryption. It explores the integration of AES encryption with Generative AI, offering a novel perspective on encryption methodologies. This integration potentially enhances encryption algorithms and techniques, with practical applications in ensuring security and privacy in social media platforms. While Rashidi's [71] research enriches the understanding of ECC hardware implementations, this study aims to contribute to the broader field of cybersecurity and privacy, particularly within the dynamic context of social media and secure data transmission. Both research areas have their unique merits, catering to different aspects of encryption and security. The choice between them hinges on specific research objectives and applications [72].

4.5.1 Advantage of the proposed method

The proposed method of integrating AES encryption with Generative AI for enhancing encryption methodologies offers several distinct advantages. Firstly, it can significantly enhance security. By leveraging Generative AI, the encryption process can potentially become more robust and adaptable. Generative AI can intelligently adapt encryption algorithms in response to emerging threats, making it harder for malicious actors to decipher encrypted data. This dynamic response to evolving threats enhances overall network security [73]. It improves usability. The integration of Generative AI can enhance the usability of encryption tools. AI can assist users in setting up encryption, generating and managing encryption keys, and troubleshooting any issues, ultimately making encryption more user-friendly [74]. This can encourage more users to adopt encryption practices. It enables real-time threat detection. Generative AI can continuously monitor network traffic for suspicious patterns and adapt encryption strategies in real-time to counter emerging threats. This proactive approach adds an extra layer of security to the system. Lastly, data anonymization is improved. Generative AI can help anonymize data before encryption, adding an extra layer of privacy protection. This is particularly important in scenarios where user privacy is paramount, such as in social media platforms.

4.5.2 Disadvantage of the proposed method

Despite the numerous advantages, there are potential disadvantages associated with this approach. One significant concern is computational complexity. Implementing Generative AI in encryption systems may introduce computational overhead, potentially slowing down data encryption and decryption processes. This could affect the performance of the system, especially in resource-constrained environments where computational resources are limited [74]. Another issue is dependence on AI. Relying on AI for encryption introduces a new dependency. If the AI system encounters issues or is compromised, it could potentially lead to vulnerabilities in the encryption process. Ensuring the reliability and security of the AI component is crucial. Ethical concerns are also relevant. The use of AI in encryption should be carefully monitored to prevent potential ethical

concerns, such as AI bias or the misuse of AI-generated encryption strategies. Ethical considerations are paramount in maintaining user trust. Lastly, integration challenges may arise. Integrating Generative AI with existing encryption systems may pose technical challenges and require substantial development effort. Compatibility and seamless integration are essential for the success of this approach.

In conclusion, while the proposed method offers significant advantages in enhancing encryption methodologies, it is essential to be aware of these potential disadvantages and address them effectively during implementation to maximize its benefits while mitigating risks.

5. Conclusions and Limitations

While this research offers significant contributions, it is imperative to acknowledge and address its inherent limitations. A noteworthy constraint pertains to the relatively diminutive sample size, encompassing a specific cohort of participants from a particular geographical locale. Consequently, the outcomes may not lend themselves to generalization across a wider populace. Furthermore, the study centered its attention on the subjective perceptions and opinions of users, acknowledging that these may not consistently correspond with their objective behaviors or actions. The utilization of self-reported data additionally introduces the potential for response bias or social desirability bias, wherein participants may furnish responses that they perceive as socially acceptable or anticipated.

In conclusion, this study elucidates the significance of encryption functionalities within individualized social media platforms, with a specific emphasis on the widespread adoption and favourability of Advanced Encryption Standard (AES) encryption by users. The results underscore the importance of integrating strong encryption methodologies to fortify data security, augment user satisfaction, and ultimately enhance platform profitability. The amalgamation of AES encryption and Generative AI presents auspicious prospects for value generation, wherein personalized and secure experiences have the potential to captivate and retain users, all the while upholding data privacy and fostering trust. However, it is imperative to acknowledge the inherent limitations of this study and contemplate the prospects for future investigations encompassing broader and more heterogeneous participant cohorts. In its entirety, the research emphasizes the imperative nature of giving precedence to encryption and embracing cutting-edge technologies, including education to foster a secure and user-centric milieu within personal social media platforms.

Acknowledgment

This research was not funded by any grant.

References

[1] Al Badawi, Ahmad, Chao Jin, Jie Lin, Chan Fook Mun, Sim Jun Jie, Benjamin Hong Meng Tan, Xiao Nan, Khin Mi Mi Aung, and Vijay Ramaseshan Chandrasekhar. "Towards the alexnet moment for homomorphic encryption: Hcnn, the first homomorphic cnn on encrypted data with GPUs." IEEE Transactions on Emerging Topics in Computing 9, no. 3 (2020): 1330-1343.

[2] Mansouri, Najme, R. Ghafari, and B. Mohammad Hasani Zade. "Cloud computing simulators: A comprehensive review." Simulation Modelling Practice and Theory 104 (2020): 102144.

[3] Kharroub, Suleiman K., Khalid Abualsaud, and Mohsen Guizani. "Medical IoT: A comprehensive survey of different encryption and security techniques." 2020 International Wireless Communications and Mobile Computing (IWCMC) (2020): 1891-1896.

[4] Hidayat, Taufik, and Rahutomo Mahardiko. "A Systematic literature review method on AES algorithm for data sharing encryption on cloud computing." International Journal of Artificial Intelligence Research 4, no. 1 (2020): 49-57.

[5] Alouffi, Bader, Muhammad Hasnain, Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, and Muhammad Ayaz. "A systematic literature review on cloud computing security: threats and mitigation strategies." IEEE Access 9 (2021): 57792-57807.
[6] Aggarwal, Puneet Kumar, P. S. Grover, and Laxmi Ahuja. "Security aspect in instant mobile messaging applications." In 2018 Recent Advances on Engineering, Technology and Computational Sciences (RAETCS), pp. 1-5. IEEE, 2018.
[7] Johansen, Christian, Aulon Mujaj, Hamed Arshad, and Josef Noll. "The Snowden phone: a comparative survey of secure instant messaging mobile applications." Security and Communication Networks 2021 (2021): 1-30.
[8] Basit, Abdul, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil, and Kashif Kifayat. "A comprehensive survey of AI-enabled phishing attacks detection techniques." Telecommunication Systems 76 (2021): 139-154.
[9] Zhang, Shiwen, Tingting Yao, Voundi Koe Arthur Sandor, Tien-Hsiung Weng, Wei Liang, and Jinshu Su. "A novel blockchain-based privacy-preserving framework for online social networks." Connection Science 33, no. 3 (2021): 555-575.
[10] Singh, Raman, Ark Nandan Singh Chauhan, and Hitesh Tewari. "Blockchain-enabled end-to-end encryption for instant messaging applications." In 2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 501-506. IEEE, 2022.
[11] Wu, Yuezhong, Wei Chen, Shuhong Chen, Guojun Wang, and Changyun Li. "A New User-controlled and Efficient Encrypted Data Sharing Model in Cloud Storage." Recent Patents on Engineering 13, no. 4 (2019): 356-363.
[12] Zhang, Aiqing, and Xiaodong Lin. "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain." Journal of Medical Systems 42, no. 8 (2018): 140.
[13] Schoinianakis, Dimitrios. "Residue arithmetic systems in cryptography: a survey on modern security applications." Journal of Cryptographic Engineering 10, no. 3 (2020): 249-267.
[14] Sadkhan, Sattar B., and Akbal O. Salman. "A survey on lightweight-cryptography status and future challenges." In 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA), pp. 105-108. IEEE, 2018.
[15] Sharma, Arvind K., and S. K. Mittal. "Cryptography & network security hash function applications, attacks, and advances: A review." In 2019 Third International Conference on Inventive Systems and Control (ICISC), pp. 177-188. IEEE, 2019.
[16] Sharma, Arvind K., and S. K. Mittal. "Cryptography & network security hash function applications, attacks, and advances: A review." In 2019 Third International Conference on Inventive Systems and Control (ICISC), pp. 177-188. IEEE, 2019.
[17] Bhimani, Hardik, Anne-Laure Mention, and Pierre-Jean Barlatier. "Social media and innovation: A systematic literature review and future research directions." Technological Forecasting and Social Change 144 (2019): 251-269.
[18] Kreuter, Frauke, Georg-Christoph Haas, Florian Keusch, Sebastian Bähr, and Mark Trappmann. "Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent." Social Science Computer Review 38, no. 5 (2020): 533-549.
[19] Sun, Zhong, Chin-Hsi Lin, Minhua Wu, Jianshe Zhou, and Liming Luo. "A tale of two communication tools: Discussion-forum and mobile instant-messaging apps in collaborative learning." British Journal of Educational Technology 49, no. 2 (2018): 248-261.
[20] Privacy Policy | Snapchat Privacy. “Privacy Policy | Snapchat Privacy,” n.d.
[21] JosephNg, P. S. "Hotel room access control: an NFC approach ecotourism framework." Journal of Science and Technology Policy Management ahead-of-print (2023).
[22] JosephNg, Poh Soon, Xiaoxue Gong, Narinderjit Singh, Toong Hai Sam, Hua Liu, and Koo Yuen Phan. "Beyond Your Sight Using Metaverse Immersive Vision With Technology Behaviour Model." Journal of Cases on Information Technology (JCIT) 25, no. 1 (2023): 1-34.
[23] JosephNg, Poh Soon. "Innovative Usage of Grid Solutions with a Technology Behavior Model in a Medium-Size Enterprise." Applied System Innovation 6, no. 1 (2023): 11.
[24] JosephNg, Poh Soon, and Xiaoxue Gong. "Technology behavior model—Impact of extended reality on patient surgery." Applied Sciences 12, no. 11 (2022): 5607.
[25] JosephNg, P. S. "EaaS infrastructure disruptor for MSE." International Journal of Business Information Systems 30, no. 3 (2019): 373-385.
[26] JosephNg, Poh Soon. "EaaS Optimization: Available yet hidden information technology infrastructure inside medium size enterprise." Technological Forecasting and Social Change 132 (2018): 165-173
[27] JosephNg, Poh Soon, and Chon Moy Kang. "Beyond barebone cloud infrastructure services: Stumbling competitiveness during economic turbulence." Journal of Science & Technology 24, no. 1 (2016): 101-121.

[28] Joseph, Ng Poh Soon, Ahmad Kamil Mahmood, Choo Peng Yin, Wong See Wan, Phan Koo Yuen, and Lim Ean Heng. "Barebone cloud IaaS: revitalization disruptive technology." International Journal of Business Information Systems 18, no. 1 (2015): 107-126.
[29] Joseph, Ng Poh Soon, Ahmad Kamil Mahmood, Peng Yin Choo, See Wan Wong, Koo Yuen Phan, and Ean Heng Lim. "IaaS cloud optimization during economic turbulence for Malaysia small and medium enterprise." International Journal of Business Information Systems 16, no. 2 (2014): 196-208.
[30] Joseph, N. P. S., Ahmad Kamil Mahmood, Peng Yin Choo, See Wan Wong, Koo Yuen Phan, and Ean Heng Lim. "Battles in volatile information and communication technology landscape: the Malaysia small and medium enterprise case." International Journal of Business Information Systems 13, no. 2 (2013): 217-234.
[31] Gong, Xiaoxue, and Poh Soon JosephNg. "Technology Behavior Model—Beyond Your Sight with Extended Reality in Surgery." Applied System Innovation 5, no. 2 (2022): 35.
[32] Rania, F. N., J. Y. Chan, E. S. Ng, J. Y. Fong, S. Z. B. Zulkifli, and P. S. JosephNg. "SDWAN with IDPS Efficient Network Solution." In 2023 IEEE 13th Symposium on Computer Applications & Industrial Electronics (ISCAIE), pp. 145-150. IEEE, 2023.
[33] Subair, M. S. M., A. Sahthiyan, S. S. Bhaskaran, F. N. Zaini, A. F. Rozley, and P. S. JosephNg. "Enhanced Network Solution for Flexible Working Environment." In 2022 IEEE 10th Conference on Systems, Process & Control (ICSPC), pp. 191-196. IEEE, 2022.
[34] Soong, Cai-Juan, Rosshairy Abd Rahman, Razamin Ramli, Mohammed Suhaimee Abd Manaf, and Chek-Choon Ting. "An Evolutionary Algorithm: An Enhancement of Binary Tournament Selection for Fish Feed Formulation." Complexity 2022 (2022).
[35] Ghaleb, Ebrahim AA, P. D. D. Dominic, Narinderjit Singh Sawaran Singh, and Gehad Mohammed Ahmed Naji. "Assessing the big data adoption readiness role in healthcare between technology impact factors and intention to adopt big data." Sustainability 15, no. 15 (2023): 11521.
[36] Wider, Walton, Leilei Jiang, Jiaming Lin, Muhammad Ashraf Fauzi, Jingjing Li, and Choon Kit Chan. "Metaverse chronicles: a bibliometric analysis of its evolving landscape." International Journal of Human–Computer Interaction (2023): 1-14.
[37] A. Bryman and E. Bell, "Business research methods.," Oxford University Press., 2019.
[38] M. N. K. Saunders, P. Lewis, and A. Thornhill, "Research methods for business students.," Pearson., 2019.
[39] Singh, Kuwar Kuldeep VV, and Himanshu Gupta. "A New Approach for the Security of VPN." In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, pp. 1-5. 2016.
[40] Han, Jinguang, Willy Susilo, Yi Mu, and Jun Yan. "Privacy-preserving decentralized key-policy attribute-based encryption." IEEE Transactions on Parallel and distributed systems 23, no. 11 (2012): 2150-2162.
[41] Fallatah, Khalid U., Mahmoud Barhamgi, and Charith Perera. "Personal data stores (PDS): a review." Sensors 23, no. 3 (2023): 1477.
[42] Kotha, Sita Kumari, Meesala Shobha Rani, Bharat Subedi, Anilkumar Chunduru, Aravind Karrothu, Bipana Neupane, and V. E. Sathishkumar. "A comprehensive review on secure data sharing in a cloud environment." Wireless Personal Communications 127, no. 3 (2022): 2161-2188.
[43] Chauhan, Adviti, and Jyoti Gupta. "A novel technique of cloud security based on hybrid encryption by Blowfish and MD5." In 2017 4th International Conference on signal processing, computing and control (ISPCC), pp. 349-355. IEEE, 2017.
[44] Ruzai, Wan Nur Aqlili Wan Mohd, Abderrahmane Nitaj, Muhammad Rezal Kamel Ariffin, Zahari Mahad, and Muhammad Asyraf Asbullah. "Increment of insecure RSA private exponent bound through perfect square RSA diophantine parameters cryptanalysis." Computer Standards & Interfaces 80 (2022): 103584.
[45] Yu, Lantao, Weinan Zhang, Jun Wang, and Yong Yu. "Seqgan: Sequence generative adversarial nets with policy gradient." In Proceedings of the AAAI conference on artificial intelligence, vol. 31, no. 1. 2017.
[46] Karras, Tero, Samuli Laine, and Timo Aila. "A style-based generator architecture for generative adversarial networks." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 4401-4410. 2019.
[47] Navidan, Hojjat, Parisa Fard Moshiri, Mohammad Nabati, Reza Shahbazian, Seyed Ali Ghorashi, Vahid Shah-Mansouri, and David Windridge. "Generative Adversarial Networks (GANs) in networking: A comprehensive survey & evaluation." Computer Networks 194 (2021): 108149.
[48] Lewis, Sarah. "Qualitative inquiry and research design: Choosing among five approaches." Health Promotion Practice 16, no. 4 (2015): 473-475.
[49] Schoonenboom, Judith, and R. Burke Johnson. "How to construct a mixed methods research design." *Kolner Zeitschrift fur Soziologie und Sozialpsychologie* 69, no. Suppl 2 (2017): 107.

[50] Tashakkori, A., & Teddlie, C. (Eds.). (2019). Handbook of Mixed Methods in Social & Behavioral Research (2nd ed.). SAGE Publications.
[51] Flick, U. (2018). Designing Qualitative Research (2nd ed.). SAGE Publications.
[52] Johnson, R. B., & Christensen, L. (2019). Educational Research: Quantitative, Qualitative, and Mixed Approaches (7th ed.). SAGE Publications.
[53] Onwuegbuzie, Anthony J., R. Burke Johnson, and Kathleen MT Collins. "Call for mixed analysis: A philosophical framework for combining qualitative and quantitative approaches." International journal of multiple research approaches 3, no. 2 (2009): 114-139.
[54] Denzin, N. K., & Lincoln, Y. S. (2018). The SAGE Handbook of Qualitative Research (5th ed.). SAGE Publications.
[55] Semwal, Pradeep, and Mahesh Kumar Sharma. "Comparative study of different cryptographic algorithms for data security in cloud computing." In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall), pp. 1-7. IEEE, 2017.
[56] Akhil, K. M., M. Praveen Kumar, and B. R. Pushpa. "Enhanced cloud data security using AES algorithm." In 2017 International Conference on Intelligent Computing and Control (I2C2), pp. 1-5. IEEE, 2017.
[57] Harbi, Yasmine, Zibouda Aliouat, Allaoua Refoufi, and Saad Harous. "Recent security trends in Internet of things: A comprehensive survey." IEEE Access 9 (2021): 113292-113314.
[58] Patil, Priyadarshini, Prashant Narayankar, D. G. Narayan, and S. Md Meena. "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 (2016): 617-624.
[59] Wang, Yong, Aiqing Zhang, Peiyun Zhang, Youyang Qu, and Shui Yu. "Security-aware and privacy-preserving personal health record sharing using consortium blockchain." IEEE Internet of Things Journal 9, no. 14 (2021): 12014-12028.
[60] Namasudra, Suyel. "An improved attribute-based encryption technique towards the data security in cloud computing." Concurrency and Computation: Practice and Experience 31, no. 3 (2019): e4364.
[61] Soofi, A.A., Khan, M.I. and Amin, F.E., 2017. A review on data security in cloud computing. International Journal of Computer Applications, 96(2), pp.95-96.
[62] Sajay, K. R., Suvanam Sasidhar Babu, and Yellepeddi Vijayalakshmi. "Enhancing the security of cloud data using a hybrid encryption algorithm." Journal of Ambient Intelligence and Humanized Computing (2019): 1-10.
[63] Ramachandra, Mohan Naik, Madala Srinivasa Rao, Wen Cheng Lai, Bidare Divakarachari Parameshachari, Jayachandra Ananda Babu, and Kivudujogappa Lingappa Hemalatha. "An efficient and secure big data storage in a cloud environment by using triple data encryption standard." Big Data and Cognitive Computing 6, no. 4 (2022): 101.
[64] Dong, Xuefan, and Ying Lian. "A review of social media-based public opinion analyses: Challenges and recommendations." Technology in Society 67 (2021): 101724.
[65] Chung, Kuo-Cheng, Chun-Hung Chen, Hsueh-Hsuan Tsai, and Ya-Hsueh Chuang. "Social media privacy management strategies: A SEM analysis of user privacy behaviors." Computer Communications 174 (2021): 122-130.
[66] Mitchell, Damion R., and Omar F. El-Gayar. "Privacy and online social networks: A systematic literature review of concerns, preservation, and policies." Pacific Asia Journal of the Association for Information Systems 14, no. 4 (2022): 1.
[67] Senarath, Awanthika, Nalin AG Arachchilage, and Jill Slay. "Designing Privacy for You: A Practical Approach for User-Centric Privacy: Practical Approach for User-Centric Privacy." In Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings 5, pp. 739-752. Springer International Publishing, 2017.
[68] Mahmoodi, Jasmin, Jitka Čurdová, Christoph Henking, Marvin Kunz, Karla Matić, Peter Mohr, and Maja Vovko. "Internet users' valuation of enhanced data protection on social media: Which aspects of privacy are worth the most?." Frontiers in Psychology 9 (2018): 1516.
[69] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
[70] Thabit, Fursan, Sharaf Alhomdy, Abdulrazzaq HA Al-Ahdal, and Sudhir Jagtap. "A new lightweight cryptographic algorithm for enhancing data security in cloud computing." Global Transitions Proceedings 2, no. 1 (2021): 91-99.
[71] Rashidi, Bahram. "A survey on hardware implementations of elliptic curve cryptosystems." arXiv preprint arXiv:1710.08336 (2017).
[72] Roslan, Nur Widad, Normaliza Abd Rahim, Nur Maisarah Roslan, and Siti Nur Aliaa Roslan. "Students' presupposition towards incorporating AI (Artificial Intelligence) technology in virtual and face-to-face classes." International Journal of Advanced Research in Future Ready Learning and Education 27, no. 1 (2022): 16-19.
[73] Masrom, Maslin, Mohd Nazry Ali, Wahyunah Ghani, and Amirul Haiman Abdul Rahman. "The ICT implementation in the TVET teaching and learning environment during the COVID-19 pandemic." International Journal of Advanced Research in Future Ready Learning and Education 28, no. 1 (2022): 43-49.

[74] Zainal, Salbiah, Rasimah Che Mohd Yusoff, Hafiza Abas, Suraya Yaacub, and Norziha Megat Zainuddin. "Review of design thinking approach in learning IoT programming." International Journal of Advanced Research in Future Ready Learning and Education 24, no. 1 (2021): 28-38.