Insights on Data Security Schemes and Authentication Adopted in Safeguarding Social Network

Nithya S[1], Rekha B[2]
Research Scholar, SJB Institute of Technology, Bangalore, India[1]
SJB Institute of Technology, Bangalore, India[2]

***Abstract*—With the increased social network usage, there is a rising concern about potential security and privacy risks related to digital information data. Although there have been numerous studies in this area, a summary is necessary to understand the effectiveness of existing security approaches. The ultimate goal is to provide valuable insights into the effectiveness of existing security schemes in the social network ecosystem. Therefore, the proposed paper discusses the existing research that has been done on authentication and data security measures, including methodologies, issues, benefits, and drawbacks. The inquiry further contributes to highlighting existing research trends and identifying the gap. The paper concludes by stating its learning results that help to open possible insights into the effectiveness of existing security schemes in the social network. Furthermore, blockchain is witnessed with increased interest in distributed security over large data. The paper's outcome states that blockchain-based authentication systems possess better scope if subjected to amending their inherent shortcomings. The findings of this paper emphasize the importance of continuous innovation in data security to ensure the safety and privacy of user data in an ever-evolving digital landscape. This paper offers a foundational aspect for future research toward developing more secure, privacy-preserving solutions for social network users.**

Keywords*—Social network; security threat; authentication; blockchain

I. INTRODUCTION

With an ongoing demand and trend of sharing information, social network has been creating breakthrough innovations in this perspective [1]. It is not only used for sharing information but also extensively used for constructing business opportunities too [2]. A social network can be more generalized, while its implication can be multi-formed based on usage. It can be represented or rather classified into a consumer review network (e.g., TripAdvisor, Yelp, etc.), a network with content curation (e.g., Flipboard, Pinterest, etc.), a forum for discussion (e.g., Quora, Reddit, etc.), the network for media sharing (YouTube, Snapchat, Instagram, etc.), for the social purpose (LinkedIn, Twitter, Facebook, etc.) [3]. This classification of social network usage will eventually state that volumes of information are involved in each application that is stored, shared, and accessed seamlessly and concurrently [4]. Although most social network offers a simplified design that the account owner can customize, a security breach cannot be fully stopped [5]. As social networks are formed by highly interconnected networks over the internet, recognizing and comprehending harmful behavior and differentiating them from regular behavior is quite challenging [6]. The attacker intrudes on the network by hiding their identity as a regular node whose malicious intention cannot be guessed initially. Using various alternative means and tools, it is always possible for an attacker to gain access to the user's private information in the social network [7]. Various studies have reported different variants of intrusive activities in the social network [8]. There are also accomplished studies and ongoing research toward strengthening social network security [9]. However, due to their publicly exposed contents, no tool or program has yet been identified or benchmarked as offering full-proof security in social networks. At present, the blockchain-based approach over large data, along with integrated encryption, is highly in demand and is increasingly adopted for securing the contents to avoid falling into the hands of an attacker [10]. Encryption is another preferred technique for securing the contents to offer more data integrity and privacy [11].

However, blockchain and encryption have potential flaws irrespective of their known beneficial features for security. One of the significant problems in blockchain implementation is achieving performance scalability [12]. It also suffers from limiting the number of transactions a network with the block can process. A different arena of problems also exists for an encryption-based solution. Usually, the strong encryption algorithm is characterized by a higher size of keys and is iterative in its operation [13]. Aside from that, the encryption technique is also reliant on a precise set of resources to be fully executed. These shortcomings eventually offer a possible hindrance to a robust authentication method in social networks.

Therefore, the proposed paper discusses existing security approaches in social networks, specifically emphasizing data security and authentication. The contributions of the paper are i) reviewing existing data security approaches exercised in social networks, ii) highlighting a few prominent works using encryption, privacy preservation, learning approaches, and other miscellaneous methodologies towards data security in social network, iii) identifying advantages and shortcomings of various methodologies, iv) highlighting research trends towards publications and v) exploring prominent research gap. The paper is organized as follows: Section II discusses security insights into social networks and discusses existing data security approaches in Section III. Section IV discusses the

current contribution of authentication. At the same time, research trends are highlighted in Section V. Discussion of the research gap is presented in Section VI. Section VII presents the findings and discussions. Section VIII concludes with highlights of its learning outcomes of the proposed review work in social network security.

II. Security Insights in Social Network

In the current era of social networks, it is noted that most social media applications are publicly disclosed, where it is feasible for the attacker to aggregate the data stealthily without letting the user know [7]. The next level of attackers is more interested in illegitimately gaining access to genuine users' accounts. However, the degree of threat in the social network depends on their planned motive. Attackers deploy various alternative techniques to understand the user in social media, thereby initiating malicious activities. Various forms of intrusive activities performed by attackers are briefed as follows:

- Data Breach: Using multiple alternative approaches, an attacker can steal a user's credentials and gain illegitimate access to their account. This led to a potential breach of users' private information at the hand of the attacker.
- Malware propagation: An attacker can easily divert users to visit their sites using various counterfeited portals. Once the user visits such sites, they are prompted to do simple activities which lead to the activation of malicious codes, and thereby malicious malware starts propagating.
- Data Theft: If an attacker can access any business account on the social network, they can also exfiltrate sensitive information channeled to their account. Hence, both data and account eventually get compromised.
- Impersonation of the brand: An attacker can construct a counterfeited account of a specific brand where prospective customers can be tricked in various ways, either by maliciously draining their finances or stealing confidential data.
- Phishing: Such an attack calls for forwarding a malicious link in messages to the user in various ways. When the user clicks, it directs them to various security threats, including account hijacking. It could also lead to latent stealing of personal information stored in the device.
- Social Engineering: In this form of threat, the attacker convinces or tricks the user of their genuine and trustworthy profile. The users are prompted to forward either a financial asset or high-profile information at their wish that is maliciously forwarded to the attacker's account.

All of the above-mentioned invasive actions are common, but a standard classification also explains their variations. Apart from the above-mentioned activities, other forms of attacks in social network are cyberbullying too which are used to intimidate and harass the user by posting objectional comments and spreading counterfeited rumors. Fig.1 highlights further classification in the form of traditional adversaries, modern adversaries, and targeted adversaries. All these adversaries work with different techniques; hence, there is no fair possibility of developing a common solution to stop all these adversaries. Work is being carried out towards modeling lethal threats in the social network [8], yet it has a restricted security feature.

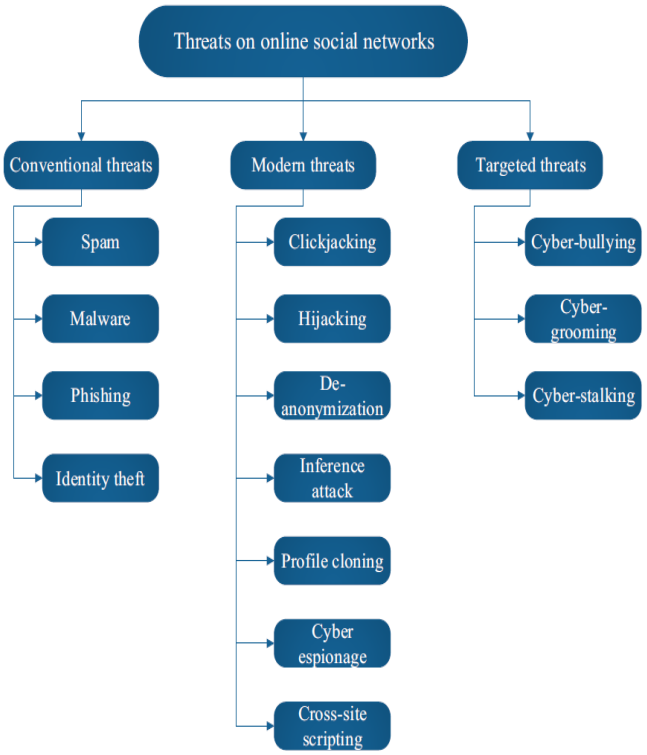

Fig. 1. Classification of adversaries in social networks [14].

Nevertheless, much research is being done to combat the risks spread through social networks. [8], there is also the evolution of smart solutions: cyberstalking, clickjacking, cyber grooming, cyberbullying detection, and phishing detection. From the commercial application viewpoint, the normal recommendation towards securing a social network is to adopt a strong credential, restrict location sharing, install threat detection software, understand and be aware of a third-party application, be vigilant towards sharing content, and review every new friend request [14]. However, from the research perspective, it is suggested to use a strong security protocol that uses potential data encryption, understanding the network connectivity, and vigilant towards usage of underlying threads in the device [15].

Unfortunately, the degree of attacks on social networks is consistently rising despite knowing the facts to be considered for security. It will eventually mean a potential tradeoff between actual security demand and existing effectiveness in security schemes. One of the most primitive intrusion points is via weak authentication in social networking applications [16][17]. Unfortunately, denser and more aggressive authentication protocol usage will also affect the actual motive of social networks, which is towards large-scale data sharing in

a multi-dimensional manner. Further social networking applications migrating to a cloud-based ecosystem offer some application-feature-based advantages but at the cost of security. Moreover, as one social network application is also connected to different applications, the level of threat propagation is quite excessive. Therefore, there is a potential demand to investigate better authentication with better data security. The next section discusses some of the contributions of existing schemes toward securing social networks.

III. Data Security Approaches in Social Network

The prior section noted various security threats in social network applications. There is also the evolution of various research techniques to circumvent such forms of threats due to different forms of threats. Due to a large chain of sophisticated networks, offering robust data security in the social network is challenging. Therefore, this section outlines the contribution of some of the identified essential techniques to offer data security.

A. Encryption-based Approaches

This approach is designed and implemented to encrypt the data propagated in social media. From the viewpoint of data, it is found that multimedia data is in circulation and shared in social networks along with the text. The recent work carried out by Ali, and Ali [18] has implemented an encryption strategy toward securing a color image by adopting a chaotic map. A non-linearity element is generated by amending the pixel values, which further results in a random sequence by diffusion. This operation is followed by mixing the encrypted image to generate a consistent distribution of randomness further. Huang et al. also investigated data encryption [19], where a re-encryption policy is applied based on the identity-based sharing of confidential data.

One of the significant advantages of this policy is that it only permits a re-encryption process for matched encrypted data, thereby offering better access control. The work by Qiu et al. [20] discussed a selective encryption system based on coding an embedded block. The investigation also uses optimized truncation to secure a selected part of bitstreams. The work by Zuo et al. [21] used homomorphic encryption to secure the graph operation in social networks associated with untrusted clouds. This investigation model offers effective data security and retains better privacy preservation. The beneficial point of adopting an encryption-based approach is its explicit resistivity towards a specific attack; however, its scope of applicability is limited to specific intruders and involves quite a sophisticated key computation that demands many computational resources.

B. Privacy Preservation-based Approaches

This type of security approach mainly concerns safeguarding all the necessary information that holds privacy details of the data and the user in the social network. A unique investigation formulated by Barni et al. [22] discussed security issues related to adopting biometrics in social media, specifically using iris. As a solution, the author has used a generative adversarial network to generate images with eliminated biometric information in social networks. Another work by Chen et al. [23] used an integrated method of searchable encryption and blockchain to offer privacy. The presented mechanism is highly decentralized and uses public-key encryption to secure communication in a vehicular network. Li et al. [24] have provided a de-anonymization strategy for the heterogeneous social network in a different piece of work—the model claims to improve the detection system by using user profile and network structure information. Li et al. also presents a similar work form [25]. The investigation model assesses privacy factors associated with the behavioral attributes in social networks based on structural similarity.

The work carried out by Qu et al. [26] has addressed the solution to the gap between the utility of data and privacy customization. The investigation model customizes the level of protecting privacy by using the shortest distance between two nodes in the social network. The model has also adopted an improved version of the Laplacian method for noise modeling that is finally subjected to decoupling to prove its resistivity against collusion attack. Another unique work is carried out by Xu et al. [27] investigating the context behind the communication of anti-social elements using social networks. This investigation has presented a mechanism to retrieve data associated with privacy preservation which further performs a query on suspect communication. The method also securely implements classification and regression trees to resist privacy leakage. The work by Xu et al. [28] presented a selection technique of an optimal trajectory and adopted a heuristic method. The implemented technique also performs clustering operations for facilitating multiple forms of trajectories that finally assist in discovering the community. Assurance of privacy preservation was also discussed by Yin et al. [29] using deep learning approaches.

A hybrid scheme has been deployed using a Bayesian network, a federated learning approach, and a sparse differential gradient. This work aims to optimize the functional encryption operation to secure data sharing among social network multi-parties. A similar investigation was also carried out by Zhang et al. [30], where the data privacy factor is assessed by evaluating the sentence correlation using a convolution neural network and the firefly algorithm. This work aims to ensure secure privacy preservation for social users using large communication scenarios like Internet-of-Things (IoT). The investigation by Zhu et al. [31] presented a computational model for the propagation of privacy information for more in-depth identification of the malicious nature of social nodes. The benefit of adopting the privacy preservation model in securing social network communication is that it offers various techniques while offering higher coverage of security problems in the social network. However, the limiting factor associated with privacy preservation schemes of existing studies is related to their non-applicability in a different test environment.

C. Learning-based Approaches

Learning-based approaches are a part of artificial intelligence that can identify and solve complex problems facilitated by predictive outcomes. The algorithm written for

learning-based approaches offers an extensive capability of execution with a higher adaptation rate of intelligence. Adopting a learning approach facilitates evaluating the problems in social networks and further evolves with more accurate solutions.

The investigation carried out by Abbasi et al. [32] essentially focuses on implementing a learning approach toward identifying any drift factor associated with the concept of massive ranges of social data. The author uses ensemble learning for this purpose, where the idea is to perform an optimal classification of social data to identify the concept drift. The work carried out by Chen et al. [33] presented a model for evaluating multiple trusts for users of social networks considering discrete criteria as well as features, e.g., link, feedback, behavior, and profile. The investigation model implements multiple machine-learning approaches to evaluate its performance.

Another learning-based approach is implemented by Gao et al. [34] to confirm the presence of a Sybil attacker. The technique implements a convolution neural network for extracting low-end and high-end features by Long Short-Term Memory. Discussion towards the applicability of the deep learning approach to the social network security aspect has been carried out by Garg et al. [35]. The investigation has emphasized using Software Defined Networks (SDN) to improve social network security systems. The first module of the investigation uses a support vector machine with gradient descent for anomaly detection.

In contrast, the second module of the investigation implements SDN to ensure a better delivery system. Mei et al. [36] have presented a solution to inference attacks in social media by amending the existing deep learning approach. The work by Sansonetti et al. [37] has presented a technique for identifying the propagation of counterfeited news in social media. The learning-based technique is applied for this analysis in both online and offline modes.

Another learning-based approach is discussed by Shen et al. [38], where an encryption system and blockchain have been introduced to secure the classification operation. The presented investigation uses a support vector machine for performing training operations, while the scheme also assists in resisting any collusion of data involved in it. The adoption of an adversarial learning scheme has been presented by Zhang et al. [39], emphasizing privacy protection. The research helps defend against attacks that try to establish a connection between two nodes in graph embedding.

Consequently, the scheme minimizes the accuracy of the prediction of an attacker. The beneficial factor for adopting a learning-based approach is its effective modeling toward predictive computation considering complex security loopholes. However, a closer look into existing approaches exhibits the prevalence of using static use cases of adversaries, implying its applicability only to specific case studies. In addition, the computational complexity linked to a higher number of repeats is still unaddressed by the current scheme.

D. Miscellaneous Approaches

Apart from the conventional security practices in social networks seen in prior sections, various off-beat mechanisms are introduced to address similar security problems. From the work presented by Song et al. [40], game theory has been increasingly adopted in modeling social networks. This article claims that game theory is used in behavioral analysis, community identification, and information dissemination to improve the security of social networks by improving access controls and formulating privacy policies. The adoption of game theory is seen in the work of Du et al. [41], where privacy protection is emphasized using the evolutionary game concept in the social network. The idea of this work is to investigate the selection strategy of a user toward privacy protection. The outcome of this investigation is analyzed concerning computational performance cost. Although blockchain is also reported to be used in securing social network communication and services, some studies enhance blockchain's usage towards more security. The work carried out by Fan et al. [42] has used blockchain to offer better non-repudiation in security services as well as to perform a better formulation of access policy using a secret sharing scheme.

Further information used for constructing access policy is hidden for enhanced security. The work carried out by Gao et al. [43] has developed a game-based framework to investigate the social reputation and its impact on controlling data access. A similar line of work is also carried out by Wang et al. [44] towards identifying and resisting counterfeited messages. Huang et al. also adopted a game-based framework [45] to construct an economic model. The core idea of this part of the implementation is to identify any alteration in the network concerning user income. The implementation also assists in developing a model for price decisions under a specific network condition.

The framework developed by Kong et al. [46] has constructed a security framework for strengthening the reputation system over the cloud ecosystem considering the use case of a large-scale healthcare system. The investigation has implemented a convolution neural network that categorizes textual data followed by applying a dynamic game model for constructing a strategy toward incentive allocation.

Su and Xu [47] have worked on allocating resources toward secure communication in social media using the game-based model. The primary agenda of this work is to carry out secure group-based communication for social networks followed by resource gain improvement. Sun et al. [48] have presented a key-based encryption strategy for securing social network data. Using a secure data-sharing scheme, the idea is to identify and protect against intrusion. Table I summarizes all the above data security approaches in the social network.

TABLE I. SUMMARY OF DATA SECURITY APPROACHES

Authors	Problems Addressed	Methodology Adopted	Advantage
Ali & Ali [18]	Image encryption	Chaotic Map	Efficient non-linearity in encryption
Huang et al.[19]	Secure Data Sharing and encryption	Identity-based Re-encryption	Better access control
Qiu et al. [20]	Data security	Selective encryption	Can secure text, image, and video file
Zuo et al. [21]	Data security	Homomorphic encryption	Ensure better data ownership
Barni et al. [22]	Privacy issues in biometrics	Generative adversarial network	Significantly control
Chen et al. [23]	Privacy in vehicular network	Searchable encryption	Satisfactory response time
Li et al. [24]	De-anonymization of user	Modeling using user profile and network structure	Maximize accuracy of detection
Li et al. [25]	Privacy measurement	Structural similarity model of behavior intimacy	Effectively reduces privacy leakage
Qu et al. [26]	Privacy preservation	Analytical model using the Laplacian method	Customization privacy
Xu et al. [27]	Sensing criminal communication in social network	Retrieval of data for privacy, classification & regression tree	Significantly less overhead
Xu et al. [28]	Discovering latent trajectory	Community discovery model using clustering	Offers higher accuracy
Yin et al. [29]	Data sharing in multi-party	Sparse differential gradient, functional encryption, federated learning	Enhance transmission efficiency
Zhang et al. [30]	Privacy preservation for social users in IoT	Convolution Neural Network, Firefly algorithm,	Optimize more usage of data in social network
Zhu et al. [31]	Privacy propagation	Empirical approach	Applicable for dynamic social network
Abbasi et al. [32]	Identification of concept drift	Ensemble learning	Satisfactory accuracy
Chen et al. [33]	Trust evaluation in social network	Multiple machine learning for feature selection	Better accuracy performance
Gao et al. [34]	Detection of Sybil attack	Long Short-Term Memory	Higher accuracy in detection
Garg et al. [35]	Anomaly detection	Support Vector Machine (Gradient Descent), SDN	Ensure secure flow routing
Mei et al. [36]	Inference arrack in social network	Revised convolution neural network	Satisfactory accuracy performance
Sansonetti et al. [37]	Identification of counterfeited news in social media	Learning-based approach	Overall satisfactory accuracy performance
Zhang et al. [39]	Privacy preservation	Adversarial learning	Higher preservation performance
Song et al. [40]	Review of game theory	Reviewing existing approaches	Higher applicability
Du et al. [41]	Privacy protection	Evolutionary game	Offer consistency in privacy protection with increased network size.
Fan et al. [42]	Secure data sharing	Blockchain, secret sharing	Resistive against collusion attack
Gao et al. [43]	Impact on social reputation	Game-based framework	Improve the rate of cloud storage
Wang et al. [44]	Counterfeited Message	Game-based model	Increased probability of detection of malicious message
Huang et al. [45]	Issues in price decisions in cyber-physical system	Game-based model	Suitable for price adjustment
Kong et al. [46]	Data privacy for large network	Convolution neural network	Improve model reliability
Su and Xu [47]	Secure resource allocation	Coalition game model	Effective resource efficiency

IV. AUTHENTICATION APPROACHES IN SOCIAL NETWORK

Different authentication mechanisms have evolved with the increasing features of social network applications. However, such authentication mechanism differs strongly between commercially used applications and those reported in scientific papers. The commercially available applications use normal user identity-based credential mechanism that adopts user name and password. The authentication mechanism could be carried out in single execution and sometimes in multiple executions. However, almost all commercially available social network applications use a static form of security token to authenticate the user, where traces of authentications are stored in mobile devices within its cache memory system. This is a highly vulnerable state for the user where their services and data are exposed to a potential threat. On the other hand, various recently developed protocols have been carried out to strengthen and evolve of authentication scheme.

The work by Alvarez et al. [49] has discussed different authentication system mechanisms for strengthening the associated privacy factors. The investigation suggests the usage of biometrics for this purpose. The majority of the social network application is investigated using a graphical concept. One such work by Jin et al. [50] emphasizes implementing a stochastic approach to authenticate such graphs. The technique

uses a supervised learning mechanism to identify such malicious activities in the social network. An authentication model discussed by Megouache et al. [51] has presented a unique scheme for privacy preservation in an environment with multi-clouds. The investigation uses an encryption approach toward data integrity as well as authentication. The work carried out by Park et al. [52] have presented distributed scheme of authentication considering multi-factor authentication based on trust score. Ruan et al. [53] have presented a work towards location privacy where replicated information is used to secure the user's privacy. At the same time, it controls all sorts of inference of activity track of use from the location server to keep it more secure. The work by Sinha et al. [54] used elliptical curve encryption and symmetric encryption to resist replay attacks and cryptanalysis attacks in the social network. The investigation model has implemented a key exchange mechanism to carry out authentication. Soni et al. [55] have presented a security scheme using fuzzy c-means algorithm. In contrast, it uses a series of encryption techniques (e.g., Rivest Shamir Algorithm (RSA), Advanced Encryption Standard (AES), and Rivest Cipher 6 (RC6)) to cipher the data further. A recent investigation has also witnessed the adoption of blockchain to secure the trust factor in next-generation networks based on user behavior.

Tu et al. [56] carried out an investigation where a novel trust control modeling is based on user behavior. A unique authentication model is presented by Xu et al.[57] over the storage framework associated with the social network using blockchain. The authentication is provided by incorporating secure access control developed by integrating the Clark-Wilson model and blockchain technology. The adoption of homomorphic encryption was carried out by Zuo et al. [58], where a sub-graph matching mechanism was introduced to carry out authentication. The cloud carries out the query processing of the subgraph without any dependency on the secure and sensitive information of the user. The investigation model of authentication is claimed to offer data integrity too. Table II highlights the summarization of the existing authentication schemes.

TABLE II. SUMMARY OF AUTHENTICATION APPROACHES

Authors	Problems Addressed	Methodology Adopted	Advantage
Alvarez et al. [49]	Sensor-based authentication	Review work	Elaborated discussion of existing methods
Jin et al. [50]	Authentication of graph	Supervised learning, stochastic	84.4% of accuracy rate
Megouache et al. [51]	Authentication & Integrity	Encryption-based model	Stabilized system
Park et al.[52]	Cyber-security threat	Distributed authentication model	Reduced latency
Ruan et al. [53]	Privacy protection	Replicated identity construction	Lower communication and computation cost
Sinha et al. [54]	Replay attack on social network	Key exchange, Elliptical curve cryptography, symmetric encryption	Less processing time
Soni et al. [55]	Data security in the cloud	Fuzzy c-Means clustering, RSA, AES, RC6	Simplified technique
Tu et al. [56]	attacks in next-generation network	Blockchain-based trust model	Minimized network threats
Xu et al.[57]	Access Control on storage	Blockchain, Clark-Wilson Model	Offers data integrity
Zuo et al. [58]	Privacy preservation	Homomorphic encryption	Offers data privacy and integrity

V. RESEARCH TRENDS

To understand the existing research trend, data were collected from well-known publications, e.g., IEEE Xplore, Springer, ACM, Wiley, and Elsevier, ranging between the publication year of 2012-2022. It was noted that approximately 6538 conference papers and 1395 journals are being published towards discussing and evolving out of security models associated with social networks in IEEE alone [59]. After a complete evaluation of overall methodologies, it has been noted that there are different variants of techniques towards incorporating security, authentication-based approaches, blockchain technology, investigation towards data integrity, adoption of game theoretical framework, usage of different types of machine learning models, studies towards privacy preservation, and encryption-based approaches. All the studies mentioned above methodology are witnessed to address different forms of security problems arising in social media. From Fig. 2 it can be noted that more studies have been carried out to emphasize privacy preservation in social networks. The studies adopting blockchain-based and encryption-based mechanisms are also increasingly evolving. However, many of these approaches are very less than privacy preservation approaches. Games and learning-based programs are still in the early stages of development.

Therefore, the inference obtained from the simplified analysis of the research trend of publication is as follows:

- The amount of research on protecting privacy on social networks is relatively higher. The scope of this outcome is that existing privacy preservation is carried out considering a set of adversaries that it can successfully resist [14],[16],[21]-[31],[39], [49]. Therefore, such a privacy preservation scheme is robust to act against specific attacks; however, the prime shortcoming is that there is a need to address dynamic attackers in the social network that are few to be reported. Similar problems are also applicable to data integrity schemes.
- From an implementation standpoint, research on authentication and encryption-based systems is closely related [11], [13], [18]-[20], [23]. There is an increasing trend toward using a symmetric key, elliptical curve cryptography, RSA, and many other approaches in public key encryption. Such encryption approaches introduce sophisticated techniques of private key

computation without considering encrypting default public keys. Apart from this, most authentication-based approaches using key-based mechanisms do not consider the device complexity used in social networks. Each social network application has a unique performance signature on different devices, which is not evaluated in existing research.

- Machine learning [16], [29],[32]-[35], [37], [39] and game theoretical models [40]-[47] are slowly gaining pace toward social network security. However, such approaches are yet to be addressed from their practical world implementation owing to their larger dependencies on additional information and data. The complex problems associated with them are yet to be researched.

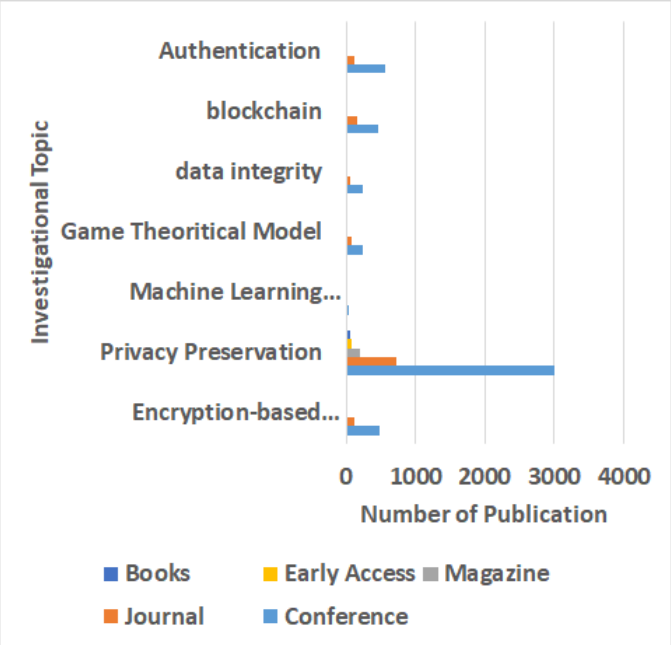

Fig. 2. Research trends of publication (2012-2022).

VI. Gap Analysis

Undoubtedly, current research on secure social network applications has significantly contributed. With different classes of algorithms, various security solutions are available to resist potential threats. After reviewing various classes of existing schemes for securing communication in social networks, the following shortcomings have been witnessed in the form of a research gap:

- *Attack Specific Investigation*: There are variously reported adversaries present in the social network, e.g., cross-site scripting, clickjacking, SQL injection, whaling attack, malware propagation, spamming attack, etc., apart from various other conventional reported attacks. Different variants of methodologies presented to date have used only specific forms of attacks, and hence that solution is rendered inapplicable when exposed to a different set of attacks. The problem becomes more significant when the attacker introduces malicious activities dynamically. Hence, there is a need to develop an adversarial model first which bears the maximum characteristics of existing attackers to prove the resiliency of security protocols.

- *Unbalance computational efficiency*: The primary stage of developing the social network is constructing a higher linked and inter-connected topology of the user (or nodes). As social networking application is run over user handheld device, hence, is predicted to support such resource constraint device. Applying a strong encryption algorithm will only negatively affect the system's performance, even if it can resist certain threats. Hence, introducing a simplified, lightweight encryption scheme can only ensure computational efficiency. Unfortunately, no reported work has presented evidence of consistency in the computational performance of security when confronted with large and heavy traffic on the social network.

- *Usage of Conventional Authentication Scheme*: From the viewpoint of practical deployment, existing social network applications still use static passwords. Adopting a key-management scheme induces maximized resource dependencies while using encryption sets introduces computational burden over the long run. Existing multi-factor schemes are executed without protecting the location where algorithms are executed and thereby introduce a tradeoff between security and computational demands.

- *Lack of integrated schemes*: As a social network is a large chain of nodes formed in a complex way, data leakage is also possible. Hence, the authentication mechanism should be studied alongside data privacy and integrity to offer maximum protection. Such integrated schemes are not yet found been introduced or benchmarked.

VII. Findings and Discussion

There are mainly two core classes of research toward the direction of security in the existing system, i.e., data security and authentication approaches. More studies have been carried out on data security approaches compared to authentication approaches. The core approaches discussed in this paper are encryption-based, privacy preservation-based, machine learning-based, and game-based modeling to strengthen social network security.

Reviewing existing research trends showcase more concentrated work towards privacy preservation while very little research is towards learning and data integrity-based methods. It is, therefore, evident that current solutions do not provide comprehensive security services and can only provide data integrity, data privacy, or non-repudiation. A social network is a complex network exposed to multi-dimensional threats. Hence, it's predicted to offer maximum security services, which is not found reported in existing security schemes.

It has been also identified that the blockchain is one of the evolving solutions for security in the social network. However,

there are various pitfalls seen in implementation effectiveness. i) blockchain-based scheme demands a potential form of the secured and interconnected topology of nodes integrated with a service provider with resources to operate. Existing blockchain schemes don't address this fact, ii) adoption of blockchain approach is associated with complexity, especially if it's a large and heterogeneous network of complex user behavior; hence computational burden is inevitable in the blockchain. Hence, there is potential for improving these blockchain problems to harness their security strength. None of the existing solutions has discussed the essential type of content in the social network. Textual content is more extensively used than other forms, e.g., images, GIFs, video, and audio. Encryption algorithms are eventually a better alternative; however, achieving encryption performance with computation and service relaying performance in social networks is yet to be seen. Therefore, there is a need for an investigation that would emphasize securing the text contents from dynamic attackers in the social network.

VIII. Conclusion and Future Work

This paper has presented a compact discussion of securing communication in the social network. It is noted that various classes of methodologies are being adopted towards improving the security aspect with claimed benefits; however, the paper has identified a shortcoming associated with it. Hence, based on the complete review, it can be said that multifold findings state that there is still a large open scope for improving the security aspect of the social network. Exploring the existing research literature followed by methodologies, challenges, benefits, and drawbacks has highlighted the need for continuous innovation and improvement to protect user data effectively. The paper also emphasizes the growing interest in blockchain technology as a promising distributed security and authentication solution. Ultimately, the findings of this paper underscore the importance of a collaborative and multidisciplinary approach to data security and authentication in social networks. In future work, the scope of this paper will be extended toward modeling computationally efficient and robust security approaches to address dynamic security and privacy issue in social networking applications.

References

[1] M. Burcher, Social Network Analysis, and Law Enforcement-Applications for Intelligence Analysis, Springer International Publishing, ISBN: 9783030477714, 3030477711, 2020.

[2] S. Alavi, V. Ahuja, Managing Social Media Practices in the Digital Economy, IGI Global, ISBN: 9781799821878, 1799821870, 2019.

[3] D. Zahay, M. L. Roberts, J. Parker, D. I. Barker, M. Barker, Social Media Marketing: A Strategic Approach, Cengage Learning, ISBN: 9780357516287, 0357516281, 2022.

[4] A. E. Hassanien, A. Abraham, M. Panda, Big Data Analytics-A Social Network Approach, Taylor & Francis Group, ISBN: 9780367780777, 0367780771, 2021.

[5] B. B. Gupta, S. R. Sahoo, Online Social Networks Security-Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN: 9781000347111, 1000347117, 2021.

[6] R. Luttrell, Social Media-How to Engage, Share, and Connect, Rowman & Littlefield Publishers, ISBN: 9781538154434, 1538154439, 2021.

[7] B.D. Deebak, Fadi Al-Turjman, Security in IoT Social Networks, Elsevier Science, ISBN: 9780128216033, 0128216034, 2020.

[8] E. Etuh, F. S. Bakpo, E. Agozie H, "Social Media Networks Attacks and their Preventive Mechanisms: A Review," ArXiv, Social and Information Networks, 2022. DOI: https://doi.org/10.48550/arXiv.2201.03330.

[9] R. Abid, M. Rizwan, P. Veselý, A. Basharat, U. Tariq, and A. R. Javed, "Social Networking Security during COVID-19: A Systematic Literature Review", Hindawi-Wireless Communications and Mobile Computing, Article ID 2975033, 2022, DOI: https://doi.org/10.1155/2022/2975033.

[10] S. X. Wu, Z. Wu, S. Chen, G. Li and S. Zhang, "Community Detection in Blockchain Social Networks," in Journal of Communications and Information Networks, vol. 6, no. 1, pp. 59-71, March 2021, doi: 10.23919/JCIN.2021.9387705.

[11] H. Qiu, M. Qiu, M. Liu, and Z. Ming, "Lightweight Selective Encryption for Social Data Protection Based on EBCOT Coding," in IEEE Transactions on Computational Social Systems, vol. 7, no. 1, pp. 205-214, Feb. 2020, doi: 10.1109/TCSS.2019.2952553.

[12] A. Hafid, A. S. Hafid and M. Samih, "Scaling Blockchains: A Comprehensive Survey," in IEEE Access, vol. 8, pp. 125244-125262, 2020, doi: 10.1109/ACCESS.2020.3007251.

[13] C. -I. Fan, Y. -F. Tseng, J. -J. Huang, S. -F. Chen and H. Kikuchi, "Multireceiver Predicate Encryption for Online Social Networks," in IEEE Transactions on Signal and Information Processing over Networks, vol. 3, no. 2, pp. 388-403, June 2017, doi: 10.1109/TSIPN.2017.2697580.

[14] A.K. Jain, S.R. Sahoo, & J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," SpringerOpen-Complex & Intelligent Systems volume 7, pp.2157–2177, 2021. DOI:https://doi.org/10.1007/s40747-021-00409-7.

[15] S. Szymoniak, "Security protocols analysis including various time parameters," AIMS-Press-Mathematical Biosciences and Engineering, Volume 18, Issue 2, pp.1136-1153, 2021. Doi: 10.3934/mbe.2021061.

[16] T. Guo, F. Li, "Machine Learning-based Online Social Network Privacy Preservation," ACM-Proceedings of the 2022 ACM on Asia Conference on Computer and Communications SecurityMay 2022 Pages 467–478https://doi.org/10.1145/3488932.3517405.

[17] X. Yu, R. Ge, F. Li, "Research on Blockchain-Based Identity Authentication Scheme in Social Networks," ACM-Machine Learning for Cyber Security: Third International Conference, ML4CS 2020, Guangzhou, China, October 8–10, 2020, Proceedings, Part IOct 2020 Pages 558–565https://doi.org/10.1007/978-3-030-62223-7_49.

[18] T.S. Ali, R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," Springer-Multimedia Tools and Applications, vol.81, pp.20585–20609, 2022, DOI: https://doi.org/10.1007/s11042-022-12268-6.

[19] Q. Huang, Y. Yang, J. Fu, "PRECISE: Identity-based private data sharing with conditional proxy re-encryption in online social networks," Elsevier-Future Generation Computer Systems, vol.86, pp.1523-1533, 2018 DOI: http://dx.doi.org/10.1016/j.future.2017.05.026.

[20] H. Qiu, M. Qiu, M. Liu, and Z. Ming, "Lightweight Selective Encryption for Social Data Protection Based on EBCOT Coding," in IEEE Transactions on Computational Social Systems, vol. 7, no. 1, pp. 205-214, Feb. 2020, doi: 10.1109/TCSS.2019.2952553.

[21] X. Zuo, L. Li, S. Luo, H. Peng, Y. Yang, and L. Gong, "Privacy-Preserving Verifiable Graph Intersection Scheme With Cryptographic Accumulators in Social Networks," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4590-4603, 15 March 15, 2021, doi: 10.1109/JIOT.2020.3028417.

[22] M. Barni, R. D. Labati, A. Genovese, V. Piuri and F. Scotti, "Iris Deidentification With High Visual Realism for Privacy Protection on Websites and Social Networks," in IEEE Access, vol. 9, pp. 131995-132010, 2021, doi: 10.1109/ACCESS.2021.3114588.

[23] B. Chen, L. Wu, H. Wang, L. Zhou, and D. He, "A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5813-5825, June 2020, doi: 10.1109/TVT.2019.2959383.

[24] H. Li, Q. Chen, H. Zhu, D. Ma, H. Wen, and X. S. Shen, "Privacy Leakage via De-Anonymization and Aggregation in Heterogeneous Social Networks," in IEEE Transactions on Dependable and Secure

Computing, vol. 17, no. 2, pp. 350-362, 1 March-April 2020, doi: 10.1109/TDSC.2017.2754249.

[25] X. Li, Y. Xin, C. Zhao, Y. Yang, S. Luo, and Y. Chen, "Using User Behavior to Measure Privacy on Online Social Networks," in IEEE Access, vol. 8, pp. 108387-108401, 2020, doi: 10.1109/ACCESS.2020.3000780.

[26] Y. Qu, S. Yu, W. Zhou, S. Chen, and J. Wu, "Customizable Reliable Privacy-Preserving Data Sharing in Cyber-Physical Social Networks," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 1, pp. 269-281, 1 Jan.-March 2021, doi: 10.1109/TNSE.2020.3036855.

[27] J. Xu, A. Wang, J. Wu, C. Wang, R. Wang, and F. Zhou, "SPCSS: Social Network Based Privacy-Preserving Criminal Suspects Sensing," in IEEE Transactions on Computational Social Systems, vol. 7, no. 1, pp. 261-274, Feb. 2020, doi: 10.1109/TCSS.2019.2960857.

[28] C. Xu, L. Zhu, Y. Liu, J. Guan, and S. Yu, "DP-LTOD: Differential Privacy Latent Trajectory Community Discovering Services over Location-Based Social Networks," in IEEE Transactions on Services Computing, vol. 14, no. 4, pp. 1068-1083, 1 July-Aug. 2021, doi 10.1109/TSC.2018.2855740.

[29] L. Yin, J. Feng, H. Xun, Z. Sun and X. Cheng, "A Privacy-Preserving Federated Learning for Multi-party Data Sharing in Social IoTs," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2706-2718, 1 July-Sept. 2021, doi: 10.1109/TNSE.2021.3074185.

[30] P. Zhang, Y. Wang, N. Kumar, C. Jiang, and G. Shi, "A Security- and Privacy-Preserving Approach Based on Data Disturbance for Collaborative Edge Computing in Social IoT Systems," in IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 97-108, Feb. 2022, doi: 10.1109/TCSS.2021.3092746.

[31] T. Zhu, J. Li, X. Hu, P. Xiong, and W. Zhou, "The Dynamic Privacy-Preserving Mechanisms for Online Dynamic Social Networks," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 6, pp. 2962-2974, 1 June 2022, doi: 10.1109/TKDE.2020.3015835.

[32] A. Abbasi, A. R. Javed, C. Chakraborty, J. Nebhen, W. Zehra and Z. Jalil, "ElStream: An Ensemble Learning Approach for Concept Drift Detection in Dynamic Social Big Data Stream Learning," in IEEE Access, vol. 9, pp. 66408-66419, 2021, doi: 10.1109/ACCESS.2021.3076264.

[33] X. Chen, Y. Yuan, L. Lu, and J. Yang, "A Multi-dimensional Trust Evaluation Framework for Online Social Networks Based on Machine Learning," in IEEE Access, vol. 7, pp. 175499-175513, 2019, doi 10.1109/ACCESS.2019.2957779.

[34] T. Gao, J. Yang, W. Peng, L. Jiang, Y. Sun and F. Li, "A Content-Based Method for Sybil Detection in Online Social Networks via Deep Learning," in IEEE Access, vol. 8, pp. 38753-38766, 2020, doi: 10.1109/ACCESS.2020.2975877.

[35] S. Garg, K. Kaur, N. Kumar and J. J. P. C. Rodrigues, "Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective," in IEEE Transactions on Multimedia, vol. 21, no. 3, pp. 566-578, March 2019, doi 10.1109/TMM.2019.2893549.

[36] B. Mei, Y. Xiao, R. Li, H. Li, X. Cheng, and Y. Sun, "Image and Attribute Based Convolutional Neural Network Inference Attacks in Social Networks," in IEEE Transactions on Network Science and Engineering, vol. 7, no. 2, pp. 869-879, 1 April-June 2020, doi: 10.1109/TNSE.2018.2797930.

[37] G. Sansonetti, F. Gasparetti, G. D'aniello, and A. Micarelli, "Unreliable Users Detection in Social Media: Deep Learning Techniques for Automatic Detection," in IEEE Access, vol. 8, pp. 213154-213167, 2020, doi: 10.1109/ACCESS.2020.3040604.

[38] M. Shen, J. Zhang, L. Zhu, K. Xu, and X. Tang, "Secure SVM Training Over Vertically-Partitioned Datasets Using Consortium Blockchain for Vehicular Social Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5773-5783, June 2020, doi: 10.1109/TVT.2019.2957425.

[39] K. Zhang, Z. Tian, Z. Cai, and D. Seo, "Link-privacy preserving graph embedding data publication with adversarial learning," in Tsinghua Science and Technology, vol. 27, no. 2, pp. 244-256, April 2022, doi: 10.26599/TST.2021.9010015.

[40] X. Song, W. Jiang, X. Liu, H. Lu, Z. Tian, and X. Du, "A survey of game theory as applied to social networks," in Tsinghua Science and Technology, vol. 25, no. 6, pp. 734-742, Dec. 2020, doi: 10.26599/TST.2020.9010005.

[41] J. Du, C. Jiang, K. -C. Chen, Y. Ren, and H. V. Poor, "Community-Structured Evolutionary Game for Privacy Protection in Social Networks," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 574-589, March 2018, doi: 10.1109/TIFS.2017.2758756.

[42] K. Fan et al., "A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5826-5835, June 2020, doi: 10.1109/TVT.2020.2968094.

[43] L. Gao, Z. Yan, and L. T. Yang, "Game Theoretical Analysis on Acceptance of a Cloud Data Access Control System Based on Reputation," in IEEE Transactions on Cloud Computing, vol. 8, no. 4, pp. 1003-1017, 1 Oct.-Dec. 2020, doi: 10.1109/TCC.2016.2632110.

[44] X. Wang et al., "Game Theoretic Suppression of Forged Messages in Online Social Networks," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 3, pp. 1601-1611, March 2021, doi: 10.1109/TSMC.2019.2899626.

[45] M. Huang et al., "A Game-Based Economic Model for Price Decision Making in Cyber-Physical-Social Systems," in IEEE Access, vol. 7, pp. 111559-111576, 2019, doi: 10.1109/ACCESS.2019.2934515.

[46] F. Kong, Y. Zhou, B. Xia, L. Pan, and L. Zhu, "A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment," in IEEE Access, vol. 7, pp. 161822-161830, 2019, doi 10.1109/ACCESS.2019.2950731.

[47] Z. Su and Q. Xu, "Security-Aware Resource Allocation for Mobile Social Big Data: A Matching-Coalitional Game Solution," in IEEE Transactions on Big Data, vol. 7, no. 4, pp. 632-642, 1 October 2021, doi: 10.1109/TBDATA.2017.2700318.

[48] J. Sun, H. Xiong, S. Zhang, X. Liu, J. Yuan, and R. H. Deng, "A Secure Flexible and Tampering-Resistant Data Sharing System for Vehicular Social Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 12938-12950, Nov. 2020, doi: 10.1109/TVT.2020.3015916.

[49] L. H. Álvarez, J. M. de Fuentes, L. G. Manzano, and L. H. Encinas, "Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review," MDPI-Sensor, vol.21, No.92, 2021. DOI: https://dx.doi.org/10.3390/s21010092.

[50] S. Jin, V. V. Phoha and R. Zafarani, "Graph-Based Identification and Authentication: A Stochastic Kronecker Approach," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 7, pp. 3282-3294, 1 July 2022, doi: 10.1109/TKDE.2020.3025989.

[51] L. Megouache, A. Zitouni, and M. Djoudi, "Ensuring user authentication and data integrity in the multi-cloud environment," Springer-Human-Centric Computing & Information Sciences, vol.10, No.15, 2020.DOI: https://doi.org/10.1186/s13673-020-00224-y.

[52] N-E Park, S-H Park, Y-S Oh, J-H Moon, and I-G Lee, "Distributed Authentication Model for Secure Network Connectivity in Network Separation Technology," MDPI-Sensors, vol.22, No.579, 2022. DOI:https://doi.org/10.3390/s22020579.

[53] O. Ruan, L. Zhang, and Y. Zhang, "Location-sharing protocol for privacy protection in mobile online social networks," EURASIP Journal on Wireless Communications and Networking, 2021.DOI: https://doi.org/10.1186/s13638-021-01999-z.

[54] V.K. Sinha, D. Anand, S. Kaur, P. Singh, and I. D. Noya, "Security Verification of Social Network Model Using Improved Three-Party Authenticated Key Exchange Protocol," MDPI-Symmetry, vol.14, No.1567, 2022. DOI: https://doi.org/10.3390/sym14081567.

[55] D. Soni, D. Srivastava, A. Bhatt, A. Aggarwal, S. Kumar, and M.A. Shah, "An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol," Hindawi-Mathematical Problems in Engineering, Volume 2022, Article ID 4696649, 14 pages, 2022.

[56] Z. Tu, H. Zhou, K. Li, H. Song, and Y. Yang, "A Blockchain-Enabled Trusted Protocol Based on Whole-Process User Behavior in 6G Network", Hindawi-Security and Communication Networks, Volume 2022, Article ID 8188977, 12 pages, 2022.

[57] D. Xu, W. Wang, L. Zhu, J. Zhao, F. Wu, and J. Gao, "CL-BC: A Secure Data Storage Model for Social Networks," Hindawi-Security and Communication Networks, Volume 2022, Article ID 5428539, 13 pages, 2022.

[58] X. Zuo, L. Li, H. Peng, S. Luo and Y. Yang, "Privacy-Preserving Subgraph Matching Scheme With Authentication in Social Networks," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 2038-2049, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.3012999.

[59] https://ieeexplore.ieee.org/search/searchresult.jsp?queryText=security,%20social%20network&highlight=true&returnFacets=ALL&returnType=SEARCH&matchPubs=true&ranges=2012_2023_Year.