

Security and privacy concerns in social networks mathematically modified metaheuristic-based approach

Raguru Jaya Krishna [†]

Department of Computer Science and Engineering

Manipal Institute of Technology Bengaluru

Manipal Academy of Higher Education

Manipal 560064

Karnataka

India

T. Gopalakrishnan ^{*}

Department of Information Technology

Manipal Institute of Technology Bengaluru

Manipal Academy of Higher Education

Manipal 560064

Karnataka

India

M. Divyapushpalakshmi [§]

Department of Computer Science and Engineering

GITAM University

Bengaluru 561203

Karnataka

India

K. Amarendra [‡]

Department of Computer Science and Engineering

Koneru Lakshmaiah Education Foundation

Vaddeswaram 522502

Andhra Pradesh

India

[†] E-mail: raguru.krishna@manipal.edu

^{*} E-mail: gopalakrishnan.ct@gmail.com (Corresponding Author)

[§] E-mail: drdivyanatchim@gmail.com

[‡] E-mail: amarendra@kluniversity.in

Pankaj Dadheech [@]

*Department of Computer Science and Engineering
Swami Keshvanand Institute of Technology,
Management & Gramothan (SKIT)
Jaipur 302017
Rajasthan
India*

Sudhakar Sengan [#]

*Department of Computer Science and Engineering
PSN College of Engineering and Technology
Tirunelveli 627152
Tamil Nadu
India*

Abstract

Potential risks and vulnerabilities in Social Networks (SN) that may threaten the confidentiality, accuracy, and accessibility of data provided by users have been identified as safety risks. Unauthorized usage of the system, breaches of data, privacy violations, cyber-attacks, and other malicious behaviors that negatively impact the SN's reliability and security may be addressed within these. Innovative techniques that use scientifically enhanced metaheuristic algorithms are the subject of the study, which attempts to address evolving issues of security and privacy in SNs. In order to improve the security of online social networking data encryption, researchers recommend implementing the MMCSSOA approach, which is the Mathematically Modified Cuckoo Search Optimization Algorithm. An enhanced tuning of elliptic curve parameters can be accomplished by adapting the Cuckoo Search method, which, in consequence, provides an encrypted environment for multi-party computing. Users' preferences for confidentiality are considered while applying a fuzzy logic (FL) decision matrix to select individuals. Data security is improved, and users receive additional authority over data shared with MMCSSOA. Research findings prove that MMCSSOA is higher compared to other methods in securing users' privacy.

Subject Classification: 68N30.

Keywords: Security, Optimization, Social network, Accuracy, Encryption, Privacy, Cuckoo search.

1. Introduction

Social media is a technology that facilitates the exchange of different thoughts, ideas, and information. Various communities and virtual

[@] E-mail: pankajdadheech777@gmail.com

[#] E-mail: sudhasengan@gmail.com

networks are channels for sending and receiving valuable particulars. Users' access to social media is made dependable through computers, mobile phones, and tablets [1]. While using Social Networks (SN) for communication among several communities, the exposure of private and personal information becoming public without the individual's consent is the core issue confronted by the end users [2]. Significant personal details can be exchanged between friends and family, and further confidential information related to the profession can be shared among suitable communities [3]. An individual's privacy is the most significant parameter associated with any SN system. However, this aspect is most challenged by a lack of data/information security. The privacy dispute in SN has become a pertinent, common social issue in the present era. This issue includes antisocial activities like stealing personal data, sharing malware, hacking accounts, and obtaining personal information by cybercriminals [4]. There are several ways to invade an individual's privacy, such as by disclosing private and confidential information to a third party without any authentication. Therefore, privacy protection is essential to prevent the access of personal information among multiple users. This helps reduce stress and relax personally by swapping interests and entertainment.

The behavioral patterns can be differentiated by classifying the posts, profiles, and images uploaded by them. Users overlooked privacy even though some menacing activities like embezzlement of information, identity theft, and stalking problems in social media did exist initially. The privacy of the client is paramount. Because of the negligence of privacy, several conflicts among the users occurred in the later stage. Privacy preservation was lacking in social media, such as blogs, wikis, networking sites, messaging applications, micro-blogs, sites for video sharing, and more. When a group of information is shared by an individual in the group, others can raise disputes since they want to keep the information private [5]. Privacy protection is needed significantly to prevent access to confidential information among multiple users. From the current state-of-the-art methods, secure multiparty computations can be established to protect the sensitive information exchanged between the users. As privacy conflicts and computational overhead cannot be controlled in managing privacy through a single party, many researchers prefer multiparty computation as no trusted third parties can access the data. Most MP management algorithms use secure multiparty computation, Homomorphic Encryption (HE), or k-means clustering. But all the above three had their disadvantages. Communication devices are needed to

bring participants together. This increases the deployment cost, which is the main disadvantage of secure multiparty computation.

One of the most significant drawbacks of HE is that it requires either application modifications/or dedicated client-server applications for it to work correctly. In addition, organizations cannot use their methodology to run ad-hoc/discovery-based queries. K-Means clustering algorithm has a disadvantage as it requires the specification of the number of clusters (k) in advance. It cannot handle noisy data and outliers. It is not suitable to identify clusters with non-convex shapes. Hence, in our proposal, we are not using these existing methods. The trade-off between data usability and privacy can be eliminated in order to preserve the data so that privacy conflicts can be minimized.

Individual data can be protected from several attacks from cyber theft hackers by implementing MP. Multiparty privacy management achieves high accuracy and precision when transacting quantum-safe data in social media [6]. Ensuring user privacy is of paramount significance in modern multimedia social networks. Conventional anomaly detection techniques that exclusively depend on user log files and behavioral patterns are inadequate in delivering comprehensive privacy protection. To address this constraint, it is crucial to implement an improved security framework for SNs that integrates various security methods and uses supplementary user profile data. This study presents a privacy preservation approach that combines supervised and unsupervised machine learning anomaly detection methods with access control models. The extended attribute-based access control model enhances the detection model by adjusting authorization rights according to individual user threat evaluations. The algorithm promotes user consciousness within interconnected groups of users. The simulation results demonstrate the comparative performance of Bayesian, Deep Neural Network (DNN) [7], and Long Short-Term Memory (LSTM)- Recurrent Neural Network (LSTM-RNN) [8] anomaly detection techniques concerning other systems such as Kolmogorov–Smirnov test (KSE) [9], Support Vector Machine (SVM) [10], Principal Component Analysis (PCA) [11], and isolation forests [12]. The results illustrate the algorithm's effectiveness in fulfilling privacy criteria by maintaining user anonymity and availability within the online SN. The incidence of privacy problems on social media is increasing daily, and more problems occur in multiparty privacy [13-15]. As the privacy of every individual is essential, many researchers suggest several techniques for upgrading privacy management. Several tools, strategies, and methods are initiated to maintain the privacy needs of every user. Even though

many facilities are available to manage multi-party privacy, many conflicts arise between users. The paper is organized as follows: the literature reviewed is presented in Section 1, the problem is defined in Section 2, Section 3 presents the system model, Section 4 presents the experiment analysis, and Section 6 concludes the work.

2. Proposed Modified Elliptic Curve Cryptography Using Cuckoo Search Optimization Algorithm (MECCSOA) Methodology

MECC is known as the Asymmetric Cryptography Method (ACM), including Private Key (PrK) and Public Keys (PuK). A public channel is kept by the Public Key (PuK), a sharing key. The user uses PrK, and it is a secret key. Consider two users, X and Y ; their PrKs are X_{pr} and Y_{pr} . The public keys of these users are X_{pu} and Y_{pu} . The key generation point k_p is agreed upon by users, and a standard elliptical curve is $b^2 = a^3 + xa + y$. Users select PrK randomly, and EQU (1) and EQU (2) are used to calculate PuK.

$$X_{pu} = k_p \times X_{pr} \quad (1)$$

$$Y_{pu} = k_p \times Y_{pr} \quad (2)$$

Applying an inaccurate PrK may trigger PuK evaluation to result in infinite results. To deal with these problems, researchers invented the Cuckoo Search Optimization Algorithm (CSOA) to select PrK properly before attempting to generate PuKkeys that are possible to implement. In order to enhance the solutions to challenges with optimization, the CSOA presents an innovative meta-heuristic approach. Cuckoo birds, which are renowned for putting their eggs within different birds' nesting sites, are the most significant behavioral impacts of this approach. This algorithm functions based on three essential laws: firstly, a cuckoo places a single egg in the host nest and selects a nest randomly at detailed breaks; secondly, nests with higher egg quality are chosen for the next group; and thirdly, the host bird harvests eggs with a likelihood signified by $P \in [0,1]$, where 1 implies success and 0 specifies error in Algorithm 1. There is a significant relationship between the total number of nests and the availability of adequate security.

Algorithm 1. MECCSOA

- Step 1. Function Fuzzy_TOPSIS(Attributes, Alternatives)
- Step 2. Fuzzy_Decision_Matrix = Generate_Fuzzy_Decision_Matrix(Attributes, Alternatives)
- Step 3. Normalized_Decision_Matrix = Normalize (Fuzzy_Decision_Matrix)
- Step 4. Weighted_Normalized_Fuzzy_Decision_Matrix = Weighted_Normalize (Normalized_Decision_Matrix)
- Step 5. FPIS, FNIS, Separation_Measures=Compute_Measures (Weighted_Normalized_Fuzzy_Decision_Matrix)
- Step 6. Rank_Index = Calculate_RankIndex (Separation_Measures)
- Step 7. Ranked_Alternatives = Rank_Alternatives (Rank_Index)
- Step 8. Return Ranked_Alternatives
- Step 9. Function Participant_Selection (Ranked_Alternatives):
- Step 10. Selected_Participants = Select_Participants (Ranked_Alternatives)
- Step 11. Return Selected_Participants
- Step 12. Function MECCSOA (Data_To_Encrypt, Set_of_PrK):
- Step 13. Encrypted_Data = Encrypt_Data (Data_To_Encrypt)
- Step 14. Optimal_PrK = Select_Optimal_PrK (Set_of_PrK)
- Step 15. Authentication Result = Authenticate (Encrypted_Data, Optimal_PrK)
- Step 16. Decrypted_Data = Decrypt_Data (Encrypted_Data, Optimal_PrK)
- Step 17. Return Encrypted_Data, Authentication_Result, Decrypted_Data

This method establishes the authorization of participants to access data and resources. At first, users X and Y collaboratively select the parameters for an elliptic curve. User X chooses k_p and then sends it to user Y . The CSOA is subsequently applied to autonomously determine a unique PrK for each user. The PrK are kept confidential and not revealed. They are employed to calculate the PuK of the corresponding users. The definitive verification points are determined using EQU (3) and EQU (4).

$$V_{px} = X_{pr} \times Y_{pu} \quad (3)$$

$$V_{py} = X_{pr} \times Y_{pu} \quad (4)$$

Here, the final verification points of users X and Y are represented as V_{px} and V_{py} . The shared secret key method is implemented as EQU (5) to EQU (7) and its derivation.

$$V_{px} = X_{pr} \times Y_{pu} \quad (5)$$

$$= X_{pr} \times Y_{pu} \quad (6)$$

$$= V_{py} \quad (7)$$

In the CSOA method, the optimal selection of a random number $\mathfrak{R}$ is crucial. Before the encryption process, both users must collaboratively determine the parameters of the elliptic curve and perform a numeric translation of the text using ASCII values. The users are responsible for selecting the encryption process's key generation point and elliptic curve parameters. PrK selection is conducted by both users using the CSOA algorithm. PuK are derived from the PuK and the PrK generation points. Subsequently, these PuK are exchanged between users. User X encrypts data using the PuK of user Y , and vice versa. User X commences the encryption process by adhering to a sequence of steps. Initially, the text messages meant to be transmitted are obtained and transformed into their respective ASCII numeric representation. The random number $\mathfrak{R}$, essential for the encryption process, is carefully selected using the CSOA. The encryption process involves performing point addition and point multiplication operations, which yield the computation of the cipher text. Finally, the cipher text produced is sent to user Y to provide secure communication using EQU (8) to EQU (10).

$$\zeta_1 = k_p \times R \quad (8)$$

$$\zeta_2 = Y_{pu} \times R \quad (9)$$

$$\zeta_3 = k_2 \times P_m \quad (10)$$

Here, the cipher parts are $\zeta_1, \zeta_2, \zeta_3$ and message point is P_m . The cipher text is evaluated by EQU (11).

$$\zeta = \{\zeta_1, \zeta_3\} \quad (11)$$

Separate ζ_1 and ζ_3 from the cipher text. Multiply ζ_1 with Y_{pr} and then subtract from ζ_3 then get P_m , EQU (12)

$$P_m = \zeta_3 - \zeta_1 \times Y_{pr} \quad (12)$$

The encryption procedure commences by transforming the message points into ASCII numbers and associating them with their corresponding textual attributes. The private data and keys have been shared with selected users after completing the data encryption mechanism and key selection. Users' privacy is secured, and system transfer, reception, and storage can be done privately with this approach. The use of encryption is the procedure of converting plaintext into an unreadable code that can only be decoded by the person who intended it. When it comes to securing confidential information, cryptography is vital for maintaining user data secure and undeleted.

3. Result and Discussion

The JAVA technology is employed by the model that has been suggested, which was developed on a Windows 11 setup with 16 GB RAM. The review of multiparty privacy control is performed by employing MySQL as the database of records and JSP as the front-end application. An Apache webserver introduces the Java file encoding the programming code into an open-source blogging website. JSP stores this source code. The current setup is more significant compared to others because it stores enormous volumes of data efficiently, which prevents incorrect procedures from being implemented. It is simpler to evaluate an approach when a graphical representation is employed. Two primary factors, A3P-core and A3P-social, utilize metadata and content data for the classification of images Table 1.

Secure Multiparty Computation (SMPC) also serves to evaluate the method's performance under the limitations of the cost. In contrast with competing methods, the system has been demonstrated to be more successful. Time for implementation, accuracy, and integrity in terms of security were the parameters used for evaluating the recommended system's efficiency.

- A. *Execution Time*: The total amount of time that it requires for an entire system or a particular procedure within a system to complete a

task or a collection of functions is referred to as the time needed for execution Figure 1 (a).

$$\text{Execution Time} = \text{End Time} - \text{Start Time}$$

(13)

The two, the Starting Time and the End Time, are date and time stamps that correspondingly indicate the start and end of the task.

B. *Accuracy*: It signifies how well the system’s findings match up with actual data or user assumptions; this encompasses factors like image classification and secure environment design Figure 1(b).

$$\text{Policy Accuracy} = \frac{\text{Number of Correctly Generated Policies}}{\text{Total Number of Policies Generated}} \times 100$$

(14)

Table 1
Comparison of Performance

Algorithm	Execution Time (hrs)	Accuracy (%)	Encryption Time (ms)	Decryption Time (ms)
DNN	0.14	89	34534	42812
LSTM-RMM	0.12	91	31453	46712
MMCSOA	0.1	95	25332	49123

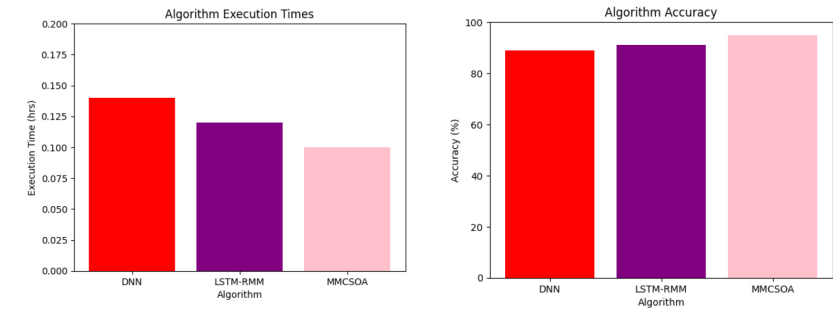


Figure 1 (a). Execution Time

Figure 1 (b). Accuracy

Figure 1

Comparison of Execution Time and Accuracy

The Comparison of Encryption and Decryption Time is shown in Figure 2. By examining the results they produce, the three methods, LSTM-RMM, MMCSOA, and Deep Neural Network (DNN), are distinguished. MMCSOA distinguishes out primarily because of its highly

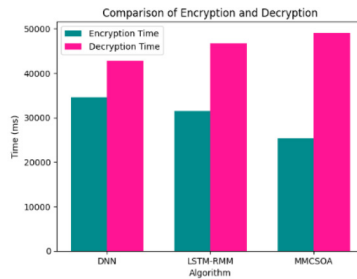


Figure 2

Comparison of Encryption and Decryption Time

effective encryption as well as decryption processes, which take 25332 *ms* and 49123 *ms*, respectively, and its relatively minimal execution time of 0.1 hours. In addition to this, it exhibits the maximum feasible level of accuracy, which is 95%. Because of its unique features, MMCSOA is an effective option for tasks requiring speed as well as precision. After this, LSTM-RMM demonstrates superior efficiency with an accuracy score of 91%. The DNN indicates significant execution and decryption periods, which could be enhanced, even though it reaches an accuracy score of 89%. The results of this study underline the value of modifying algorithmic trade-off analyses for particular application demands, with MMCSOA offering possibilities in cases requiring accurate as well as effective computing.

4. Conclusion and Future Work

The fundamental need of online social networking users for the avoidance of private information and an enhancement of a high level of security is multi-party privacy. In order to ensure complete data security, conventional methods for identifying anomalies that rely upon user data logs and behavioral patterns are inappropriate. Applying mathematically enhanced metaheuristic methods, this research investigation proposes an original method for dealing with these problems. Data encryption robustness in social networking sites is being targeted by introducing the Mathematically Modified Cuckoo Search Optimization Algorithm (MMCSOA). The method-based optimizes elliptic curve variables by updating the CSOA, which generates a secure multiparty computing system. The selection of users additionally employs the use of a fuzzy logic decision matrix that considers confidentiality preferences into

account. Studies illustrate that MMCSOA is preferable compared to various privacy-preserving approaches and contributes to improved data security by offering users more control over their publicly available data. Algorithms for machine learning (ML) have been shown to strengthen MP management further on social media platforms on the Internet. Implementing hybrid optimization methods may be practical to lower the computational time as well as costs. The development and design of techniques that can be employed by a smartphone application for instantly identifying images being shared is also feasible from a technical standpoint. Adopting precise privacy controls can be highly successful when it comes to sharing data. Integrating MP with Deep Learning (DL) approaches can be accomplished to identify fraudulent data. To address image security issues, image extraction techniques such as steganography can be deployed.

References

- [1] A. C. Hsu and I. Ray, Specification and enforcement of location-aware attribute-based access control for online social networks, *Proceedings of ACM International Workshop on Attribute Based Access Control-ABAC*, vol. 16, New Orleans, LA, USA (2016).
- [2] A.C. Enache and V. Sgârciu, Enhanced intrusion detection system based on bat algorithm-support vector machine, *Proceedings of the 11th International Conference on Security and Cryptography*, Vienna, Austria (2014).
- [3] M. Shehab et al., Access control for online social networks third-party applications, *Computers & Security*, vol. 31, no. 8, pp. 897–911 (2012).
- [4] B. Al-Otaibi et al., Privacy-preserving vehicular rogue node detection scheme for fog computing, *Sensors*, vol. 19, no. 4, p. 965 (2019).
- [5] H. Rong et al., Deep rolling: a novel emotion prediction model for a multi-participant communication context," *Information Sciences*, vol. 488, pp. 158–180 (2019).
- [6] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.

- [7] W. Stallings, et al., "Authentication, Access Control, and Intrusion Detection, *Computer Science Handbook*, CRC Press, Boca Raton, FL, USA, 2nd Edition (2004).
- [8] M. H. Bhuyan et al., Network traffic anomaly detection techniques and systems, *Computer Communications And Networks Network Traffic Anomaly Detection And Prevention*, Springer, Berlin, Germany (2017).
- [9] S. K. Sharma, A. Chaurasia, V. S. Sharma, C. L. Chowdhary and S. Basheer, "GEMM, a Genetic Engineering-Based Mutual Model for Resource Allocation of Grid Computing," in *IEEE Access*, vol. 11, pp. 128537-128548 (2023), doi: 10.1109/ACCESS.2023.3333278.
- [10] D. M. D. Reis et al., Fast unsupervised online drift detection using incremental Kolmogorov-Smirnov test, in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco, CA, USA (2016).
- [11] T. Ko et al., "Machine learning-based anomaly detection via integration of manufacturing, inspection, and after-sales service data," *Industrial Management & Data Systems*, vol. 117, no. 5, pp. 927-945 (2017).
- [12] C.P. Tran and D. K. Tran, Anomaly detection in POSTFIX mail log using principal component analysis, 10th International Conference On Knowledge And Systems Engineering, Ho Chi Minh City, Vietnam (2018).
- [13] M. Ye et al., A Novel Self-Supervised Learning-Based Anomalous Node Detection Method Based on an Autoencoder for Wireless Sensor Networks, *IEEE Systems Journal*, doi: 10.1109/JSYST.2023.3347435.
- [14] Y. Li et al., Enhancing Network Intrusion Detection through the Application of the Dung Beetle Optimized Fusion Model, *IEEE Access*, doi: 10.1109/ACCESS.2024.3353488.
- [15] Z. Hu et al., Enhancing Detection of Malicious Traffic Through FPGA-Based Frequency Transformation and Machine Learning, *IEEE Access*, vol. 12, pp. 2648-2659 (2024), doi: 10.1109/ACCESS.2023.3348234.