IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 2, February 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302031 |

Enhance User Privacy by Relationship Verification through Data Sharing on Social Network

S.Sadhana, R.Jeeva Bhaviya, K.Sowmiya, S.Vivetha

Assistant Professor, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

Student, Department of Cyber Security, Muthayammal Engineering College, Rasipuram, India

ABSTRACT: To provide a collaborative approach for efficient data sharing in OSN. To make threshold based on which the user makes the final decision on data posting. A high threshold indicates that the user has a relatively low tendency to share the data with others, and only when the majority of the involved users or users that are highly trusted agree to post the data, the data can finally be posted. By tuning the threshold, the user can make a trade-off between data sharing and privacy preserving.

To provide automatic comment analysis and comment blocking approach for secure image sharing. Traditional platforms often grapple with issues of fake profiles, identity theft, and inadequate user authentication mechanisms, prompting the exploration of innovative frameworks. Our study delves into the theoretical underpinnings and feasibility of employing encrypted, voluntary data sharing to authenticate user connections, enhancing network authenticity. It critically examines ethical implications, emphasizing user consent, transparency, and the imperative need for robust security measures.

I. INTRODUCTION

Enhancing user privacy through relationship verification via data sharing on social networks is an innovative approach aimed at bolstering the security and confidentiality of user interactions. In today's digital landscape, where online interactions play a pivotal role in our lives, ensuring trust and privacy within social networks is paramount. Traditional social networking platforms often face challenges in validating the authenticity of connections, leading to concerns about fake profiles, fraudulent activities, and compromised user privacy. By implementing relationship verification mechanisms that involve secure data sharing, these platforms can establish a more reliable network where users can interact with greater confidence and trust.

The concept revolves around a framework where users voluntarily share specific data points or verification credentials with the platform to verify their relationships with other users. This data sharing could encompass mutually agreed-upon information, such as shared experiences, geographical proximity, common affiliations, or even cryptographic proofs, all encrypted and secured to protect user privacy. Moreover, this approach prioritizes user consent and transparency. Users have control over the data they share and with whom they share it, ensuring that their privacy remains protected while enabling a more secure and authentic social networking experience.

By employing relationship verification through data sharing, social networks can mitigate risks associated with impersonation, fake accounts, and unauthorized access. This not only fosters a safer online environment but also cultivates a sense of trust among users, encouraging more genuine and meaningful connections.

II. SYSTEM ANALYSIS

The system analysis for enhancing user privacy via relationship verification through data sharing on social networks involves a multifaceted examination of the existing social networking infrastructure and its associated challenges. It entails a thorough evaluation of the current mechanisms employed for user authentication and relationship verification within these platforms, highlighting vulnerabilities such as fraudulent accounts, data breaches, and privacy infringements. This analysis emphasizes the need for a more robust system that ensures the authenticity of user connections while safeguarding individual privacy. It involves the exploration of potential frameworks or methodologies that enable secure data sharing among users to validate relationships, considering factors like encryption techniques, data storage, transmission security, and user consent protocols.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302031 |

Moreover, ethical considerations regarding the collection, storage, and utilization of shared data are integral to this analysis, focusing on ensuring transparency, user control over their information, and compliance with privacy regulations. Additionally, the evaluation encompasses the technical feasibility, scalability, and potential integration challenges of implementing such a system within the existing social network infrastructure, aiming to strike a balance between improved security, user trust, and preserving individual privacy rights.

III. EXISTING SYSTEM

In existing system implemented SentiTrust, whose main component estimates trust through people's direct social interactions. SentiTrust leverages the power of AI and sentimental analysis to achieve a more in-depth understanding of how a person responds to social interactions.Three features, namely Sentiment Analysis, Profile Similarity and Common Friends, each trying to capture a distinct aspect of the relationship among people. Some platforms have introduced features such as two-factor authentication, identity verification for public figures or businesses, and content moderation algorithms to enhance security and weed out fake accounts. However, these measures may not directly address the need for relationship verification through data sharing in a comprehensive manner. Therefore, the existing system primarily relies on user-controlled privacy settings and some rudimentary authentication methods, but it might lack sophisticated mechanisms for secure relationship verification through data sharing to ensure authenticity and protect user privacy within social networks. Innovations in this space are ongoing, and new systems or features might have emerged after my last update that address these concerns more effectively. These platforms typically offer basic tools for users to manage their privacy settings, control who can view their information, and report suspicious accounts.

Limitations:

The trust model of a OSN is more complex due to the decentralized nature of the network. This makes privacy, information gathering, and computational power usage more complex. The assignment of a score becomes challenging because users most likely do not want to share their trust information with other peers.

Detecting malicious nodes that are likely to deceive in the future is also an aspect to take into account. One primary limitation of enhancing user privacy through relationship verification via data sharing on social networks lies in the potential trade-off between privacy and the necessity of sharing personal data for verification purposes. While the concept aims to authenticate connections and bolster security, there's a risk of users feeling reluctant or apprehensive about sharing sensitive information due to privacy concerns. Balancing the need for verification with user trust and comfort levels regarding data sharing poses a significant challenge. Moreover, ensuring the security of shared data against breaches or misuse, as well as addressing ethical considerations regarding consent and transparency, adds complexity to the implementation of such a system within social network environments. Finding a harmonious equilibrium between verification efficacy and preserving user privacy remains a critical hurdle in this approach.

IV. PROPOSED SYSTEM

A trust-based mechanism is proposed for collaborative privacy management in OSNs. Generate a relationship based group, for verifying the shared information.

The trust values between users are associated with users' privacy loss. Proposed relationship graph with opinion collection to help the user make a tradeoff between data sharing and privacy preserving. The UCB (Upper Confidence Bound) policy was proposed to determine whether the threshold get satisfied or not. Then provide comment analysis for filtering unwanted comments without user knowledge. The proposed system for enhancing user privacy through relationship verification via data sharing on social networks involves a sophisticated framework leveraging advanced encryption techniques and selective data sharing protocols. It aims to provide users with the option to securely share specific, encrypted data points with connections to verify relationships without compromising their overall privacy. This system prioritizes user consent and control, allowing individuals to manage and authenticate connections while maintaining a high level of data confidentiality. Additionally, the proposed system focuses on implementing transparent and user-friendly mechanisms for data sharing, ensuring that the verification process enhances trust without infringing upon user privacy rights.

Expected Merits:

The expected merits of enhancing user privacy through relationship verification via data sharing on social networks encompass a fortified layer of trust and authenticity within the platform. By implementing this approach, users can expect heightened security through verified connections, reducing the prevalence of fake profiles and enhancing the overall credibility of interactions. Moreover, this system is anticipated to empower users by providing greater control over shared data, fostering transparency, and allowing individuals to verify connections while

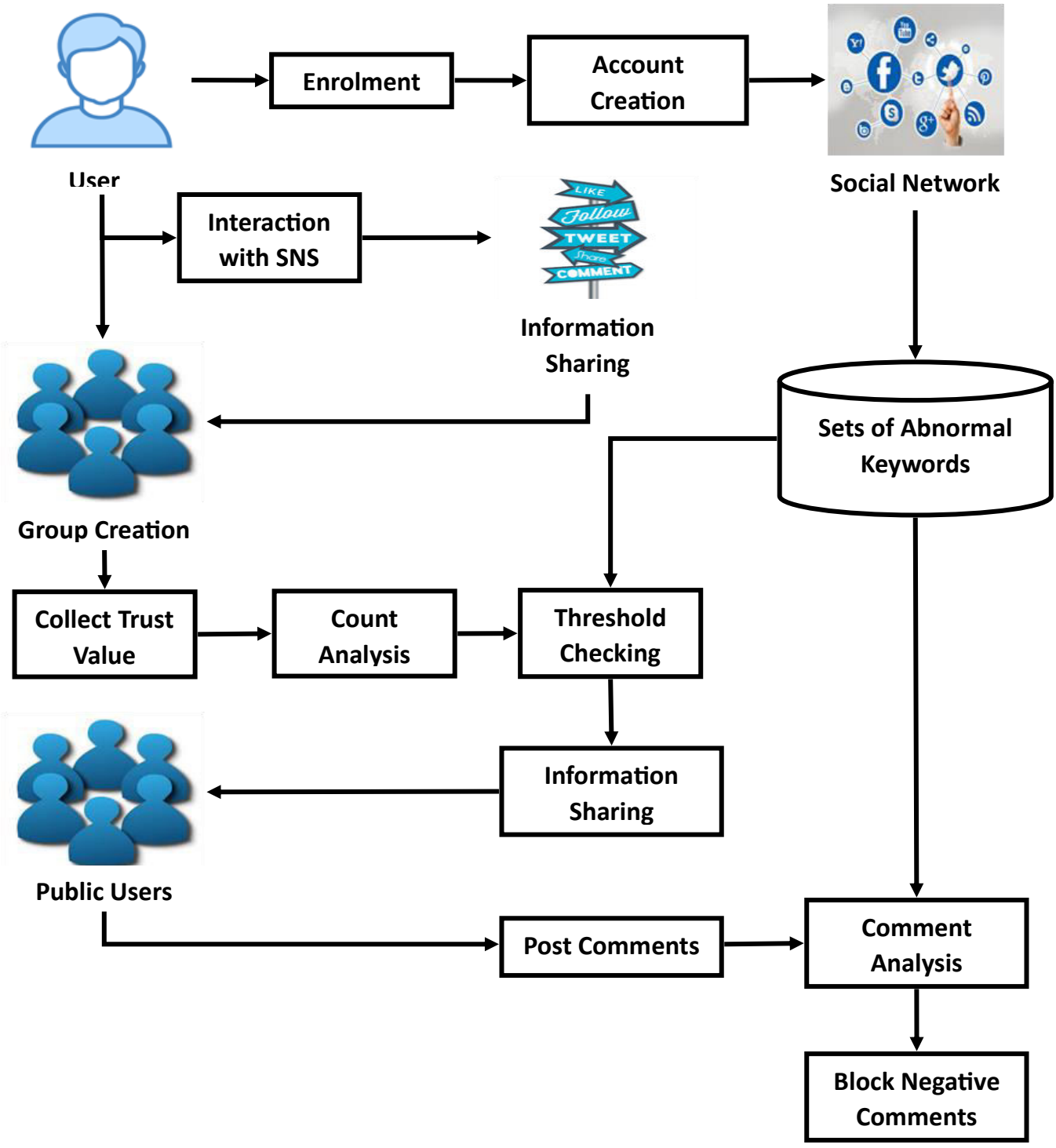
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302031 |

preserving their privacy. Ultimately, this framework is poised to cultivate a safer, more genuine social networking environment where users can engage confidently, knowing that their connections are authenticated without compromising their sensitive personal information.

System Architecture :



|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302031 |

V. SOFTWARE DESCRIPTION

OSN FRAMEWORK:

Social network refers to interaction among people in which they create, share, and/or exchange information and ideas in virtual communities and networks. In face book, GUI is a type of user interface thatallows users to interact with others through graphical icons and text-based interfaces, typed command labels or text navigation. In this module, we can have three types of users such as content owner, users and server. Content owner can be upload the information into system and server stores the information in database. Image users use images which are shared by image owner.

Information Sharing :

To post a data item the privacy policy specified by the user, every involved user makes a "vote" to state whether approves of the privacy policy. The importance of the vote depends on the trust value between the two users. Only when the aggregation of the votes satisfies a certain condition, the data can be posted.

Moreover, the trust values between users are not fixed. The interaction between the trust value and the privacy loss implies that if the user wants to reduce his/her privacy loss, then when posting a data item. The user should always consider others' privacy requirements rather than taking a unilateral decision.

Trust Value Estimation :

Trust-based privacy management mechanism, introduce a threshold based on which the user makes the final decision on data posting. Only when the majority of the involved users or users that are highly trusted agree to post the data, the data can finally be posted. The threshold selecting provides a sequential decision-making problem. Formulate the problem and apply the upper confidence bound (UCB) policy to solve the problem. Dynamically adjusting the threshold according to the UCB policy can lead to a higher payoff than using a fixed threshold.

Comment Analysis :

Comment analysis refers to the use of natural language processing, text analysis, computational linguistics to systematically identify, extract, quantify, and study affective states and subjective information. Comment analysis is widely applied to predict the opinion of such as reviews and ratings for applications. Apply text mining approach to tokenize and detect the keyword in given comment. System can analyze whether the comment is positive or negative.

Filter Approach :

The filtering rules should allow users to state constraints on message creators. This means filtering rules identifying messages according to constraints on their contents. To improve flexibility, this information is in the system by a set of rules.

Rules are generated by server for setting threshold values. Block the users who are post the negative comments more than five times and also send mobile intimation to users at the time offline.

VI. CONCLUSION

The expected outcomes of implementing relationship verification through data sharing to enhance user privacy on social networks encompass a transformative shift towards a more secure, authentic, and privacy-respecting online environment. By fostering a system that enables users to verify connections through encrypted data sharing, one of the primary expectations is a significant reduction in the prevalence of fake profiles and impersonation, thereby bolstering the credibility and trustworthiness of social networking interactions.

This approach is anticipated to empower users with greater control over their shared information, instilling confidence in their online relationships while safeguarding their privacy. Furthermore, by enhancing authenticity and trust among users, the platform can potentially see increased user engagement, fostering more meaningful interactions and a strengthened sense of community.

A successful implementation would also lead to a paradigm shift in how social networks approach user privacy, setting a precedent for more transparent, consent-driven data-sharing practices while respecting stringent data protection regulations. Ultimately, the expected outcome is to establish a precedent for a safer, more trustworthy social networking ecosystem where users feel more confident in their interactions while having control over their personal data.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302031 |

REFERENCES

[1] Greco, Alberto, Gaetano Valenza, Jesus Lazaro, Jorge Mario Garzon-Rey, Jordi Aguilo, Concepcion De-la-Camara, Raquel Bailon, and Enzo Pasquale Scilingo. "Acute stress state classification based on electrodermal activity modeling." IEEE Transactions on Affective Computing (2021).
[2] Marín-Morales, Javier, Carmen Llinares, Jaime Guixeres, and Mariano Alcañiz. "Emotion recognition in immersive virtual reality: From statistics to affective computing." Sensors 20, no. 18 (2020): 5163.
[3] Boutet, Isabelle, Megan LeBlanc, Justin A. Chamberland, and Charles A. Collin. "Emojis influence emotional communication, social attributions, and information processing." Computers in Human Behavior 119 (2021): 106722.
[4] Guidi, Barbara, Kristina G. Kapanova, Kevin Koidl, Andrea Michienzi, and Laura Ricci. "The contextual ego network p2p overlay for the next generation social networks." Mobile Networks and Applications 25 (2020): 1062-1074.
[5] Guidi, Barbara, Andrea Michienzi, and Laura Ricci. "Steem blockchain: Mining the inner structure of the graph." IEEE Access 8 (2020): 210251-210266.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details