International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I7P202

Volume 71 Issue 7, 15-27, July 2023

Original Article

A Bi-Fold Trust Model for Cooperative Privacy and Security Management in Online Social Media

A. Satish Kumar[1], S. Revathy[2]

[1]*School of Computing, Sathyabama Institute of Science and Technology, Chennai, India*
[2]*Department of IT, Sathyabama Institute of Science and Technology, Chennai, India*

[1]*Corresponding Author : satishathmakuri@gmail.com*

Received: 20 April 2023 Revised: 17 June 2023 Accepted: 21 June 2023 Published: 21 July 2023

Abstract *- The most significant platforms for people to engage with others are now Online Social Networks (OSNs) such as Facebook, Google, and Twitter. Text messages, videos, and photos describing users' daily lives are posted by tens of thousands to millions of people on OSNs. Sensitive information about users is frequently discovered in such data. If unauthorised parties can access data, the user's privacy is at risk. The trust-based mechanism's threshold in this study is established at a value that guarantees the user receives a significant long-turn return. This value is calculated by the difference between the benefit of uploading data and users' privacy risks. To address the lack of trust and lack of collaboration that is comparable to peer-to-peer systems. By adjusting the proposed mechanism's parameter, users can choose between sharing data and protecting their privacy. In this paper, Thompson Sampling (TS) Algorithm is used to solve the Multi-armed Bandit (MAB) problem formulation of the parameter selection problem. The weighting of user opinions is determined by their trust values, upgraded as privacy is violated. In this research work, the trust score of the users is computed via a new bifold trust model. The publisher must thus change the threshold to strike a balance between privacy protection and document sharing, and trust-based integration of trust values into the document anonymisation process may help to minimise the loss of user privacy. Simulations demonstrate that a trust-based approach ensures user trust by protecting privacy and minimising information loss in the system, intended to be implemented in the PYTHON working environment.*

Keywords *- Online social networks, Thompson Sampling (TS) Algorithm, Multi-Armed Bandit (MAB), Bifold trust model.*

1. Introduction

Social media makes people communicate with one another by creating and sharing data and has recently become a common platform for sharing information with others. Social media users create text posts, digital photos, or videos of large amounts of information. While comparing textual data and photos, the photo may give detailed data to the observer, which is harmful to the user's privacy. The privacy problem in online social networks (OSN) by photo sharing is how user data is researched by the service provider [1] [2]. Researchers have offered a variety of solutions to the conflict between users' access control rules [3] [4]. A mediator will present a list of people permitted access to the data to implement an aggregated policy [5].

It is recommended that cooperative privacy management in OSNs use a trust-based method. The suggested approach requires the user to ask for other users' opinions before disclosing a data item to others. The publisher is recommended to make decisions using a trust-based strategy. The simulation's results demonstrate how the trust-based photo-sharing system minimises privacy loss. A user's willingness to allow another user to view his details typically hinges on how much of that user's faith is still intact. The recommended method establishes a threshold to control the number of users excluded from the image. Whether or whether a user's privacy is protected depends on how trustworthy other users are. This article offered a method for adjusting the threshold to the trust connections between users to strike a balance between preserving user privacy and sharing photographs. A trust-based technique of exchanging photographs in OSNs has been proposed [6] [7].

The degree of user trust is taken into account when determining whether a user's privacy will be respected. (Kumar & Revathy, 2021) The recommended approach can protect the user from disregarding the privacy of other users since trust values alter in reaction to privacy loss. By altering the threshold determining the number of users excluded from images, this study provided a method to balance photo sharing with privacy protection [8] [9]. In order to demonstrate the efficacy of the offered methodologies, this research has run a number of simulations.

The specifics of data are secured in social networking [10] [11]. Multiparty resources contain personal information about users, such as images taken using them. Users of services can communicate with their contacts and other people. Due to these preferences, policy conflicts will arise, making access control difficult to implement [12].

OSNs provide a basic degree of security for dealing with the multiparty access control issue [13] [14]. This study created a control model to enable parties to agree on access regulations through a straightforward dispute resolution process. The existing OSNs offer a minimal level of protection as a solution to the multiparty access control challenges [15]. The strategy relies on trust between partners and requesters to make access choices. A multiparty control paradigm built on trust was created for Facebook through this procedure. This work broadens the system by raising the total number of policy specifications, which gives users more precise control over resources shared by several parties.

The contribution of this research work is:

- To solve the multi-armed bandit (MAB) problem happening during data transmission in online social networks via the newly proposed Thompson Sampling (TS) Algorithm.

- To enhance the privacy preservation of documents, a new bifold trust model is introduced, including direct and indirect trust.

This paper is structured as follows: Section II deals with the findings and an analysis of related existing work of the presented model. Section III gives the proposed methodology of the work. The work is experimented with and analysed. Section IV deals with the result analysis and the comparative discussion of the work. Finally, Section V gives the conclusion of the work.

2. Related Works

In 2020, Urena R. *et al.* [16] proposed the decitrustnet concept for trust and reputation in social networks based on graphs. This contribution intends to build decitrustnet, a trust and reputation-based framework for social networks that take user connections, reputation history, and profile similarities into account in order to build a tamper-resistant network that ensures trustworthy communications and transactions. This experiment does not use multi-granular language data or the context-aware customisation of the suggested system.

In 2021, Yang G. *et al.* [17] proposed that the decitrustnet idea is built on graphs and addresses trust and reputation in social networks. In order to create a tamper-resistant network that provides trustworthy communications and transactions, this contribution aims to develop decitrustnet, a trust and reputation-based framework for social networks that consider user connections, reputation history, and profile similarities. This experiment does not make use of context-aware customisation of the proposed system or multi-granular linguistic data.

In 2018, He, Y. *et al.* [18] suggested a deep reinforcement learning method for computing, caching, and communications in trust-based social networks. In order to enable users to share resources within the 3C framework, this research takes advantage of the intrinsic characteristics of social networks, including the trust built via social interactions among users. This research focuses on device-to-device (D2D) interactions, in-network caching, and mobile edge computing (MEC). This study does not sufficiently explore the proposed integrated framework to address an energy-efficient resource allocation strategy.

In 2018, Wei W. *et al.* [19] described Using attribute-based encryption techniques, fractal intelligent privacy protection is provided in OSN. In order to address security and privacy concerns in OSNs, this study offers an intelligent privacy protection approach. Support vector machines were utilised to preprocess the OSN data before applying the attribute-based encryption method to encrypt it. Finally, a particle swarm optimisation technique was used to increase OSN security and privacy protection. This paper overlooked the topological similarity attack in OSN.

In 2019, Ahmed, A.I.A., *et al.* [20] examined basics, taxonomy, and open research difficulties for the Internet of Things' reputation and trust. Some IoT entities may be physically seized by attackers because of the potential for uncontrolled and unsupervised deployment. This paper presented a thematic taxonomy for trust in the Internet of Things. It considers a number of issues, including the duties of trust entities, their attributes, their applications, their levels of trust management, their metrics, their trust calculation algorithms, and their vulnerability to TR assaults.

In 2021, Wang F. *et al.* [21] have suggested increasing your impact on social networks that are competitive. First, a brand-new competitive influence diffusion model based on trust replicating the spread of positive and negative influence was created. Second, generalised network flows were employed to calculate influence probabilities after estimating trust levels. Finally, an effective method for trust-based competitive influence maximisation was developed utilising a heuristic pruning technique. This work does not optimise the competitive effect on large-scale datasets.

In 2018, He, Y. *et al.* [22] presented mobile edge computing, caching, and device-to-device communication, secure social networks may be accessed in 5g systems. This article in this paper introduces a social trust model that enhances the security of MSNs. Utilising Google TensorFlow, the suggested deep reinforcement learning method was put into practise. Using simulation results with different network

characteristics, the effectiveness of the recommended technique was proved.

In 2021, Mohammadi V. *et al.* [23] examined a buddy selection algorithm for the social Internet of Things that is based on trust. A general reference model and optimisation decision theory were developed for the best buddy selection to conserve resources. This created a network with good connectivity by decreasing the average distance and increasing the number of links. Users also benefited from scale-free degree distribution, which showed the presence of hubs or high-degree nodes.

In 2017, Cui L. *et al.* [24] suggested investigating a recommendation system for OSN movies based on trust. This article focused on the issue that the present video recommendation techniques for videos on OSN are not addressing the users' demands. In this study, a user discovery model and a video discovery model were combined as part of a novel trust-based video recommendation technique. A sophisticated mathematical model for a theoretical examination of the performance was not presented in the study.

In 2021, Liu, Z.J. *et al.* [25] recommended the benefits of mobile social networking and trust management: A method for assurance and security. This study claimed that issues with trust management in global crowdsourcing initiatives are caused by the enormous volumes of questionable data. This research argued that intuitively-based techniques for data verification should be used with functional algorithms for news filtering. It was anticipated that the suggested method would decrease the number of variables influencing the accuracy of crowdsourced data analysis.

3. Problem Methodology and System Design

3.1. Problem Statement

Social networking plays a significant role on the internet, transforming interpersonal connections into channels for information to flow. This implies that human decisions influence the way information travels online to a great extent. Information security, therefore, depends on the caliber of the users' collective judgments. Recently, several control systems have been put out to limit the spread of information in online social networks without authorisation; nevertheless, procedures are still required to assess the danger of information leakage inside social networks. The popularity of sharing information and images in online social networks as a way to keep in touch with friends has increased as social media technology has developed. However, a malevolent observer may find it simpler to infer private information about persons who appear in a collection containing photographs due to the wealth of information included in it. Recently, there has been a lot of focus on the concern of privacy revelation brought on by the sharing of data with photographs. Publishers of the data with photos should consider all linked users' privacy while distributing data with images that involve many users. (A. Satish Kumar & S. Revathy, Review on Social Network Trust With Respect To Big Data Analytics, 2020)

The data of a few users may be in danger if a user distributes a set of data that contains other users, even if different users often have different ideas about who has authority over the data. Trust-based tool for achieving coordinated confidentiality management. Consumers' views are weighed as per the user trust values, which are reviewed when users' privacy is impacted. Peer-to-peer is suggested to balance the confidentiality secured by the information shared with others and anonymisation. (A. Satish Kumar & S. Revathy, An Integrated Privacy on OSN using Advanced Trust Policy, 2021)

3.2. Dataset Description

Simulations run using both real-world data and synthetic. Small-world networks and s Scale-free networks can be produced using Muchnik's complex network package. The scale-free network consists of 1000 nodes and 20001 undirected edges. The average clustering coefficient is 0.052, and the average node degree is 20. There are 20,000 undirected edges and 1000 nodes in the small-world network. The average clustering coefficient is 0.105, and the average node degree is 20. Designers use Facebook data from the Stanford large network dataset collection for modelling purposes. The Facebook network consists of 88234 undirected edges and 4039 nodes. The clustering coefficient average is 0.276, with an average node degree of almost 22.

3.3. Proposed Methodology

In order to ensure that the user receives a high long-turn payoff—the difference between the gain from posting data and the privacy loss brought on by other users—this work establishes a trust-based threshold in the mechanism. The multi-armed bandit (MAB) problem formulation of the parameter selection problem is solved in this paper using the Thompson Sampling (TS) algorithm. This section deals with the proposed work of this paper. Fig. 1 explains that the black arrowed line's thickness represents the stakeholder's truthfulness to the owner. The blue arrowed line's thickness represents stakeholder trust in the owner. After the owner determines whether to post the data, the stakeholder's degree of trust in the owner is updated. The stakeholder's degree of confidence in other individuals is shown by the thickness of the green arrowed line. (A. Satish Kumar & S. Revathy, A hybrid soft computing with big data analytics based protection and recovery strategy for security enhancement in large scale real world online social networks, 2022) Following the publisher's delivery of photographs and information to the receiver that has been anonymised, each stakeholder's evaluation of the publisher is updated.

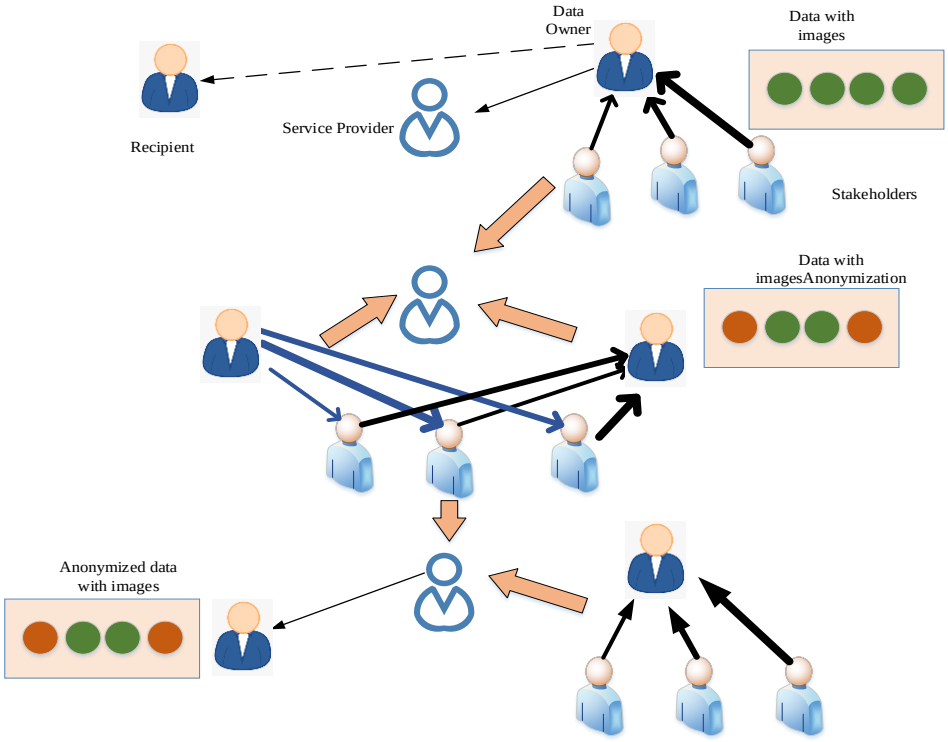

Fig. 1 A mechanism for trust-based privacy management

3.3.1. Social Networking Sites Online

$R = (E, D)$, a directed graph with edge labels, where E denotes the set of vertices and D denotes the set of edges, is used to represent social networking sites online. Each vertex denotes a user. Each edge represents a connection between two users in the graph. Let TR stand for the collection of relationship types that the OSN accepts. A 3-tuple (v_a, v_b, v_{ba}) can be used to describe the edge between users v_a *and* v_b , where $r_{ab} \in TR$ is the label attached to the edge and calculates the distance between any two users by swapping out directed edges in G for un-directed ones. If a path is made available to a pair of users (v_a, v_b), the length of the shortest route between them is defined as the distance D_{ab} . No route connecting users v_a *and* v_b , so researchers set $D_{ab} = \infty$.

3.3.2. Trust Evaluation

The privacy management mechanism suggested in this paper relies heavily on trust. T_{ab} is representing the trust between any two users, v_a *and* v_b, whether or not they are directly connected by an edge. $T_{ab} \in [0,1]$ is defined. User v_a is more trusted by the user v_b when T_{ab} is higher. The symbol for the user v_b confidence in user v_a is v_{ba}. In most cases, $v_{ab} \neq v_{ba}$. To assess trust in social networks, several models, including interaction-based models and network structure-based models, have been put forth. This research concentrates on how collective privacy management may be accomplished through user trust. In this case, first, determine the starting trust levels by applying a recently suggested equation in Eq. (1). As per the newly proposed trust model, both the indirect and direct trust is computed for each of the users.

$$T^{v_a,v_b} = [(W_D * DT^{v_a,v_b} + W_I * IT^{v_a,v_b})] * \frac{S^{v_a,v_b}}{S^{v_a,v_b}+F^{v_a,v_b}} * D_{v_a,v_b} \quad (1)$$

$$DT^{v_a,v_b} = \sum_{m=1}^{k} W_m * \frac{S^{v_a,v_b}+1}{S^{v_a,v_b}+F^{v_a,v_b}+2} * t_m^{v_a,v_b} \quad (2)$$

$$IT^{v_a,v_b} = \sum_{j=1}^{n} W_{v_a,N_j} * DT \quad (3)$$

Here, total trust T is a function of DT^{v_a,v_b} and IT^{v_a,v_b} where W_D and W_I are the weight assigned, W_{v_a,N_j} is the recommendation's weight for the jth neighboring node, S^{v_a,v_b} defines the success rate, F^{v_a,v_b} defines the failure rate and W_m is the trust of each metric.

If users v_a *and* v_b are given, $T_{ab} = 0$ if $D_{ab} = \infty$. When $D_{ab} = 1$, and the two users are connected directly; the kind of connection R_{ab} determines the value of the positive constant T_{ab} . T_{ab} is determined by using using the trust's transitivity characteristic to determine its value,

$$T_{ab} = \Pi_{c=1,\ldots,D_{ab}\left(v_{p_c},v_{p_{c+1}}\right)\in Path_{ab}} T_{p_c p_{c+1}} \quad (4)$$

Where $p_1 = a$ and $p_{D_{ab}+1} = b$; The term $Path_{ab}$ designates the shortest route between users v_a to v_b where $\left(v_{p_c}, v_{p_{c+1}}\right)$ signify two neighbouring users on the path.

Given that the trust value can range from 0 to 1, The relationship between the two users' trust in one another is suggested by Eq. (4) to decrease as their distance grows.

3.3.3. Control of Multiple Parties

The ability for users to easily access data with others is a key component of OSNs. In order to submit a message, the user can:

- Share the data item, like an image, a video, or a text, in their own space or another user's space.
- Distribute a piece of information already published by making it available in one's own location.

Declare the user to be the data owner in the aforementioned two situations. D is defined as a given data item, and the owner of D is represented as O_D. If d contains various users, the users co-own d. Apart from O_D all users connected with D are called stakeholders. H_D defines the group of stakeholders. It should be emphasised that every stakeholder $h \in H_D$ may possess a duplicate of D (D') that contains the exact same information as D. Consider the two data items D and D' separately if the stakeholder h and the owner O_D both want to publish the data items at the same time. This means that the stakeholder h is treated as the stakeholder for the data item D and the owner. O_D is treated as the owner.

In order to restrict who has access, the data owner must include the privacy policy when uploading the data under item D. Let u_A^O stand for the group of users who have permission from the owner. u_A^O is typically determined in practice by the kind of relationship. The owner will lose privacy if any unauthorised user accesses the data. The symbol u_U^O should be used to signify a group of users who are not allowed to access data item D. Loss of privacy for the owner is indicated by the symbol p_O, written as,

$$p_O = |u_U^O|\delta_O \tag{5}$$

where the owner-specified sensitivity of D is indicated by $\delta_O \in [0,1]$ and $|u_U^O|$ stands for the number of users in u_U^O. The data item is more sensitive the higher the value of δ_O is. Each stakeholder $h \in H_D$ can theoretically specify his or her privacy policy if several people are involved in data item D. Let u_A^h stand for the collection of permitted users identified by the stakeholder h. For a specific data item, various users typically have different privacy policies. In other terms, policy disputes between different users are unavoidable.

Owner posting data without taking stakeholder policy into account, the stakeholder will lose privacy if $u_A^h \neq u_A^O$ and $u_A^O \not\subset u_A^h$. The stakeholder h privacy loss, indicated by the letter p_h, can be described as,

$$p_h = \left|u_A^O \backslash u_A^h\right|\delta_h, \tag{6}$$

where $u_A^O \backslash u_A^h$ identifies the group of users who have been given permission by the owner but have been refused by the stakeholder, and $\delta_h \in [0,1]$ indicates the sensitivity of D as determined by the stakeholder. The loss of privacy to the stakeholders might be eliminated if the owner is considerate, the owner requests consent from all stakeholders and bases their decision on their opinions.

3.4. Collaborative Privacy Management Based on Trust

In order to encourage the owner to consult the stakeholders and reach a decision about how to address the privacy conflict resulting from the owner's privacy and the stakeholders' policies, this section of the article recommends a trust-based approach. The proposed mechanism's key is to link a loss of privacy with a loss of trust. The trust-based method is defined, and it is potential to promote a user to preserve the privacy of others is tested.

3.4.1. Voting System Employing Trust

Consider two cases once provided the related owner O_D, set of stakeholders H_D and data item D,

1) Without seeking permission from the stakeholders, the owner posts data directly. For stakeholder $h \in H_D$ to assess the privacy loss p_h, they must be aware of u_A^O. h cannot fully observe u_A^O owner has given users permission and is only known by the service provider and the app owner. Binary number to represent the loss of privacy p_h = 1 if the stakeholders feel that their privacy has been violated, otherwise p_h= 0. The stakeholder will have less faith in the owner if $p_h > 0$. A significant drop in trust results from a high privacy loss. Let t_{ho} represent h faith in O_D before D posting. The new trust value t'_{ho} is calculated after D is posted.

$$t'_{ho} = t_{ho} k(p_h), \tag{7}$$

where p_h the decreasing function is denoted by $k(\cdot)$. There is $k(p_h) \in [0,1]$ for any $p_h \geq 0$, define $k(0) = 1$ to mean that, in the absence of a privacy loss, stakeholders continue to have faith in the owner.. $k(\cdot)$ defined by,

$$k(p_h) = \frac{2e^{-p_h}}{1+e^{-p_h}} \tag{8}$$

2) Before publishing the data, the owner requests stakeholders for their feedback: The owner's ultimate choice in this situation will determine whether a stakeholder loses privacy. Assume the owner uses a voting procedure to incorporate the stakeholders' points of view. The owner advises all H_D stakeholders of his or her privacy policy for relationship types prior to uploading the data item D. It should be emphasised that the service provider might act as the owner's agent to notify the stakeholders if the owner tags each stakeholder in D. Depending on his or her privacy policies with D, each stakeholder $h \in H_D$ determines whether to endorse the owner's policy. To represent h opinion, use a binary variable called y_h: The owner's policy is approved if $y_h = 1$, and it is

disapproved if $y_h = 0$. The stakeholder's viewpoint y_h can be viewed as their vote. The results of the vote, which are calculated as an overall opinion $\bar{y}$,

$$\bar{y} = \frac{\sum_{h \in H_D} y_h t_{oh}}{\sum_{h \in H_D} t_{oh}}, \quad (9)$$

where t_{oh} represents the owner's faith in the stakeholder h. A binary variable named v_o represents the owner's ultimate decision: if $v_o = 1$, Unless the owner posts the data, the data will not be uploaded. Eq. (10) is used to determine the value of v_o:

$$v_o = \begin{cases} 1, & if\ \bar{y} \geq y_{ht} \\ 0, & otherwise \end{cases} \quad (10)$$

where the owner-specified threshold, $y_{ht} \in [0,1]$. Essentially, y_{ht} depends on the owner's willingness to make the data to others' reach. The barrier will be set to a small value if the owner is keen to release the information. In the unlikely event that $y_{ht} = 0$, the owner will post D regardless of the stakeholders' opinions. It is the same as when someone puts their info online without asking permission. Stakeholders can assess privacy loss p_h once the v_o is known. To compute p_h if u_A^O is known to h. If not, p_h is reduced to a binary number. If p_h is greater than 0, the stakeholder's confidence in the owner will decline. However, if $p_h = 0$, the stakeholder will have slightly more faith in the owner because they believe the owner respects their right to privacy. Eq. (11) updates the stakeholder's faith in the owner:

$$t'_{ho} = \begin{cases} i(t_{ho}), & if\ p_h = 0, \\ t_{ho} k(p_h), & if\ p_h > 0, \end{cases} \quad (11)$$

where $i(\cdot)$ is defined as an increasing function of t_{ho} and appeases $i(t_{ho}) > t_{ho}$ and $i(\cdot)$ is given by

$$i(t_{ho}) = t_{ho}^{\in} \text{ , where } 0 < \in < 1 \quad (12)$$

3.4.2. Trust as a Motivator

To address the lack of trust and lack of collaboration comparable to peer-to-peer (P2P) systems and to provide bare-bones privacy among social network users, this solution uses the trust connections built into the social network application itself. The trust values are updated to reflect stakeholder privacy losses in addition to being used to weigh stakeholder votes. The stakeholder's confidence in the owner will decline if the owner uploads a data item and violates their right to privacy, according to the new rule of the trust value. Let us imagine future stakeholder h wishes to upload a data item regarding the owner O_D. Stakeholders h will give the owner. O_D viewpoint less weight even if h begs for it since they have little trust in O_D. As a result, it is more probable that the stakeholder's final judgement will differ from what the owner believes. The danger that the data owner may lose their privacy therefore increases. Some of the stakeholders may be more inclined to trust the data owner if they solicit the stakeholders' opinions before posting the information. When these stakeholders seek approval to post data in the future, the owner O_D opinions will be more respected, and there will be less of a chance that privacy will be compromised. It is advised to analyse the interactions between user privacy protection preferences using an evolutionary game model. According to the game paradigm, user interactions only occur within communities. In this problem scenario, the owner and the stakeholders form a unique community in which the owner's choice may directly or indirectly influence the stakeholders' privacy.

Introduce the notion of reputation to comprehend better how the trust-based mechanism could encourage the user to look for other users' opinions. Regarding a user's reputation on r_i.

$$rep(r_i) = \sum_{r_j \neq r_i} T_{ji} \quad (13)$$

where T_{ji} represents the user r_j confidence in user r_i. Due to the significant influence that a user's reputation will have on other users' decisions to submit information in the future, it is more probable that they will only experience little privacy loss in the future. A user's reputation will change as a result of their actions if they want to submit a co-owned data item. Given a data item D, its corresponding owner O_D, and the group of stakeholders H_D, the owner O_D reputation will suffer if they upload the data item without first getting the stakeholders' consent.

$$\Delta_I = \sum_{h \in H_D} t_{ho} \left(1 - k(p_h)\right) \quad (14)$$

Owner O_D reputation will suffer if it asks for feedback from the stakeholders before deciding to publish the data.

$$\Delta_{II} = \sum_{h \in H_D} \left(t_{ho} - i(t_{ho})\right) \mathbb{1}\,(p_h = 0) + \sum_{h \in H_D} t_{ho} \left(1 - k(p_h)\right) \mathbb{1}\,(p_h > 0) \quad (15)$$

Owner O_D reputation will suffer if it decides not to post the data after asking stakeholders for their opinions.

$$\Delta_{III} = \sum_{h \in H_D} \left(t_{ho} - i(t_{ho})\right) \quad (16)$$

$$\Delta_I - \Delta_{II} = \sum_{h \in H_D} (i(t_{ho}) - t_{ho})\ \mathbb{1}\,(p_h = 0) > 0 \quad (17)$$

$$\Delta_I - \Delta_{III} = \sum_{h \in H_D} (i(t_{ho}) - k(p_h) t_{ho}) > 0 \quad (18)$$

P2P makes use of a decentralised architecture. Superior robustness, balanced load, and security are advantages of a P2P network over a traditional centrally managed network. P2P networks are extremely resilient. The service system's networks are dispersed all over. Damage to particular networks or loads has a positive impact on other components. As a result, specific points of failure can be successfully

avoided. When one or more nodes in a peer-to-peer (P2P) network collapse, the remaining peers may change the architecture on their own, maintaining internet connections and data delivery. P2P provides respectable security. Since a centralised connection is unnecessary, data transfer is distributed among the units. Personal data leakage is much less likely. Any user can offer broadcast services, greatly increasing the adaptability and dependability of encrypted communications. The peer-to-peer (P2P) network contains two parts: the Resource and Search Modules. The Resource Module can be used to describe a peer's assets accurately. The Search Module is in charge of handling and generating the customers' search queries. Asking stakeholders for their opinions will result in a smaller loss of the owner's reputation than simply posting data. Consequently, motivated by the need to preserve their privacy, users will opt to solicit feedback to maintain their good name and conduct simulations to demonstrate how accepting to preserve the user's privacy better secrecy is beneficial.

3.4.3. Privacy Maintenance through Mediator

The trust-based system discussed above may coordinate amongst different users without using an intermediary. The stakeholder is not necessary to know specifically which users the owner has granted permission to use the system in order for the stakeholder to provide basic input when deciding whether to upload data. The owner of a data item is defined as the first user to select to submit the data item, given a data item D and the group of users associated with it. Stakeholders refer to the remaining users. According to the owner, D is accessible to users in the set u_A^O. Before D is made accessible to users in u_A^O, all parties engaged in H_D will be informed. The mediator is subsequently made aware of each party's privacy policies as well as the data item's allocated sensitivity value. In this case, the mediator is assumed to be fully aware of the owners' and stakeholders' approved user lists. In other words, the mediator is aware of u_A^O, and for $h \in H_D$, u_A^h is called a mediator.

Based on what other users $r_i \in \{O_D\} \cup H_D$, each user determines whether or not to publish. For any two users $r_i, r_j \in \{O_D\} \cup H_D$, let $b_{ij} \in \{0,1\}$ signify the user r_j opinion on the user r_i privacy policy. User r_j is unaware of which users are r_i approved users, the mediator can calculate r_j privacy loss denoted as p_{ji}, should r_i post d as intended. Assuming the mediator sends p_{ji} to user r_j, r_j can use p_{ji} as a guide and conclude about r_j viewpoint p_{ji}. The mediator determines the potential privacy loss for each user r_i, gathers the views of those users, and then communicates those opinions to each user r_i. The user r_i can then determine the consensus and decide whether to upload the data item or not. Once more, the belief that the user r_i has in user r_j affects the latter's judgement. Use the binary variable a_i to indicate the final decision made by user r_i. User $\{O_D\} \cup H_D$ can re-evaluate trust in the user r_i. With the assistance of a mediator, the tailored approach described earlier gives all participating users the power to decide when to upload the data item. Thus, users can avoid having to interact recurrently.

3.5. Protecting Privacy and Sharing Data

The user can keep up a good reputation by never posting information that will reveal the privacy of other users. The user's privacy may be well maintained since other users highly appreciate the user's thoughts. In the study of data privacy, striking a balance between privacy and sharing of data is essential. To choose the optimum threshold, model it as a multi-armed bandit problem and use the top trust bound policy.

3.5.1. Decision-Making in Sequence

The user of an OSN continues to upload data until they quit utilising OSN altogether. For user $r \in R$, provide the order of time at which they want to upload jointly owned data as $1, 2, \dots, T$. At time $t \in 1, 2, \dots, T$, the user wishes to upload a co-owned data called D_t. Compiling stakeholder opinion, the decision-maker compares aggregated opinion with threshold y_{ht}. Introduce variable x_t, quantify the value the user receives from sharing of D_t. If D_t is uploaded, then $x_t = 1$; else, $x_t = 0$.

Between time t and time $t+1$, user r does not post co-owned data, but others may publish data connected to the user, which might cause the users to lose privacy. Let, m_t represent the entire amount of privacy user r has lost between t and time $t+1$. Define m_t as follows to compare the privacy loss against the benefit x_t.

$$m_t = \frac{Q_{t,t+1}}{S_{t,t+1}} \qquad (19)$$

Where $S_{t,t+1}$ indicates how frequently other users intend to post information about user r between t and $t+1$, and $Q_{t,t+1}$ indicates how frequently a user r loses privacy as a result of other users. $Q_{t,t+1}, S_{t,t+1}$ observe that $0 \le m_t \le 1$.

$S_{t,t+1}$ is a random number from the viewpoint of the user r. Regarding $Q_{t,t+1}$, the reputation of the user r at time t determines if others will invade their privacy throughout the period (t and $t+1$). Let rep_t represent user r reputation following their choice to post data at time t. You can think of the privacy loss m_t as a random variable connected to the rep_t. The user is less likely to lose privacy the higher their reputation. The way the user chooses the threshold y_{ht}, which effectively determines how reputation and update rules of trust are affected, changes to the user's reputation time t, and they differ between rep_t and rep_{t-1} is how the user gathers the views of stakeholders.

The Threshold y_{ht} selected at the time, t determines how much privacy is lost at the time m_t, a random variable. When user r decides to post data at time t, the reward is defined as follows:

$$O_t = x_t - m_t \quad (20)$$

Then O_t can be thought of as a random variable. If it is expected that a model independent of the degree of trust between users may describe users' propensity to publish co-owned data items, it is further shown that the distribution of O_t is wholly dictated by the threshold y_{ht}. Given y_{ht}, the anticipated payout t may be represented as follows.

$$\mu_t = fu_t(y_{ht}) \quad (21)$$

Since the user r is unaware of the model mentioned above, both distribution O_t and function $fu_t(\cdot)$ un-known.

3.5.2. Formulation of Bandit

The benefit of loss of privacy and data sharing are combined to form the payoff and talked about the connection between the payoff and the y_{ht} threshold. The user's objective is to choose a suitable threshold to increase the payoff. Because the user publishes data sequentially and user trust levels fluctuate over time, the threshold has to be constantly changed.

The user must decide whether focus on the threshold that so far yielded the highest payment based on existing information or look into thresholds that provide higher payoffs in future. Sequential decision-making is formalised as a bandit problem to handle trade-offs between exploration and exploitation.

Assume user r chooses threshold from the set, where N is a positive integer and $\Theta \triangleq \left\{\theta_i \middle| \theta_i = \frac{i}{N}, i = 1, \dots, N\right\}$. Limit the threshold to a set of discrete numbers to keep things simple. In bandit language, each threshold $\theta_i \in \Theta$ is referred to as an arm. If the user chooses, θ_i at time t, they will be rewarded with $re_{i,t} \triangleq O_t$. From an undisclosed probability distribution connected to the arm, the prize is selected at random. The estimated payoff for each arm $\theta_i \in \Theta$ is

$$\mu_i = fu_t(\theta_i) \quad (22)$$

To choose the best arm, the user must employ a learning strategy θ_I without knowing the function $fu_t(\cdot)$, where

$$I^* = arg \max_{i=1,\dots,N} \mu_i \quad (23)$$

In a learning policy, $\{\sigma_t\}$ indicates mapping from observed history up to time $t-1$ to the index of arm chosen at time t, designated by the letter It. This mapping defines a collection of mappings. The effectiveness learning policy is often evaluated by comparing the benefits accrued by it to incentives accrued by an ideal benchmark strategy that always selects the best arm. Below is an official definition of regret.

$$RE(T) = T\mu_I * - \mathbb{E}\sum_{t=1}^{T} \mu_{I_t}, \quad (24)$$

The expectation is taken into consideration over any potential unpredictability in the learning procedure where T defines the time horizon.

According to the above-described bandit formulation, the reward $re_{i,t}$ associated with each arm is mostly random due to the privacy loss that occurs between time t to time t + 1. Additionally, the loss is intimately tied to user reputation. Because rep_t varies with t, the probability distribution of reward is time variant. As a result, abbreviate the notation $fu_t(\cdot)$. The study of the well-known stochastic bandit issue assumes that reward distribution for each arm is time-invariant; therefore, the optimal arm is fixed. The optimum arm in this scenario may change over time.

The issue is the same as the adversarial bandit problem, which is independent of statistical forecasts on the nature of reward generation. In an adversarial bandit problem, the reward for an arm is determined by an opponent by the particular probability distribution. In the suggested bandit dilemma, rewards of arms rely on the history of the user's interactions with other users, which affects the user's reputation. This is comparable to the scenario where an unknowing opponent chooses incentives based on prior interactions between users.

Analysing an issue with hostile bandits can be challenging. The method of generating incentives is not completely random, assuming a particular model for users' inclination to contribute co-owned data. Despite not being stationary, stochastic distributions can still be used to simulate the advantages. To evaluate the effectiveness of the learning strategy, substitute mild regret, which is recommended for conflicted bandit issues. According to the government, weak remorse is described as,

$$R_{weak1}(T) = \max_{i=1,\dots,N} \sum_{t=1}^{T} re_{i,t} - \sum_{t=1}^{T} re_{I_{t,t}} \quad (25)$$

Similar to regret, weak regret compares a learning policy to a hypothetical-benchmark-policy chooses the "best" arm in order to assess how successful the learning policy is. The optimal arm in the concept of weak regret can only be determined after the event; $\sum_{t=1}^{T} re_{i,t}$ it is the one that results in the highest total benefit.

3.5.3. Knowledge Strategy

The reward allocation of different arms is designed by the Bayesian probabilistic method by Thompson Sampling (TS) algorithm. By utilising Bayesian prediction, TS, a randomly chosen algorithm, can evaluate the reward probability θ^p connected to each arm p of MAB. The state of a system intended for p armed MABs can therefore be fully specified by $\left\{(\alpha_i^1, \beta_i^1), (\alpha_i^2, \beta_i^2), \dots (\alpha_i^p, \beta_i^p)\right\}$ after conducting i MAB trials and estimating the reward probability p of each arm p using a posterior distribution over possible estimates, $Beta(\alpha_i^p, \beta_i^p)$. Each trial's arm is chosen by drawing one

sample from the random variable $\widehat{\Theta}_i^p, \widehat{\Theta}_i^p \sim Beta(\alpha_i^p, \beta_i^p)$ where $p = 1,2,3, \dots, p$, and playing the arm with the highest sample value. Using the mentioned, arm k will be played is $PR(\hat{\theta}^p > \hat{\theta}^1 \wedge \hat{\theta}^p > \hat{\theta}^2 \wedge \hat{\theta}^p > \hat{\theta}^3 \dots \hat{\theta}^p > \hat{\theta}^p)$, but the great thing about TS is that the probability does not have to be calculated explicitly. Bandit problems frequently use the TS put forth.

The core idea of TS is to predict the unknown expected reward for each arm based on previously reported arm rewards. Even if the TS policy may be applied to the presented issue, it is difficult to assess the regret conceptually. How to evaluate how effectively the learning policy is working is determined by using an empirical technique.

4. Result and Discussion

4.1. Experimental Setup

PYTHON has been used to implement the recommended model. The performance of the proposed approach and current algorithm has been analysed and compared. The recommended model's precision, recall, f-measure, accuracy, sensitivity, and specificity have all been investigated.

4.2. Overall Performance Analysis of Projected Model

The test results from the suggested procedure are examined in this section. The projected model is compared to the existing models like IIR, VLT, and TM_DPM, respectively. Precision, recall, f-measure, accuracy, sensitivity, and specificity have all been included in the evaluation. The results acquired are shown in Table I-Table VI, respectively.

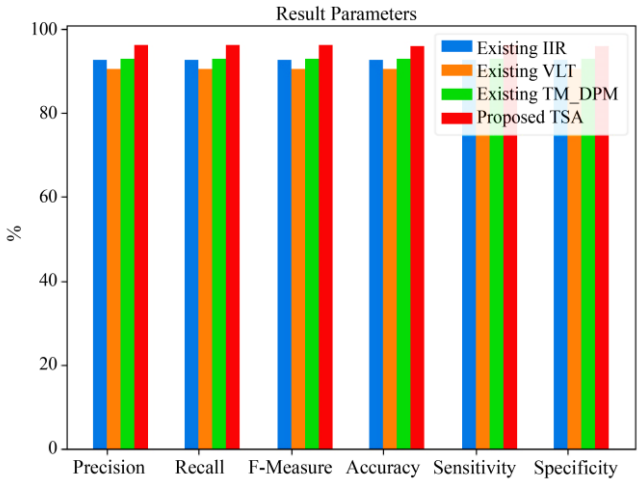

Fig. 2 Overall performance analysis

4.3. Analysis of Accuracy

The accuracy is the key parameter that decides the success of the overall proposed model. Accuracy is a measurement of how closely a value corresponds to information. The performance of accuracy is shown in Table I. The proposed model has recorded the accuracy value as 95.9232614, which is the highest value compared to the existing models (TM_A_DPM = 92.7971188, VLT = 90.3961585, and IIR = 92.5570228). The results acquired in terms of accuracy are graphically shown in Fig. 2.

Table 1. Performance of accuracy

Method	Accuracy
Proposed TSA	95.9232614
Existing TM_A_DPM	92.7971188
Existing VLT	90.3961585
Existing IIR	92.5570228

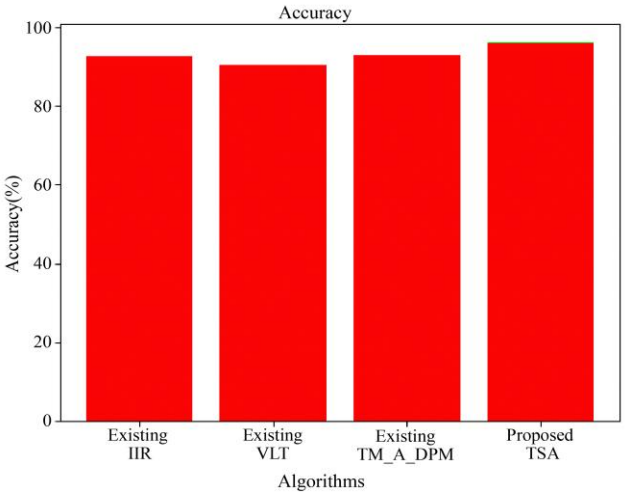

Fig. 3 Analysis of accuracy

4.4. Analysis of F-Measure

F-Measure offers a method for combining recall and accuracy into a single measure that encompasses both characteristics. The performance of the F-measure is shown in Table II. The proposed model has recorded the F-measure value as 96.01873536, which is the highest value compared to the existing models (TM_A_DPM = 92.68292683, VLT = 90.45346062, and IIR = 92.65402844). Figure 3 illustrates the findings obtained in terms of the F-measure.

4.5. Analysis of Precision

The quantity of information that a value provides is known as precision. The performance of precision is shown in Table III. The proposed model has recorded the precision value as 96.0187354, which is the highest value compared to the existing models (TM_A_DPM = 92.6829268, VLT = 90.4534606, and IIR = 92.6540284). Fig. 4 illustrates the findings obtained in terms of precision.

Table 2. Performance of F-Measure

Method	F-Measure
Proposed TSA	96.01873536
Existing TM_A_DPM	92.68292683
Existing VLT	90.45346062
Existing IIR	92.65402844

Table 3. Performance of precision

Method	Precision
Proposed TSA	96.0187354
Existing TM_A_DPM	92.6829268
Existing VLT	90.4534606
Existing IIR	92.6540284

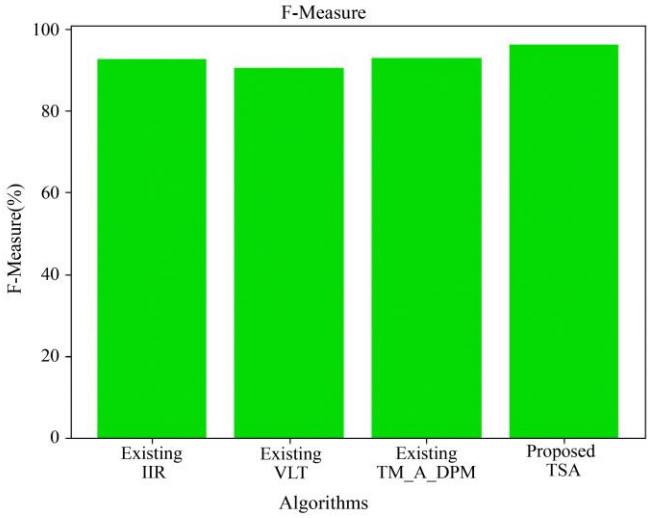

Fig. 4 Analysis of F-Measure

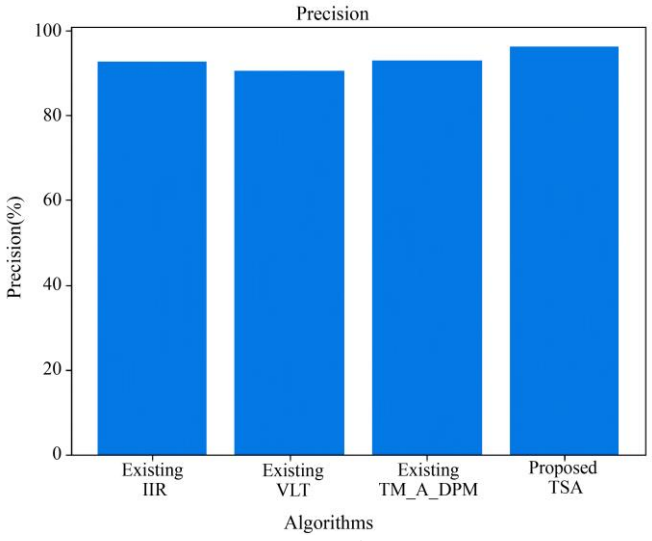

Fig. 5 Analysis of precision

4.6. Analysis of Sensitivity

The ratio of accurately classified positives to real positives is known as a classifier's sensitivity. The performance of sensitivity is shown in Table IV. The proposed model has recorded the sensitivity value as 96.0187354, which is the highest value compared to the existing models (TM_A_DPM = 92.6829268, VLT = 90.4534606, and IIR = 92.6540284). In Fig. 5, the results obtained regarding sensitivity are represented visually.

Table 4. Performance of sensitivity

Method	Sensitivity
Proposed TSA	96.01873536
Existing TM_A_DPM	92.79711885
Existing VLT	90.45346062
Existing IIR	92.65402844

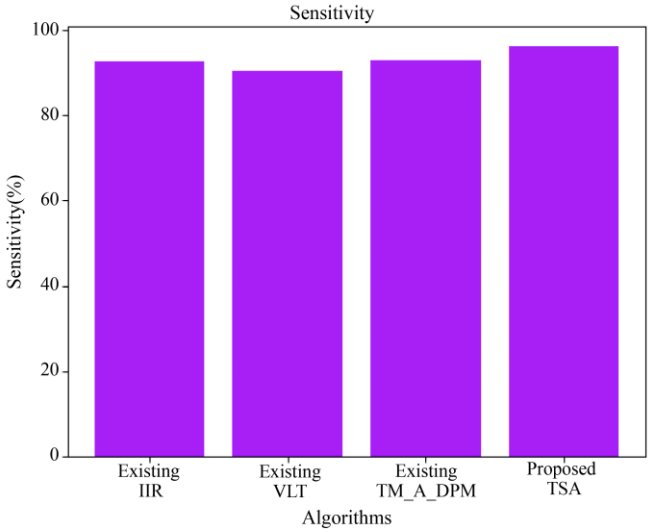

Fig. 6 Analysis of sensitivity

4.7. Analysis of Recall

The terms "recall" and "sensitivity" are equivalent. The performance of recall is shown in Table V. The proposed model has recorded the recall value as 96.0187354, which is the highest value compared to the existing models (TM_A_DPM = 92.6829268, VLT = 90.4534606, and IIR = 92.6540284). Fig. 5 visually displays the recall data that were obtained.

4.8. Analysis of Specificity

The ratio of correctly identified negative data to real negative data is known as the specificity of a classifier. The performance of specificity is shown in Table VI. The proposed model has recorded the specificity value as 95.82309582, which is the highest value compared to the existing models (TM_A_DPM = 92.90780142, VLT = 90.33816425, and IIR = 92.45742092). In Fig. 7, the findings obtained in terms of specificity are represented visually.

Table 5. Performance of recall

Method	Recall
Proposed TSA	96.01874
Existing TM_A_DPM	92.68293
Existing VLT	90.45346
Existing IIR	92.65403

Table 6. Performance of specificity

Method	Specificity
Proposed TSA	95.82309582
Existing TM_A_DPM	92.90780142
Existing VLT	90.33816425
Existing IIR	92.45742092

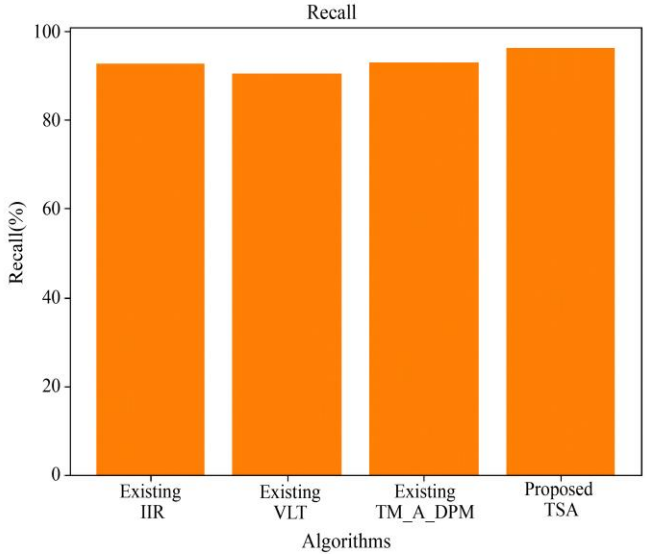

Fig. 7 Analysis of recall

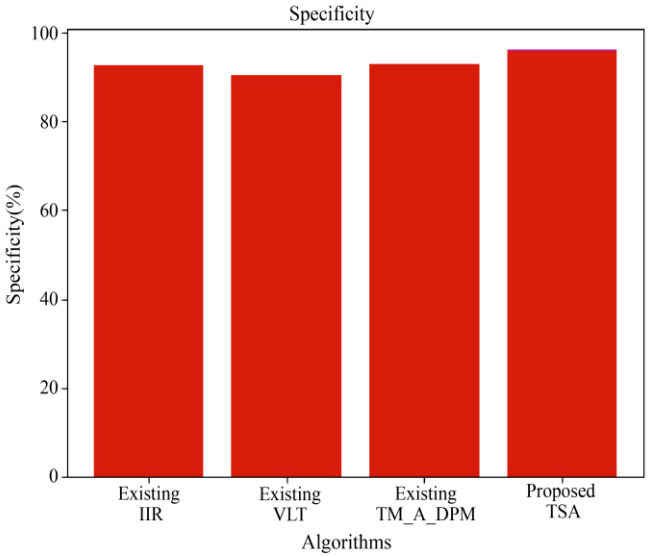

Fig. 8 Analysis of specificity

4.9. Analysis of Training Time

The time taken to train the system defines the training time. The performance of training time is shown in Table VII. The proposed model has recorded the training time value as 39003 sec, which is the highest value compared to the existing models (TM_A_DPM = 48003 sec, VLT = 53006 sec, and IIR = 57004 sec). Fig. 8 presents graphically the training time findings that were obtained.

Table 7. Performance of training time

Method	Training Time (Sec)
Proposed TSA	39003
Existing TM_A_DPM	48003
Existing VLT	53006
Existing IIR	57004

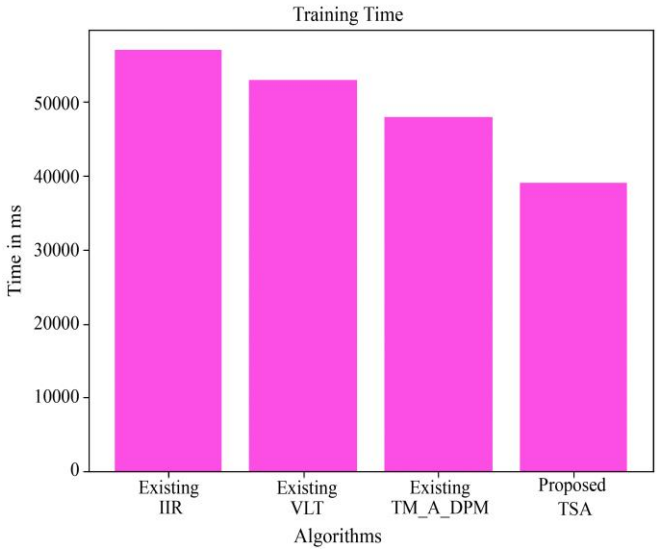

Fig. 9 Analysis of training time

5. Conclusion

The most significant platforms for people to communicate with others have arisen as online social networks (OSNs), including Google, Facebook, and Twitter. OSNs receive text messages, photos, and videos from thousands to millions of users who document their daily lives. Users' privacy is at stake if unauthorised parties access their data. In order to ensure that the user obtains a high long-turn return, this study defines threshold in a trust-based mechanism as the difference between the advantage of publishing data and privacy loss caused by other users.

To deal with the lack of cooperation and trust similar to peer-to-peer networks. The user is given the option to choose between sharing data and maintaining their privacy by altering the suggested mechanism's parameter. The Thompson Sampling (TS) approach was used in this work to resolve the parameter selection problem's multi-armed bandit (MAB) issue formulation. Based on their credibility, user opinions are assigned a specific amount of weight, which rises when privacy is violated. This study used a brand-new bifold trust model to calculate the users' trust score.

The publisher is required to adaptively alter the threshold in order to strike a balance between privacy protection and document sharing. Therefore, integrating trust-based trust values into the process of document anonymisation may assist in reducing the loss of user privacy. The system was designed

to be deployed in the PYTHON working environment, and simulations show that the trust-based method maintains user trust by safeguarding privacy and reducing information loss. The simulation outcomes demonstrate that the suggested bandit approach may provide a considerable reward and that the trust-based mechanism might motivate the user to respect users privacy.

References

[1] Lei Xu et al., "Trust-Based Privacy-Preserving Photo Sharing in Online Social Networks," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 591-602, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Kaihe Xu et al., "My Privacy My Decision: Control of Photo Sharing on Online Social Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 199-210, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[3] S. Sicari et al., "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, vol. 76, pp. 146-164, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[4] John Carlo Bertot, Paul T. Jaeger, and Derek Hansen, "The Impact of Polices on Government Social Media Usage: Issues, Challenges, and Recommendations," *Government Information Quarterly*, vol. 29, no. 1, pp. 30-40, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[5] Cheng-Kang Chu et al., "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 468-477, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[6] Lei Xu et al.,"Trust-Based Collaborative Privacy Management in Online Social Networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 48-60, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] Amin Ranjbar, and Muthucumaru Maheswaran, "Using Community Structure to Control Information Sharing in Online Social Networks," *Computer Communications*, vol. 41, pp. 11-21, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[8] Elisa Bertino, Igor Nai Fovino, and Loredana Parasiliti Provenza, "A Framework for Evaluating Privacy Preserving Data Mining Algorithms," *Data Mining and Knowledge Discovery*, vol. 11, no. 2, pp. 121-154, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[9] Yifan Wu et al., "Privacy-Protective-GAN for Privacy Preserving Face De-Identification," *Journal of Computer Science and Technology*, vol. 34, no. 1, pp. 47-60, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Nemi Chandra Rathore, and Somanath Tripathy, "A Trust-Based Collaborative Access Control Model with Policy Aggregation for Online Social Networks," *Social Network Analysis and Mining*, vol. 7, no. 1, pp. 1-13, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[11] Hadas Schwartz-Chassidim et al., "Selectivity in Posting on Social Networks: The Role of Privacy Concerns, Social Capital, and Technical Literacy," *Heliyon*, vol. 6, no. 2, p. e03298, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Zheng Yan, and Mingjun Wang, "Protect Pervasive Social Networking based on Two-Dimensional Trust Levels," *IEEE Systems Journal*, vol. 11, no. 1, pp. 207-218, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[13] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 7, pp. 1614-1627, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[14] Hanaa Alshareef et al., "A Collaborative Access Control Framework for Online Social Networks," *Journal of Logical and Algebraic Methods in Programming*, vol. 114, p. 100562, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Chrystel Gaber et al., "Liability-Aware Security Management for 5G," *IEEE 3rd 5G World Forum (5GWF), IEEE*, pp. 133-138, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Raquel Ureña, Francisco Chiclana, and Enrique Herrera-Viedma, "DeciTrustNET: A Graph-Based Trust and Reputation Framework for Social Networks," *Information Fusion*, vol. 61, pp. 101-112, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Gelan Yang, Qin Yang, and Huixia Jin, "A Novel Trust Recommendation Model for Mobile Social Network based on User Motivation," *Electronic Commerce Research*, vol. 21, no. 3, pp. 809-830, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Ying He et al., "Trust-based Social Networks with Computing, Caching and Communications: A Deep Reinforcement Learning Approach," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 66-79, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[19] Wei Wei et al., "Fractal Intelligent Privacy Protection in Online Social Network using Attribute-Based Encryption Schemes," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 736-747, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abdelmuttlib Ibrahim Abdalla Ahmed et al., "Trust and Reputation for Internet of Things: Fundamentals, Taxonomy, and Open Research Challenges," *Journal of Network and Computer Applications*, vol. 145, p. 102409, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Feng Wang et al., "Maximizing Positive Influence in Competitive Social Networks: A Trust-Based Solution," *Information Sciences*, vol. 546, pp. 559-572, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Ying He et al., "Secure Social Networks in 5G Systems with Mobile Edge Computing, Caching, and Device-to-Device Communications," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 103-109, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[23] Venus Mohammadi et al., "Trust-based Friend Selection Algorithm for navigability in social Internet of Things," *Knowledge-Based Systems*, vol. 232, p. 107479, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] Laizhong Cui et al., "Exploring a Trust-Based Recommendation Approach for Videos in Online Social Network," *Journal of Signal Processing Systems*, vol. 86, no. 2, pp. 207-219, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[25] Zhi-Jiang Liu, Sergei Chernov, and Anna V. Mikhaylova, "Trust Management and Benefits of Vehicular Social Networking: An Approach to Verification and Safety," *Technological Forecasting and Social Change*, vol. 166, p. 120613, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] A. Satish Kumar, and S. Revathy, "Review on Social Network Trust with Respect to Big Data Analytics," *4th International Conference on Trends in Electronics and Informatics*, Tirunelveli, India, pp. 721-727, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Siddhi Narendra Jadhav et al., "Implementing Secured Network for Tier 1 Organization," *SSRG International Journal of Electronics and Communication Engineering*, vol. 7, no. 4, pp. 14-20, 2020. [CrossRef] [Publisher Link]

[28] A. Satish Kumar, and S. Revathy, "An Integrated Privacy on OSN using Advanced Trust Policy," *Design Engineering*, pp. 125-132, 2021. [Google Scholar] [Publisher Link]

[29] A. Satish Kumar, and S. Revathy, "Evaluation of Trust Path Among Users in Online Social Networks Using Hadoop Map Reduce," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 5, pp. 1302-1312, 2021.

[30] A. Satish Kumar, and S. Revathy, "A Hybrid Soft Computing with Big Data Analytics based Protection and Recovery Strategy for Security Enhancement in Large Scale Real World Online Social Networks," *Theoretical Computer Science*, vol. 927, pp. 15-30, 2022. [CrossRef] [Google Scholar] [Publisher Link]