Hindawi
Security and Communication Networks
Volume 2022, Article ID 1929339, 11 pages
https://doi.org/10.1155/2022/1929339

Research Article

A Dynamic and Automated Access Control Management System for Social Networks

Sohail Abid and Malik Imran Daud

Department of Software Engineering, Foundation University Islamabad, Islamabad 46000, Pakistan

Correspondence should be addressed to Sohail Abid; sohailabid@fui.edu.pk

Received 3 September 2022; Revised 29 September 2022; Accepted 11 October 2022; Published 27 October 2022

Academic Editor: Andrea Michienzi

Copyright © 2022 Sohail Abid and Malik Imran Daud. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In recent years, online social networks (OSNs) have become an essential part of our social life. In OSNs, users can post resources to predefined groups of users, for example, family, friends, close friends. However, due to these predefined groups of users, few irrelevant users may get access to these published resources. Moreover, the users cannot configure privacy settings due to the lack of technical knowledge and the rigidity of the access control management system. To tackle these issues, we propose a text-based dynamic and fine-grain access control system for OSNs. Our proposed model uses a dynamic clustering algorithm to create user clusters based on the mutual interests of the users. After clustering, the proposed system creates automatic access rules based on the relationship between the users' clusters and their resources. The proposed system will ensure fine-grained access control and automatic assignment of policies to the text-based resources. We have implemented our system to gauge the applicability, and the results are discussed in the experiments section.

1. Introduction

In online social networks (OSN), users usually publish resources like text, photos, audio, and video messages. Due to the rapid growth of the Internet, OSNs have become one of the modern ways for people to communicate. The advancement in technology and the ease of using social media have increased the growth of OSNs over the years. In addition, most of the organizations have started business activities on OSNs. According to Zephoria digital marketing, Facebook had a monthly 2.7 billion live users worldwide. It is the third most visited website ever since 2020 [1]. These days, Twitter, another famous social network, has monthly estimated of more than 31.3 billion of live users, and these users publish their tweets in different languages [2]. Similarly, companies and employers inspect profiles of OSN users such as LinkedIn, Twitter, and Facebook [3] for recruitment/advertisement purposes. To resolve crimes, law implementation organizations are gleaning proof from OSNs [4]. Since users in OSNs are usually linked to friends and family, a general observation is that OSNs provide a more protected and trusted personal atmosphere for online communication [5]. A study reveals [6] that 72% of American use OSNs for online communication with friends, family, and visitors.

Nowadays, machine learning-based techniques are very famous, and researchers use these techniques to resolve complex problems. In machine learning, KNN (*K*-nearest neighbors) algorithm is one of the essential and straightforward classification algorithms. It is based on supervised learning and is very helpful in intrusion detection, data mining and pattern recognition, and data mining applications. In real-life situations, it is extensively used in several applications. The KNN algorithm is a lazy learning method created for real-world applications and proposed by Fix et al. in 1951 [7]. KNN algorithm is generally used for pattern arrangement based on feature resemblance, and it is categorized based on the majority vote of its neighbors and allocated to the category nearest among its K-nearest neighbors. Contrasting to the other statistical approaches, which explain a model from the information obtained from the historical data, the KNN algorithm understands the training dataset as the model itself. Therefore, there is no training stage for the KNN algorithm during the testing

stage. Further information on the KNN algorithm can be found in [8].

In OSN, users communicate with other users through mutual interests and share information and resources; therefore, OSN and related applications are full of an extraordinary amount of private information. This private information and resources are the main privacy concerns for the OSN users. These privacy and safety problems pose the main disadvantage for the users and the OSN service providers [9–11]. Moreover, the addition of unknown persons as a friend in the OSNs can be a serious privacy threat [12–14]. In most of the OSNs, the users are tagged in a published message, yet causing another mode of privacy leakage. This privacy leakage of personal information of the users may impact their private life [15].

In order to tackle the above-mentioned privacy issues, researchers proposed some useful methods. In 2016, Imran-Daud et al. [16] proposed a dynamic and automatic access control method for medical-based OSNs, which creates rules dynamically and automatically at runtime and provides users with an anonymized textual-based resource. The limitation of this method is to select users in a static way (i.e., predefined groups of users are selected), whereas the proposed privacy-based technique creates groups of users dynamically and maintains fine-grained access control. Outchakoucht et al. [17] proposed the dynamic access control method developed for IoT. The architecture of this model consists of ORBAC and blockchain techniques. Therefore, it is designed for organizational-based systems, and blockchains have their limitations which are discussed in related work in detail. This method creates dynamic policies and is applied to the predefined group of users, and due to these groups of users, few irrelevant users get access to the resource.

Kayes et al. [18] proposed another access control method for IoT based on RBAC, which dynamically creates roles based on the related contextual situations and is designed explicitly for IoT and organizational-based systems. However, these partially dynamic methods have some limitations, and users' privacy is compromised due to these limitations. Therefore, a fully dynamic and automatic access control system is required to manage privacy-aware OSN resources.

1.1. Motivation. OSNs usually provide static contact lists such as family, friends, close friends. The published resource is shared with a few irrelevant users due to this predefined group of users [19]. Similarly, predefined policies (or static policies) are applied to a specific group of users, including those that may be irrelevant to the resource. Therefore, these static policies/rules are the core reason for privacy leakage [19]. Most of the OSN users cannot configure privacy settings due to lack of technical knowledge that leads to privacy leakage. However, access control models require such a procedure that may secure the personal information of users that can automatically and dynamically administer privacy settings in OSN [19]. The dynamic and automatic access control management framework for OSN should be created as a prototype that will guarantee the resource owner privacy within the OSN, and it must adapt to current privacy requirements in a given situation to develop rules/policies accordingly [19–21]. The aim of this research is to address social network-based privacy problems as discussed above.

1.2. Contribution. In this paper, we propose a dynamic, fine-grained, and privacy-aware access control model for OSNs that automatically creates and evaluates access policies based on relationships between resources and users. The contribution of the research work is as follows:

(i) The proposed system extracts common interests of the users from user profile data.

(ii) The system generates interest-based clusters from the user profiles by creating user clusters based on common interests within the users. These user clusters are beneficial for categorizing users into different groups based on their interests.

(iii) The proposed system identifies the relationship attributes from the text resource using NLP functions.

(iv) The proposed system identifies the relationship between text resources and user clusters with the help of identified relationship attributes. These recognized relationships are beneficial for managing access to the resources.

(v) The proposed system automatically and dynamically creates rules based on the identified relationship between resources and user clusters.

(vi) The automated delegation is managed based on recognized relationships and selected user clusters.

1.3. Organization. The rest of the organization is as follows: in Section 2, the related work is deliberated. Section 3 presents a dynamic, fine-grained, and automated access control model which enhances the security and privacy of OSN resources. In Section 4, the results and discussions support our idea. In the end, we discuss the conclusion and future research directions.

2. Related Work

A critical literature assessment is an important feature to expose research areas where the investigation is needed. Numerous access control systems have been presented for access control since 2021. Inferring user profile information has been widely discussed [19, 20], and most infernal attempts to discover the personal information of a user by perceiving OSN groups and network contacts. Hence, a large portion of work has been done in this area, and a few of them are as follows.

In OSNs, access control offers some unique features dissimilar from previous access control. The mandatory and RBAC method implements an organization-wide access control policy that is naturally definite through the security manager. The author describes the resource access rule in the discretionary access control model. However, in OSN

systems, users expect to regulate access to their resources and activities related to themselves. Thus, access to OSNs is subject to user-specified policies. Access control systems used in IoT are RBAC (role-based) [21], organization-based (Or-BAC) [22], trust-based [23], capability-based (CapBAC) [24, 25], and attribute-based access control (ABAC) [26, 27]. In a centralized access control system, rights are assigned by a centralized entity that turns out to be a failure [28]. Most of the new models are based on RBAC and ABAC methods, in which the researchers introduced changes like relation and trust to improve the access level. Some famous game theory-based access control models like Wellman and Berkowitz [29] proposed a novel access control method using game theory to investigate the advantages of owners and visitor content in OSN. Tian and Lin [30] presented a method based on game control that investigates the conduct of users using game theory in OSNs and manages resource access via a trusted estimate of user conduct. Yu et al. [31] prepared a game framework for competitive information dissemination in OSNs to comprehend the inspiration of human behaviors such as money, learning, interest, and knowledge wishes on competitive info distribution. Zhu et al. [32] implement recurrent games and incentive methods to enhance the proficiency of resource allocation in OSNs. Still, the above-discussed access control approaches cannot wisely provide users with advice on what way to create access control rules [33]. In OSNs, there is no central authority to find affiliations between users and manage policies, and access control is applied by cryptographic worth [5, 34]. Pang and Zhang [35] resolved access control and privacy protection issues in OSNs by using a cryptography-based solution. They also directed a new advanced way for access control mechanisms in OSNs. This type of access control technique is proficient to define situations based on 'k-depth' and 'k-common friends. This method is more secure than traditional relationship-based access-control systems. Still, the cryptography-based models require high computational resources of computers for execution and performance.

A blockchain is an innovative and decentralized, skill behind famous cryptocurrencies like Bitcoin [36] and Ethereum [37]. Every block has a limited size and rate for storing transactions, In Bit-coin average block development time is 15 minutes, and block size is 1 Megabyte, and the maximum throughput is 7 tps (transactions per second) [38]. Ouaddah et al. [39, 40] first proposed and implemented the fair method of access. Their method of access handling utilized the consistency of the blockchain. Maesa et al. [41] published access control policies using blockchain technology. Outchakoucht et al. [17] enhanced the fair access model security using machine learning algorithms [42]. Smartly chosen contracts are implemented to analyze policies to manage access control. Zhang et al. [43] split access control contract into two streams. First is used to manage access, and the other stream is used to determine the misuse of the access control. Dukkipati et al. [44] model includes two types of policies (i). general policies and (ii). special policies in the blockchain. Maesa et al. [45] offer a model based on the Ethereum blockchain. The limitation of the above techniques is high computational capability, no microtransactions support, open ledger problem, and high transaction fee. In the paper [46], the author's proposal depends on a pair of algorithms, first for getting resources and second for sharing resources based on the collaborative access-control model. Their work is needed in the area of automatic enforcement and evaluation of the policies. The author also recommended that smart contracts may solve automatic enforcement and evaluation of policies, and IOTA currently does not support smart contracts. In collaborative-based access control known as aggregation-based models [47], the individuals involved in sharing some content should decide whether to share their information or not. The drawbacks in previous models [48, 49] deter them to handle every case in its entirety, and in a few cases, these models have to depend only on the owner's data to resolve the conflicts. Due to these reasons, there is a need for new conflict resolution strategies. In the paper [50], the researcher proposed a collaborative access control framework for OSNs which decides whether to allow or deny access to an object. It involves the privacy settings of the owner, originator, contributor, and others involved. Four things are under consideration: user's trust relationship, user's sensitivity level, weights of access types, and controller types. They proposed an algorithm to grant view and share access. Algorithm evaluation is done using theoretical and self-created scenario-based data. The limitation of this study is that while dealing with high workloads and big data, it will show problems that should be taken care of. They left this evaluation as future work.

Fong et al. [51], Gates [52], and Carminati and Ferrari [53] utilized a relationship-based model for OSN, to control whether guests can permit resources. In [54–56], Fong and Siahaan and Bruns et al. describe access control tactics in OSNs and presented a mixed logic using modal logic language. In [57, 58], Park et al. and Cheng et al. describe access control rules/policies based on regular expressions, permitting user-resource, resource-resource, and user-user relations to manage guests' permission on resources. This type of approach in OSNs gives users a way to manage permission on resources. So, the various relationships are related to various access rights. The relationship-based access management model is easy to recognize and simple to apply in OSNs. Therefore, it is tough for users to discover which access privileges a relationship must be linked providing by the resource. Another automated and dynamic access control approach is proposed by Abid and Daud [59] which is also based on dynamic relationships. The maximum present OSN models impose a basic and limited relationship-based access control method, allowing users to select rules from a predefined vocabulary, like "private," "public," "friend," and "friend of a friend." Facebook and Google + presented traditional relationships, specifically "friend list" and "circle," giving users more choices to distinguish particularly privileged-user sets [60].

Malik et al. have focused on IoT-based traditional access control and social network systems [61]. This author recommends some critical issues for access control systems; the access control systems must be dynamic and proficient in changing the access authorizations at runtime based on

requirements [61, 62]. It should be fine-grained to secure sensitive and private resources [52, 61]. Finally, it is concluded that none of the methods is fully capable of delivering dynamic and privacy-aware access control. Therefore, the need for a dynamic, fine-grained, and automated access control model in OSNs is required. This proposed system will automatically assigns the policies to the textual resources and to the captions of videos and images.

3. Proposed Methodology

Our system operates on the profile data to get the relevant information about the owner to manage access control on the shared resources (e.g., list of friends, education information, work). Based on the profile data, the system automatically generates clusters, and the users are automatically mapped to these clusters based on their relevance to them. These clusters are also known as friends' clusters (FC's). The interests are extracted from the content when a user tries to publish a message through the OSN. Our system identified the relationship between interests and FCs'. Based on the contact relationship, one or more than one cluster is selected. If more than one cluster are selected, in that case, the system automatically prepares one cluster by taking the union of selected clusters (an instance of merging two or more clusters into one cluster). In addition, a permit rule/policy is formed based on the affiliation among the interests and friends cluster. Finally, according to the rule/policy, the message is tagged to the designated friends' cluster. The selected FC members have permission to access and share the message according to the rule/policy. It is noted that only the message-related users get access to the resource or message.

Flow control of submodules of the system diagram is depicted in Figure 1. Our system is initialized by creating friends' clusters (FCs) that are achieved through the interest-based clustering algorithm, which is based on two functions: interest selection function (ISF) and clustering function (CF). The ISF selects interest categories from the user profile and sends these interest categories to the CF. The CF creates the users' clusters based on these interest categories, which are stored in the FCs database (FCs DB). This whole process of user clustering is also known as the initialization process (IP). These friends' clusters (FCs) are very useful for categorizing users into different clusters based on their interests. The IP starts at the beginning of the system and repeats whenever a new user is added to the system. The FCs' database (FCs DB) will be updated due to this process.

The processes of ISF and CF are explained in Algorithm 1. In line 1, the profile data of the users are retrieved to make friends' clusters. This profile data may contain fields such as Name, Designation, employment information, location, educational information. In lines 2–8, text processing of profile data is performed like data cleaning and transformation of profile data. Through this process, the text is prepared for feature extraction. In lines 9–20, first select interest fields (like location, job, marital status, education) and then further used them to extract interest categories from selected fields, for example, we get three categories single, married, and divorced from the marital status field. In lines 21–30, CF uses interests as a centroid for clustering, and finally, clusters are created based on the matching of interests with profile data.

Once the initialization process is completed, the next workflow of the proposed system is as follows. The owner sends a message m to the parser for publishing. The parser interprets the message by extracting interest attributes (like location, job, marital status, education) from the message. These interest attributes are helpful to select a specific set of users or friends' clusters (FCs) (details in Section 3.1). The rule creation manager (RCM) is used for creating, modifying, and regulating rules or policies for resources. The RCM identifies the relationship between message and FCs using interest attributes and creates rules that provide access to the message in the OSN (e.g., only a specific set of users or friends cluster (FC) access the published message). Moreover, these rules are stored in the rules database (rules DB) for future use. Finally, the message will be a tag to the selected FC. The RCM methodology is elaborated in Section 3.2. The transferring of owner permission on a resource to another user is called delegation. If a delegation request is received by the delegation manager (DM) and checks whether the rule/policy exists, it will send this rule/policy to the RCM. If a rule/policy does not exist, then DM checks the given criteria. Finally, the delegation manager permitted or denied it based on the criteria. The detailed process of the DM is explained in Section 3.2.

3.1. Parser Manager. The parser manager processes message m in order to drive useful features that are required to map users in friends' categories. To do so, it performs NLP-based operations on the message contents which are illustrated in Figure 2. These operations are (i) NEs (Name Entities Recognition), for example, organization, locations, person names, time, date, money, and percent, and (ii) NLP tokenization that refers to notions (e.g., a noun, pronoun). Our system depends on NEs (Named Entity) recognition libraries [63], which are capable to recognize named entities and categorize them into seven classes. As a result of this process, the parser manager identifies the attributes that reflect specific categories of users from the message. In the case of nil categories, the parser manager executes the next step. For the next step, our system relies on a set of NLPs (natural language processing) libraries [64] also known as NLP libraries.

3.2. Rule Creation Manager. The purpose of RCM is to create a rule for user clusters based on the relationship between the friends' cluster (FC) and message. Moreover, these rules are used in the future. To do so, our system administers access to the published resources according to the relationship between the resources and the friends' clusters (FCs). The RCM receives attributes that drive useful features from the message and reflect specific categories of users from the parser manager and the clusters from the ICM manager for its operation. If RCM receives more than one cluster, then a union of clusters (an instance of merging two or more

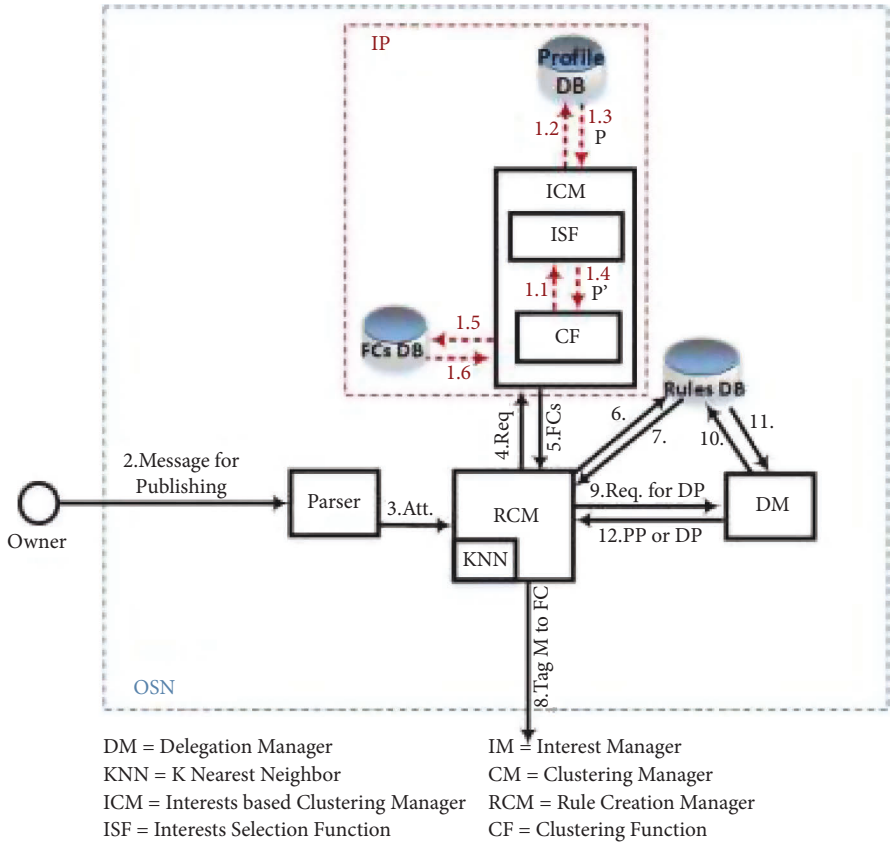

Figure 1: System diagram.

clusters into one) will be obtained, and forming a new cluster and permit/allow rule will be created. An example of allowing/deny rule is as follows:

$$\text{Rule} = \langle RO, FCi, Ri, P \rangle, \quad (1)$$

where RO is the resource owner, FC_i is the selected friends' cluster, R_i is the text resource (message), and P is the permission that may be allowed or denied. Finally, according to the selected policy, message M is tagged to the designated friends' cluster. If a delegation request is received, the delegation manager (DM) checks the relationship between FC and resource with the delegator and delegatee, respectively. If the criteria meet, allow rule/policy will be created; otherwise, deny rule/policy will be applied. If the RCM does not find attributes-related clusters, it sends these attributes to the KNN algorithm for further processing. The system initialized KNN (K-nearest neighbor) training on profile data at the beginning of the system and repeats whenever a new user is added. Due to this process, the KNN training is updated. The parser sends the message attributes to the RCM. Before sending, the RCM applies KNN (K-nearest neighbor) matching function on message attributes and finds the nearest cluster. If the nearest cluster exists, the rule creation module will create the rule for the cluster. The system will forward the cluster list to the owner if no cluster is found. The owner will check the cluster, and the rest of the procedure will be the same as previously mentioned.

4. Result and Discussion

In this section, we executed the experiments to compute all the baseline probabilities, and finally, the overall system worked as intended and showed the results.

Step 1. : Interest-based clustering

The dataset is based on "Bank Marketing" data and taken from a famous data science website [65]. The selected columns from the dataset used for the experiment are shown in Table 1. The proposed method is developed in Python and executed in Jupiter Notebook. The point of interest is three fields/columns (like Job, marital, and education), which are most related to OSN user profile data. NLTK toolkit function is used for the text cleaning process. It is a process in which most of the string is transformed to lowercase and then removes all types of stop-words like (i) language stop-words such as article, punctuation, preposition, pronoun, and conjunction (the, a, on, of, etc.), (ii) location stop-words (City and Country names, etc.), (iii) time stop-words such as name of the days and months (May, June, Monday, Today, etc.), and (iv) numerals stop-words such as hundred, thousand. After text cleaning finally, common interests are obtained from each corpus one by one using Algorithm 1.

```
(1)   reviews = read (Profile-data)
(2)   input S [i]//Select Req. Columns
(3)   for i in range (0, len (S [i])):
(4)         rev_i = read S [i] from reviews
(5)         for j in range (0, len (rev_i)):
(6)                                word.lower ()
(7)                                corpus_i.append (word)
(8)         end for
(9)         ISF (corpusi)//Define function
(10)        di = dict ()//initialize dictionary
(11)        for word in corpus_i
(12)                               if word in d_i
(13)                                                d_i [word] = d_i [word] + 1
(14)                                  else
(15)                                                d_i [word] = 1
(16)                               end if
(17)        end for
(18)        interest_i = convert d_i to array
(19)        return interesti, corpusi
(20)        end function
(21)        CF (interest_i, corpus_i)//Define function
(22)        C_i = []//initialize cluster array
(23)        for line in corpus_i:
(24)                               for word in range (0, len (interest_i)):
(25)                                                if line = = interest_i [word]
(26)                                                                    C_i.append (word)
(27)                                                end if
(28)                               end for
(29)        end for
(30)        R = reviews ['Cluster' i] = C_i
(31)        return R
(32)        end function
(33)  end for
```

Algorithm 1: Interest-based clustering.

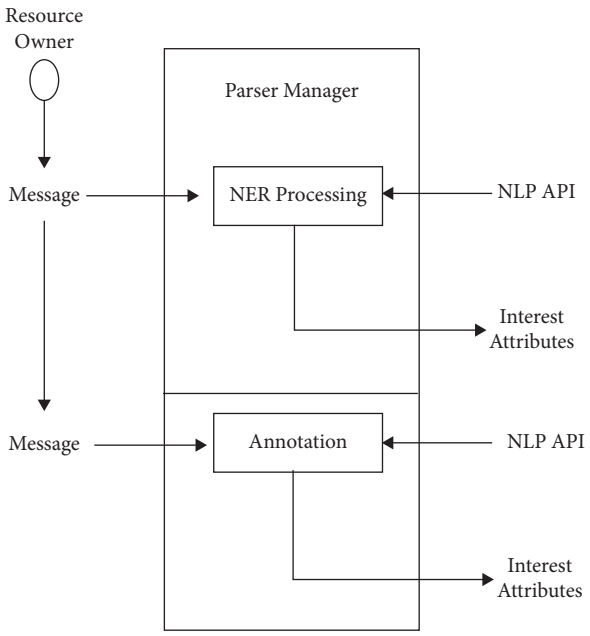

Figure 2: NLP-based operation.

Figures 3–5 illustrate the interest categories extracted from the job, marital, and education fields.

Based on the above interests, Algorithm 1 creates interest-based user clusters. According to Figure 6, the y-axis shows cluster numbers, and the x-axis shows interests. For example, the unemployed persons exist in cluster 0, those who provide services exist in cluster 1, those who do management jobs exist in cluster 2, and so on. In Figure 6, clusters 0 to 11 are based on jobs, whereas in Figure 7, clusters are based on marital status; for example, married persons exist in cluster 12, unmarried persons exist in cluster 13, and divorced persons exist in cluster 14. Similarly, in Figure 8, clusters are based on education; for example, the primary pass person exists in cluster 15, and the unknown education person exists in cluster 18.

Step 2. : Parsing manager

When the parser manager receives the owner message "M," the parser first applies the NER function and searches Person, Location, Date, Time, and Organization. Suppose the parser finds interest attributes and sends them to the RCM. If the RCM (Rule Creation Manager) finds the related

Table 1: The database used for the experiment.

Job	Marital	Education
Unemployed	Married	Primary
Services	Married	Secondary
Management	Single	Tertiary
Management	Married	Tertiary
Blue-collar	Married	Secondary
Management	Single	Tertiary
Self-employed	Married	Tertiary
Technician	Married	Secondary
Entrepreneur	Married	Tertiary
Services	Married	Primary
Services	Married	Secondary
Admin	Married	Secondary
Technician	Married	Tertiary
Student	Single	Secondary
Blue-collar	Married	Secondary
Management	Married	Tertiary
.	.	.
.	.	.
.	.	.

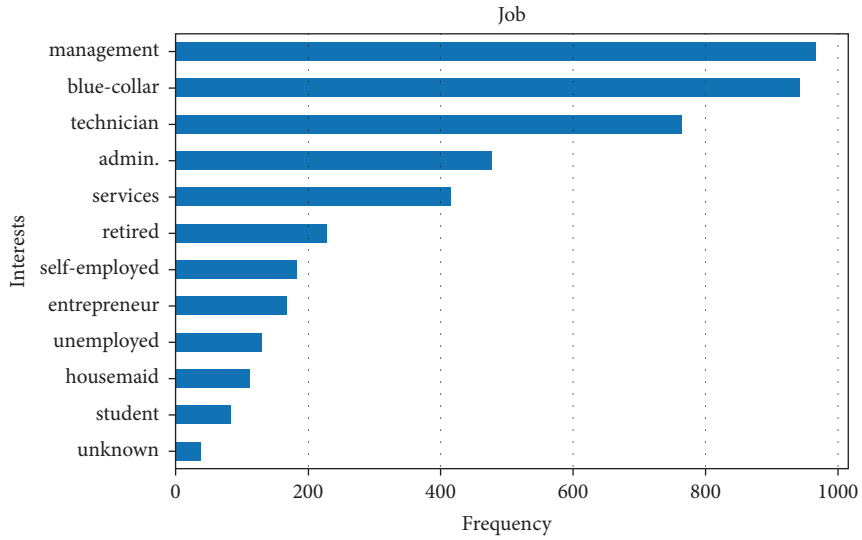

Figure 3: Job-related interests and frequency.

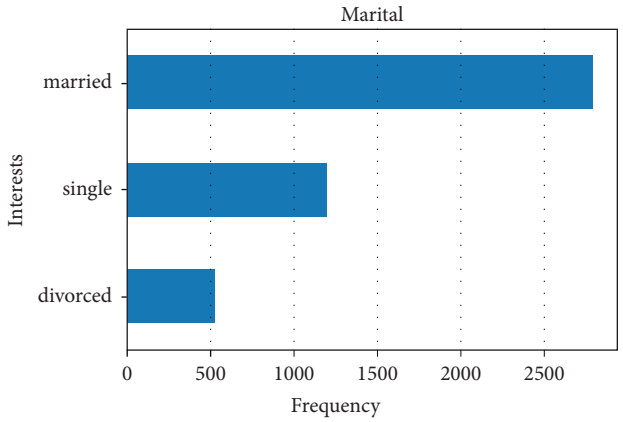

Figure 4: Marital-related interests and frequency.

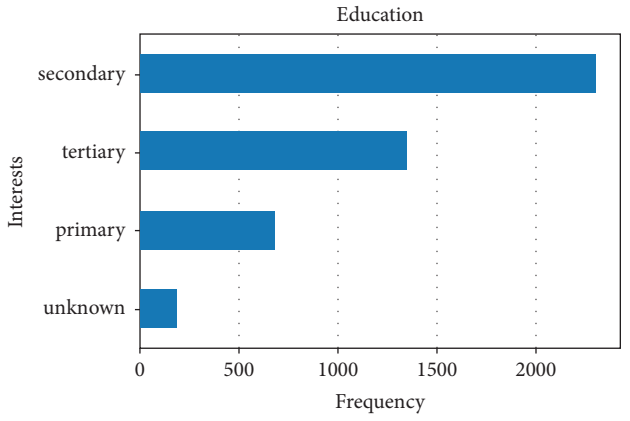

Figure 5: Education-related interests and frequency.

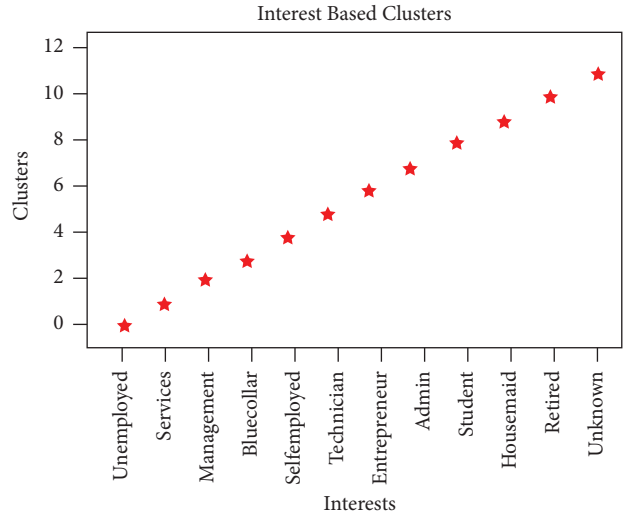

Figure 6: Interest-based clusters from 0 to 11.

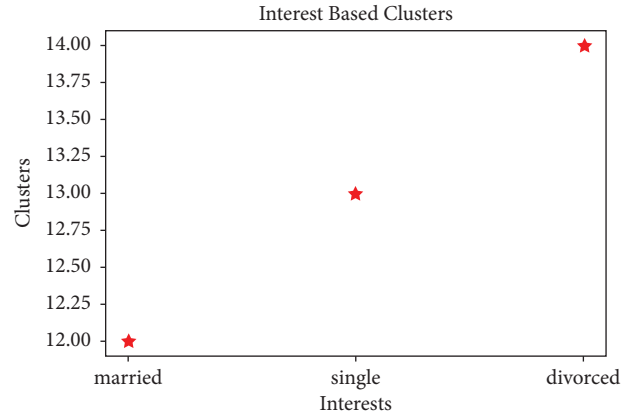

Figure 7: Interest-based clusters from 12 to 14.

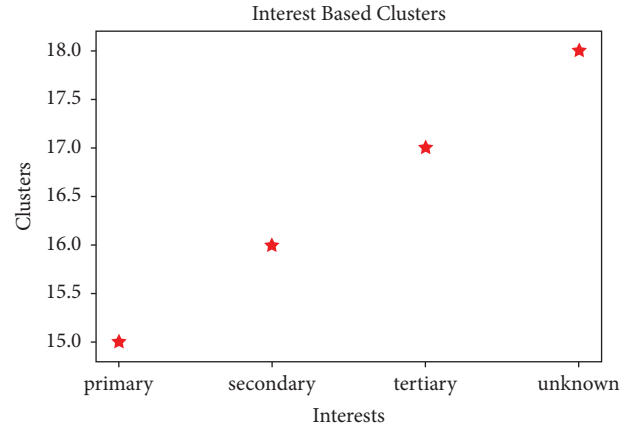

Figure 8: Interest-based clusters from 15 to 18.

clusters, then it will send these clusters for rule creation. If no attributes are found, the parser manager applies another NLP function over the message. The NLP function tokenizes the message "*M*." Based on these tokens, proper nouns and nouns are extracted and sent to the RCM for further processing. For example, a message found or received "Married person party on Monday." The NLP and NER function results are shown in Figures 9 and 10. The selected interest attributes are married, person, and party. Finally, the parser sends these interest attributes to the RCM.

In another example, a Message "'Interviews for primary pass candidates on Friday" is extracted. The NLP and NER function results are shown in Figures 11 and 12. The selected interest attributes are interviews, primary, pass, and candidates. Finally, the parser sends these interests (or interest attributes) to the RCM. The result of NLP tokenization is as follows.

Step 3. Rule creation manager

The purpose of RCM is to create a policy for clusters based on the relationship between the selected cluster and the message. The RCM sent cluster requests to the CM based on received attributes from the parser. According to example 1, the RCM receives three interest attributes married, person, and party. After cluster matching, the RCM gets cluster 12 or FC12, created based on married users. The RCM creates a permit rule for FC12 and finally tags the message to FC12. According to example 2, the RCM receives four interest attributes: interviews, primary, pass, and candidates. After cluster matching, the RCM gets cluster 15 or FC15, created based on primary pass users. The RCM creates a permit rule for FC15 and finally tags the message to FC15.

4.1. Training and Testing of KNN Matching Function. For the training purpose, the dataset is based on "Bank Marketing" data and taken from a famous data science website [65]. The selected columns (fields) from the dataset are shown in Table 1. The point of interest is three fields/columns (like Job, marital, and education), which are most related to OSN user profile data. The training and testing of the KNN matching function consist of the following steps:

(i) Import and handling of the dataset
(ii) The KNN algorithm is used from the Sci-Kit-learn package
(iii) Divide the dataset into test and training data
(iv) Find the *k*-nearest neighbor values
(v) Train the data into the model
(vi) Evaluating the accuracy

In step 1, the required dataset is imported, and then select relevant columns (fields) and convert these columns into numeric coding using label encoding from SK-learn. In step 2, import the KNN package from SK-learn. In step 3, the dataset is divided into test and training splits to avoid overfitting and better understand how our KNN function performed in the testing stage. Through this method, our function is tested on anonymous data. We use this data in the following manner: (i) 20% of the data are used for testing purpose, and (ii) 80% of the data are used for training purpose. In step 4, the system finds the *k*-nearest neighbor points, and in step 5, we train the model using the chosen dataset, and finally, in step 6, we evaluate the accuracy of the

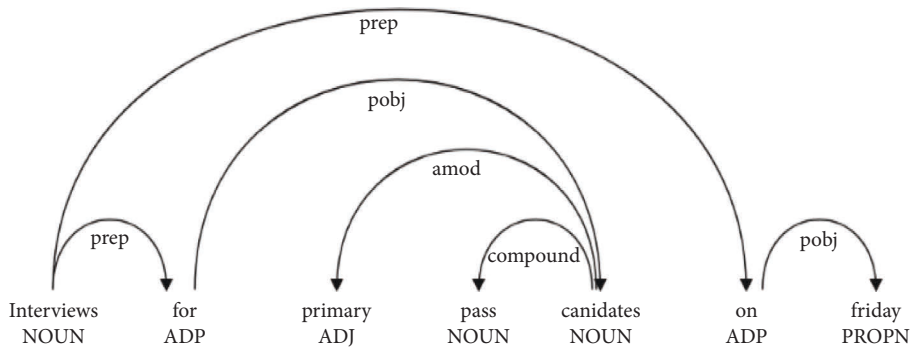

Figure 9: NLP tokens.

Interviews for primary pass canidates on friday DATE

Figure 10: NER token.

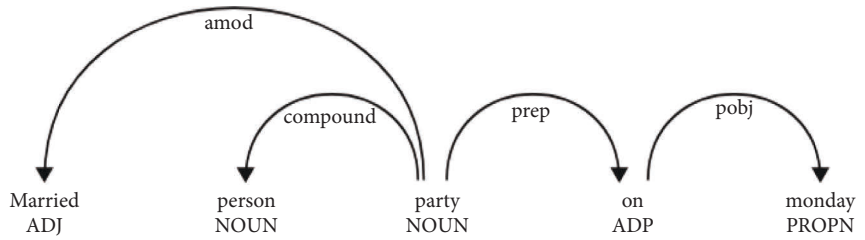

Figure 11: NLP tokens.

Married person party on monday DATE

Figure 12: NER tokens.

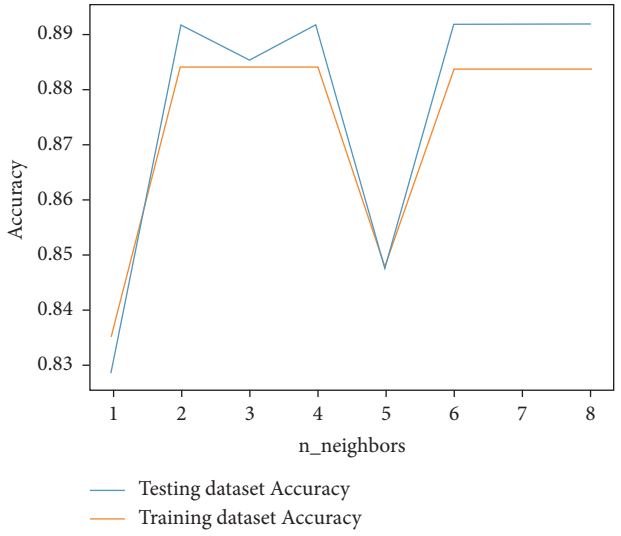

Figure 13: KNN accuracy.

training data and testing data. After training the KNN algorithm on our dataset, the results are as follows. The graph between accuracy and the number of neighbors obtained from the training dataset is mentioned in Table 1. According to Figure 13, the x-axis shows the n neighbors, and the y-axis shows the accuracy level whereas the training dataset accuracy is shown in the orange color line and the blue color line shows the testing dataset accuracy.

5. Conclusion and Future Work

This research article presented a dynamic and automated access control system in OSN for textual resources and publications. Our proposed system is content-driven, and the ideas behind the semantics of the messages are automatically evaluated to identify the interests and select the user clusters (FC) based on these interests. Finally, create a permit rule for selected user clusters (FC) based on the relationship message and FC. The delegation is automatically allowed/permitted based on the following three criteria: (i) the requester must be a member of a related FC, (ii) the delegatee and message must have the same relationship as the message and FC, and (iii) the delegatee and owner must have the same relationship as FC and owner. If the above criteria are met, delegation is permitted; otherwise denied. We have successfully implemented and evaluated each module and initial testing of our proposed concept. Finally, we have enumerated some future work for our model. The delegation module will be implemented and tested. Furthermore, interest selection and rule creation procedures will be improved.

Data Availability

The Bank Marketing dataset used to support the findings of this study is freely available from the Kaggle website by using the following link: (https://www.kaggle.com/datasets/janiobachmann/bank-marketing-dataset.).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors acknowledge Foundation University Islamabad for its support to conduct this research work.

References

[1] Zephoria, *The Top 20 Valuable Facebook Statistics*, Zephoria, Paris, France, 2020.

[2] TwitterTwitter Usage/Company Facts, San Francisco, CA, USA, 2017.

[3] E. Protalinski, *56% of Employers Check Applicants' Facebook, LinkedIn, Twitter*, ZED net, San Francisco, CA, USA, 2012.

[4] H. Kelly, *Police Embrace Social media as a Crime-Fighting Tool*, CNN.com, Atlanta, Georgia, 2012.

[5] L. A. Cutillo, R. Molva, and T. Strufe, "Safebook: a privacy-preserving online social network leveraging on real-life trust," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 94–101, 2009.

[6] J. Brenner and A. Smith, *72% of Online Adults Are Social Networking Site Users*, Pew Internet & American Life Project, Washington, DC, USA, 2013.

[7] E. Fix and J. L. Hodges, "Discriminatory analysis. Nonparametric discrimination: consistency properties," *Randolph Field, Texas, Tech. Report*, USAF School of Aviation Medicine, vol. 4, , pp. 1–21, 1951.

[8] B. V. Dasarathy, *Nearest Neighbour (NN) Norms: NN Pattern ClassificationTechniques*, IEEE Computer Society Press, DC, USA, 1991.

[9] D. Wu, B. Liu, Q. Yang, and R. Wang, "Social-aware cooperative caching mechanism in mobile social networks," *Journal of Network and Computer Applications*, vol. 149, Article ID 102457, 2020.

[10] J. Xiong, X. Chen, Q. Yang, L. Chen, and Z. Yao, "A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2347–2360, 2020.

[11] F. Li, H. Li, B. Niu, and J. Chen, "Privacy computing: concept, computing framework, and future development trends," *Engineering*, vol. 5, no. 6, pp. 1179–1192, 2019.

[12] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71–80, Alexandria, Virginia, USA, November 2005.

[13] J. Xiong, R. Ma, L. Chen et al., "A personalized privacy protection framework for mobile crowdsensing in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4231–4241, 2020.

[14] G. Liu, Q. Yang, H. Wang, and A. X. Liu, "Three-valued subjective logic: a model for trust assessment in online social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 994–1007, 2021.

[15] J. Xiong, J. Ren, L. Chen et al., "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1530–1540, 2019.

[16] M. Imran-Daud, D. Sánchez, and A. Viejo, "Privacy-driven access control in social networks by means of automatic semantic annotation," *Computer Communications*, vol. 76, pp. 12–25, 2016.

[17] A. Outchakoucht, H. Es-Samaali, and J. Philippe, "Dynamic access control policy based on blockchain and machine learning for the internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 7, 2017.

[18] A. S. M. Kayes, W. Rahayu, and T. Dillon, "Critical situation management utilizing IoT-based data resources through dynamic contextual role modeling and activation," *Computing*, vol. 101, no. 7, pp. 743–772, 2019.

[19] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," *ACM SIGCOMM - Computer Communication Review*, vol. 40, no. 1, pp. 112–117, 2010.

[20] J. Lindamood, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, *Inferring Private Information Using Social Network Data*, in *Proceedings of the 18th international conference on World wide web*, pp. 1145-1146, Madrid Spain, April 2009.

[21] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[22] N. Boustia and A. Mokhtari, "Representation and reasoning on ORBAC: description logic with defaults and exceptions approach," in *Proceedings of the third International Conference on Availability, Reliability and Security*, pp. 1008–1012, Barcelona, Spain, March 2008.

[23] L. Wang, Zhu, J. Yanqin, L. Luo, and Xizhao, "Trust mechanism in distributed access control model of P2P networks," in *Proceedings of the IEEE/ACIS*, pp. 19–24, Portland, OR, USA, May 2008.

[24] R. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 40–48, 1994.

[25] S. Gusmeroli, S. Piccione, and D. Rotondi, "IoT access control issues: a capability-based approach," in *Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 787–792, Palermo, Italy, July 2012.

[26] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[27] V. C. Hu, D. F. Ferraiolo, D. R. Kuhn, A. R. Friedman, and A. J. Lang, "Guide to attribute based access control (ABAC) definition and considerations," *NIST Special Publication*, vol. 800, no. 162, pp. 1–54, 2013.

[28] A. Sharma, D. Srinivasan, and D. S. Kumar, "A comparative analysis of centralized and decentralized multi-agent architecture for service restoration," in *Proceedings of the CEC*, pp. 311–318, Vancouver, BC, Canada, November 2016.

[29] J. R. Lincoln, B. Wellman, and S. D. Berkowitz, "Social structures: a network approach," *Administrative Science Quarterly*, vol. 35, no. 4, p. 746, 1990.

[30] L. Q. Tian and C. Lin, "A kind of game-theoretic control mechanism of user behavior trust based on prediction in a trustworthy network," *Chinese Journal of Computers*, vol. 30, no. 10, pp. 1930–1938, 2007.

[31] J. Yu, Y. Wang, J. Li, H. Shen, and X. Cheng, "Analysis of competitive information dissemination in social network based on evolutionary game model," in *Proceedings of the International Conference on Cloud and Green Computing*, pp. 748–753, Xiangtan, China, November 2012.

[32] P. Zhu, G. Wei, A. V. Vasilakos, and H. Y. Wei, "Knowledge sharing in social network using game theory," in *Proceedings of the International Conference on Bio-Inspired Models of Network, Information, and Computing Systems*, pp. 13–27, MA, USA, December 2010.

[33] F. Shan, J. Liu, X. Wang, W. Liu, and B. Zhou, "A smart access control method for online social networks based on support vector machine," *IEEE Access*, vol. 8, pp. 11096–11103, 2020.

[34] O. Bodriagov, G. Kreitz, and S. Buchegger, "Access control in decentralized online social networks: applying a policy-hiding cryptographic scheme and evaluating its performance," in *Proceedings of the PERCOM WORKSHOPS*, pp. 622–628, Budapest, Hungary, May 2014.

[35] G. Pang and K. Zhang, "Estimation of asymptotic stability regions via composite homogeneous polynomial Lyapunov functions," *International Journal of Control*, vol. 88, no. 3, pp. 484–493, 2015.

[36] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Working Papers*, Article ID 21260, 2008.

[37] D. G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," *EIP-150 REVISION*, 2017.

[38] K. Croman, C. Decker, I. Eyal, A. E. Gencer, and A. Juels, "On scaling decentralized blockchains," in *Proceedings of the International Financial Cryptography Association Workshops*, vol. 9604, pp. 106–125, Barbados, February 2016.

[39] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.

[40] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," *Advances in Intelligent Systems and Computing*, vol. 520, pp. 523–533, 2017.

[41] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain-based access control," *Proceeding of the IFIP*, vol. 10320, pp. 206–220, 2017.

[42] L. P. Kaelbling, M. L. Littman, and A. W. Moore, "Reinforcement learning: a survey," *Journal of Artificial Intelligence Research*, vol. 4, pp. 237–285, 1996.

[43] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.

[44] C. Dukkipati, Y. Zhang, and L. C. Cheng, "Decentralized, BlockChain based access control framework for the heterogeneous internet of things," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, pp. 61–69, AZ USA, March 2018.

[45] D.F. Maesa, P. Mori, and L. Ricci, "A blockchain-based approach for the definition of auditable Access Control systems," *Computers & Security*, vol. 84, pp. 93–119, 2019.

[46] S. Shafeeq, M. Alam, and A. Khan, "Privacy-aware decentralized access control system," *Future Generation Computer Systems*, vol. 101, pp. 420–433, 2019.

[47] J. M. Such and N. Criado, "Multiparty privacy in social media," *Communications of the ACM*, vol. 61, no. 8, pp. 74–81, 2018.

[48] H. Hu, G. J. Ahn, and J. 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.

[49] L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based collaborative privacy management in online social networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 48–60, 2019.

[50] H. Alshareef, R. Pardo, G. Schneider, and P. Picazo-Sanchez, "A collaborative access control framework for online social networks," *Journal of Logical and Algebraic Methods in Programming*, vol. 114, Article ID 100562, 2020.

[51] P. W. L. Fong, M. Anwar, and Z. Zhao, "A privacy preservation model for facebook-style social network systems," *Proceeding of the ESORICS*, vol. 5789, pp. 303–320, Berlin, Heidelberg, 2009.

[52] C. Gates, "Access control requirements for web 2.0 security and privacy," *IEEE Web*, vol. 2, pp. 12–15, 2007.

[53] B. Carminati and E. Ferrari, "Enforcing relationships privacy through collaborative access control in web-based Social Networks," in *Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 1–9, DC, USA, November 2009.

[54] P. W. L. Fong, "Relationship-based access control: protection model and policy language," in *Proceedings of the CODASPY*, pp. 191–202, San Antonio, Texas, USA, February 2011.

[55] P. W. L. Fong and I. Siahaan, "Relationship-based access control policies and their policy languages," in *Proceedings of the SACMAT*, pp. 51–60, Innsbruck, Austria, June 2011.

[56] G. Bruns, P. W. L. Fong, I. Siahaan, and M. Huth, "Relationship-based access control: its expression and enforcement through hybrid logic," in *Proceedings of the CODASPY*, pp. 117–124, San Antonio, Texas, USA, February 2012.

[57] J. Park, R. Sandhu, and Y. Cheng, "A user-activity-centric framework for access control in online social networks," *IEEE Internet Computing*, vol. 15, no. 5, pp. 62–65, 2011.

[58] Y. Cheng, J. Park, and R. Sandhu, "Relationship-based access control for online social networks: beyond user-to-user relationships," in *Proceedings of the International Conference on Privacy, Security, Risk and Trust and 2012 International Conference on Social Computing*, pp. 646–655, Amsterdam, Netherlands, September 2012.

[59] S. Abid and I. Daud, "Automated and dynamic access control management in OSN," in *Proceeding of the ICIC*pp. 1–6, Lahore, Pakistan, 2021.

[60] Y. Cheng, J. Park, and R. Sandhu, "An access control model for online social networks using user-to-user relationships," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 4, pp. 424–436, 2016.

[61] A. K. Malik, N. Emmanuel, S. Zafar et al., "From conventional to state-of-the-art IoT access control models," *Electronics*, vol. 9, no. 10, p. 1693, 2020.

[62] D. Ventura, A. Gomez-Goiri, V. Catania, D. López-De-Ipiña, J. A. M. Naranjo, and L. G. Casado, "Security analysis and resource requirements of group-oriented user access control for hardware-constrained wireless network services," *Logic Journal of IGPL*, vol. 24, no. 1, pp. jzv045–91, 2015.

[63] Stanford Nlp Group, *Stanford Named Entity Recognizer (Ner)*, Stanford NLP Group, CA, USA, 2014.

[64] A. Open Nlp, *Open NLP*, 2010.

[65] M. Sergio, P. Cortez, and P. Rita, "A data-driven approach to predict the success of bank telemarketing," *Decision Support Systems*, vol. 62, no. 1, pp. 22–31, 2014.