Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3 (2025)

Cluster Analysis for Assisted Healthcare Approval in Pervasive Social Networks

Vishnu Kumar Kaliappan[1], S.Vinoth Kumar[2], Dharani Jaganathan[3], S.Ilavarasi[4], Dhanasekaran Pachiyannan[5]

[1]Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India. 641407. vishnudms@gmail.com

[2]Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu - 600062, India.

profsvinoth@gmail.com

[3]Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu 641407, India. dharaninagan92@gmail.com

[4]Department of Computer Science and Engineering,Sengunthar Engineering College (Autonomous) Tiruchengode, Tamil Nadu, India. ilavaishu@gmail.com

[5]Department of Electronics and Communication Engineering, The Kavery Engineering College, Mecheri, Salem.Tamilnadu-636453, India.dhanawaves@gmail.com

Article History:

Received: *07-08-2024*

Revised: *28-09-2024*

Accepted: *09-10-2024*

Abstract:

The idea of pervasive social network (PSN)-based healthcare is prompted by contemporary wireless sensing and mobile computer technology. The main challenge is how a PSN node may safely transmit health information to other nodes in the network to implement the notion. In this research, we suggest a safe PSN-based health service. With its assistance, we were able to develop the subject category infrastructure to recognise the top research fields, the research electricity network to identify the most productive countries and institutions, the journal co-citation map to identify the distribution of core journals, the author co-citation map to identify significant investigators and their co-citation trends, and the manuscript co-citation network to expose the cutting-edge literature and identify co-citation groupings on pervasive technologies.

Keywords: pervasive social network (PSN); cluster; Healthcare; Social networks; middleware deployments; pervasive computing;

1. INTRODUCTION

In the twenty-first century, innovative paradigms for computer models are being introduced by the developing field of research known as ubiquitous and pervasive computing. The second and third waves of computing, respectively, were distributed mobile computing. In actuality, ubiquitous and pervasive computing is a post-desktop style of human-computer interaction where huge data has been thoroughly ingrained into routine objects and actions. The phrase "ubiquitous computing," which was first used to describe ideas, served as the inspiration for pervasive computing. According to Weiser's seminal article, pervasive computing (or ubicomp) is a computer ecosystem where compute clusters blend in with daily life and disappear into the backdrop. Its first iteration took the shape of "buttons," "pad," and "board" created at Xerox PARC between 1988 and 1994.

A wide range of research topics, including reduced wattage, incorporated innovations, embedded devices, portable devices, wireless and portable connectivity, development tools, interfaces, software, assistance, security, confidentiality, and so on, have been driven by pervasive and ubiquitous coding, a cross-disciplinary field with enormous potential. It has advanced quickly in terms of theory and practical application after many decades of development. Due to the fact that, according to earlier studies, very few studies have examined the research status quo of pervasive and ubiquitous computer science in a thorough and comprehensive research methods, we need to analyse papers on pervasive and ubiquitous computer science from the WoS over the past 15 years to gain understanding into its development stage in general [1].

In their daily lives, people connect with one another in a variety of different relationships. They would also make use of a variety of intelligent IoT applications and services to enhance their quality of life. As a result, the effectiveness of those products and apps rests on their ability to meet the demands that are motivated by interpersonal relationships. Additionally, the interaction with people in a connection tied to service results in a high degree of practical correctness for each demand. As was already said, in IoT, users connect via legacy networks. In contrast, groups of things work together online to share data with intelligent applications and services that each user utilizes. As a result, the IoT employs two paradigms of interaction: thing-to-thing and human-to-human. Humans only use the data obtained from things like the customer model from the past. It implies that IoT has not yet adopted a true human-to-thing link necessary for true ubiquitous computing [2].

These are the study's goals:

- *to analyze the range of subject areas covered by pervasive and ubiquitous computer development;*
- *to identify the nation's, institute's, and individuals' most viable research laborers;*
- *to determine the distribution of key publications on ubiquitous and pervasive computers;*
- *by examining the document co-citation networks, analyse the main research themes in the field of pervasive and ubiquitous computing;*

The following is how the essay's succeeding sections are structured. The research on the pertinent older works is presented in Section 2. The characteristics of the proposed system, including its proposed system architecture, implementation model, graph-based approach components, and data analysis, are described in Section 3. In Section 4, the system's efficacy is evaluated, and the setting for its deployment is presented. The resolution is presented in Section 5.

2. RELATED WORKS

Kasim, N. M., Fauzi et.al [3] Typically, an employee uses social media (SM) while at work for one of two main reasons: personal or professional. Although the necessity of using social media for work-related purposes has been acknowledged by academics, multiple studies have also revealed the detrimental effects of SM use on employee results. At first, using social media for work reasons boosts employee morale, but overusing it can have a detrimental impact on both productivity and motivation. Additionally, the frequent use of social media during work hours may inadvertently create a stressful atmosphere there. Additionally, employees who use social media for employment, particularly after regular working hours, may find it harder to devote the necessary time and energy

to fulfilling the demands of their life roles. This could eventually lead to conflicts between their work and personal lives that are effort-based.

Yan, Z., & Wang, M et.al [4] Users with permissions are the only ones who can decode encrypted data thanks to access control. To ensure that each user can only decode the material that has been granted to them, it is best to encrypt each piece of information only once and send the necessary keys to each user only once. As was already stated, in order to maintain the necessary level of security in PSN due to the shifting user membership and trust connections, the decryption needs to be changed constantly. Pure symmetric key-based encryption and public key encryption are not the best options for PSN, particularly for quickly socialising in a group. Distributed key management of symmetric keys is difficult, strictly speaking. Using pure symmetric key cryptography for data access control makes it impossible to implement various restrictions, whereas public key-based encryption is ineffectual for multicasting data to a number of users. The data owner must encrypt the keys or data in order for correctness.

Yan, Z., Kantola, R., Shi, G., & Zhang et.al [5] it was suggested filtering spam using a reporter-based reputation system. A trust-maintenance component of the system allows users to improve or degrade their reputation depending on how frequently they report spam. This method of managing trust depends on a centralized component; it cannot be used in the PSN environment directly. Other spam management solutions, such as MailTrust, which detects spammers based on email originator behavior and employ a different system architecture or methodologies from our solution, and provide a multi-level prestige grey-listing remedy, albeit sharing some characteristics with it. In contrast to the study mentioned above, in addition to traffic and activity analysis, user or node concerns are taken into account when determining how trustworthy our system is.

Zhou, J., Sun, J., Athukorala, K., Wijekoon, D et.al [6] A ubiquitous social application's capacity for behavior awareness is its capacity to observe participants' actions or social cues, to discern their intentions, and to react by offering the users' preferred services. Community awareness refers to an application's capacity to identify, explore, and grow users' social communities in light of their issues. By providing users with all forms of information pertinent to their interests, community awareness enhances their social element. Pervasive social software with interaction awareness can recognize trends in how users interact with their physical and virtual settings and adjust their communication style accordingly. A pervasive social application's capacity to enhance users' aggregated media content to broaden and improve their social experience is known as content awareness.

Mokhtar, S. B., McNamara, L., & Capra, L et.al [7] in this research, we provide a middleware application for social computing it enables the PSN vision of semi-distribution. Each records frequent interactions with other mobile devices that are located using Bluetooth radio communication. During times of colocation, middleware, hosted on a collection of nodes known as brokers, automatically compiles these logs in addition to user interests and related social networks. Brokers share the data they have gathered and use social network propagation techniques to infer the existence of any social links that may be missing. Brokers then utilize that score to give users personalized suggestions by computing a similarity measure that takes into account both social and geographic proximity information between users. In this study, we do not investigate ways to protect users' social network privacy; we also do not comment on brokers' election tactics that depend on

brokers' reliability; and we do not explore incentive systems for nodes to participate as brokers. Both issues are on our radar, and they will be looked into in the future.

Ben Mokhtar, S., & Capra, L et.al [8] by considering their social connections and recommending other users who have similar interests to them, we hope to help users complete their daily duties. Because of the nature of the projects we are contemplating, only users in the same area can contribute to their completion. We require software that supports; to enable this type of technology-mediated social involvement. Users' tasks are realized through social-based similarity to increase customer satisfaction, (2) user tasks are realized through the semantic specification of their people's preferences and tasks to enable unambiguous reasoning on users' prerequisites, (3) user tasks are dynamically propagated in the network to increase the likelihood of finding suitable matches.

Raatikainen, K., Christensen, H. B., & Nakajima et.al [9] collaborate closely with hospital physicians since testing prototype solutions in real-world environments are one of the pillars of our experimental research. Clinicians play a significant role in the process of conceptualizing, designing, and testing ideas for potential pervasive computer support in the future. Easy access to online health information (EPR) systems has been a major priority. A good testing ground for pervasive middleware systems is the healthcare industry. First, the movement that distinguishes modern hospitals for healthcare is severe and doctors are on the go virtually continuously. Second, very few medical professionals even have a desk or a spot to put a device.

3. METHODS AND MATERIALS

To ascertain how closely two users are related in both the social network and the physical proximity network, respectively, we first provide the models for both networks in this section. We next give an example of how our PSN software service integrates these variables into a user’s similarity measure that will be employed to suggest individuals to one another. Before assessing them in the following part, we finally talk about several middleware service deployment choices.

Threat and system modeling:

We take into consideration a PSN system that consists of two different types of entities, as shown in Figure 3.1: PSN nodes that interact with one another to facilitate pervasive social communication systems and a PSN that possesses capabilities and features that PSN nodes don't have and is dependable for providing online social networking support, individuality, and key distribution, and confidentiality. It is capable of gathering adequate data to carry out precise trust analysis [4]. It is necessary to secure communications data protection in PSN across its nodes because some ubiquitous social communications depend on their authenticity and secrecy. In a number of situations, PSN nodes may use the Internet or mobile Internet to retain ids, keys, and trust models for providing secure PSN connections, saving computation resources and processor loads. Nodes can identify one another using aliases to ensure the integrity and privacy of PSN communications. Another area of our research involves anonymized identification in PSN, and this work is described in a different paper.

By implementing secure data protection technologies, we presume that is dependable and trustworthy for maintaining nodes' private records. The existence of corporate incentives is the basis of this

presumption. On the TS, there should be plenty of storage and processing power. Even though a PSN node's existence is not necessary for PSN interactions, it is feasible for nodes to enroll themselves into the network. Applying an existing security protocol, such as security socket layer, protects interactions between the networks and SSL. Each node registers with a special identification number, which can map to the node's present PSN identity. The nodes might not have mutual trust. Some nodes might purposefully spy on PSN communications to benefit themselves. Social interactions between reliable nodes are anticipated. Additionally, the TS issue a secret key pair to each node at the time of node registration. If necessary for identity verification and identity, Exchanges are made with other nodes using either the public key or a derived one-off public key that matches the node identity. Due to the majority of PSN nodes being strangers, delegating is not permitted.

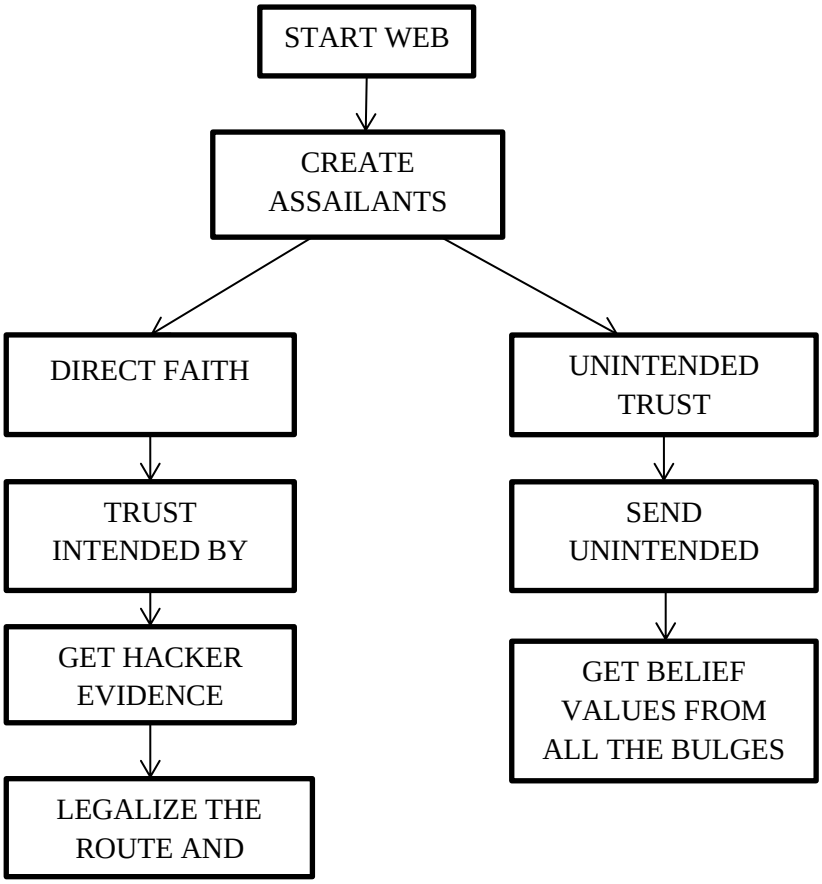

Figure 3.1 PSN's trust management system

Design Objectives:

According to the abovementioned paradigm, our solution should accomplish the essential performance and security objectives to protect PSN:

- **Adaptability and understanding:** Regardless of whether the TS is accessible or not, the system should enable PSN access control in either a centralized or decentralized fashion, or maybe both, and the administration of data access based on individual trust in PSN should be adaptable.

- **phenotypic variation:** The suggested method accommodates various PSN access control requirements, such as both general access control rules established by the TS or specific node-handled private access influencing policy;
- **protection:** Only qualifying routers that are reliable enough can obtain the PSN information; and
- **Portable:** With the least amount of communication and processing overhead, the approach protects PSN.

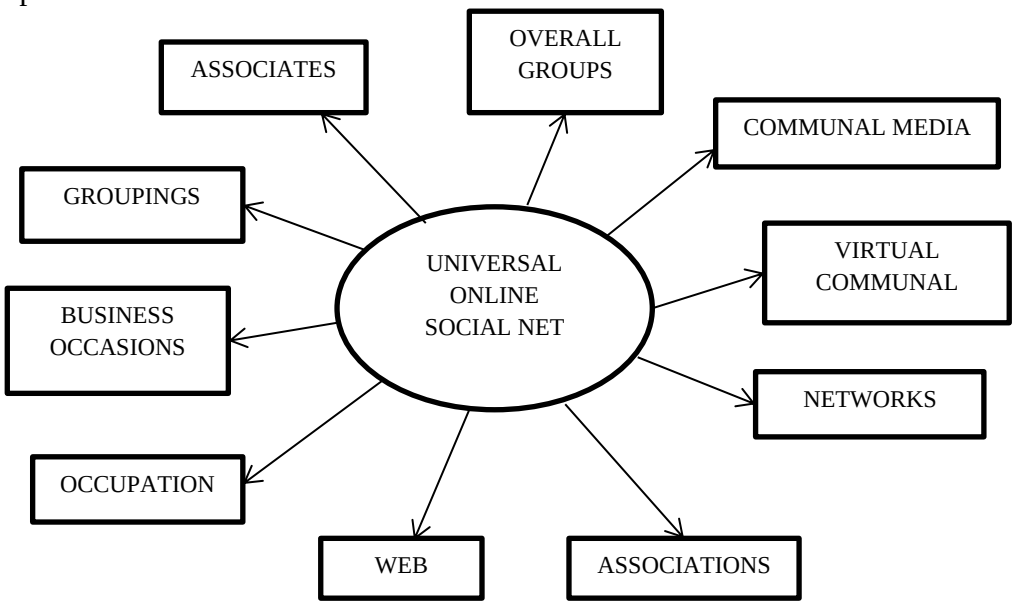

Figure 3.2 Pervasive Social Network applications

To determine whether a node lr_j^i (2... uk) has been compromised or infected, it is necessary to track its local traffic. The shifts in both outbound and incoming traffic in a node might, in turn, signal the likelihood of its invasion and disease.

$$\emptyset_L = |2 - 1g\left\{e_t\left\{lr_j^i(l) + lr_j^i(l)\right)\right| \qquad (1)$$

A node's processing activities suggest what it wants or enjoys about the insides. This evidence can be used to determine if the happy is desired, or undesirable based on individual needs. When a piece of content is received at time e_j^i and deleted at moments s_j^i, or when the node moves it to the spam box or marks it as undesirable, undesirable traffic indication L provided by the behaviour of the node digesting content is explicable as:

$$\partial_j = 2 - \frac{e_j^i - s_j^i}{L}, when\ e_j^i - s_j^i < L \qquad (2)$$

Nodes could disseminate a complaint on PSN regarding irrelevant posts. The node has the option to personally rate if the material has the potential to be undesired. Using traffic auto-monitoring and node behaviour from material processing (i.e., $s_j^i(L)$ quality) is measured. As a result, the unwanted traffic identification value s_j^i at time U_j^i by ∂_j concerning content $U_j^i(L)$ is as follows [5]:

$$s_j^i(L) = U_j^i(L) * \partial_j * \partial_i \qquad (3)$$

To regulate undesired content, we solely take into account the objective facts that are observed at the node. Technique 1 describes the algorithm employed for undesired content identification at the nodes. If the de_m^l does not file a complaint, the detecting trust de_m^l is left alone. We also add a caution indicator to track the frequency of incorrect detections to identify attackers with on-off and conflict behaviour has a starting value of 1. Each time a false detection occurs, it is raised by 0. Criterion 1 (thr1) is a marker for conflicting behaviour and on-off attacks. A variable to adjust the penalties for bad detection is 0. Based on the effectiveness of the detection, we modify φx of $(de_m^l > 2$ at time t as follows:

$$de_m^l = \{de_m^l + \varphi x(x < thr2) = \{1\ (de_m^l > 2\} \qquad (4)$$

Since attacker nodes complains should be excluded from confidence assessment, we combine complaints on de_m^l from various K1 nodes with subjective ratings using both the node trust φx and detecting trust vtl_j^i as measures of their trustworthiness in Equation (5).

$$st_m^l = \frac{\sum_{l=1}^{l1} de_m^l * vtl_{j*}^i \varphi x * \partial_i}{\sum_{l=1}^{l1} de_m^l * vtl_{j*}^i \varphi x * f} \qquad (5)$$

Similar to this, we group the complaints filed on Vt_p^l by a variety of vt_m^l customers without assigning subjective ratings as:

$$Vt_p^l = \frac{\sum_{l=2}^{l2} et_p^l * \varphi x * \partial_i}{\sum_{l=2}^{l2} et_p^l * vt_m^l} \qquad (6)$$

The development of Vt_p^l cannot be aided by l, however, if the intrusive flow from ∂_i is substantial but constant. We use Formula to figure out Vt_p^l likes for all materials supplied from L_m and for each item from $\sum_{j=1}^{lm} \partial_i$ that we calculate I to display vt_m^l hate (7).

$$\mathrm{C} = \frac{2}{L_m} \sum_{j=1}^{lm} \partial_i \qquad (7)$$

Finally, we compile the data mentioned above in order to assess vt_k^l confidence. We take into account the quantity of complaints by simulating their impact using the Rayleigh distribution function as vt_k^l. The more grievances, the more $L1 + L2$ is deducted, which is maintained in Equation (8).

$$vt_k^l = vt_k^l - \emptyset(L1 + L2)\left(\propto * st_m^l * \partial * Vt_p^l\right) - y\sqrt{} \qquad (8)$$

Where the parameters, and are weighting variables that can be adjusted by a real-world scenario. For computing vt_k^l', and st_m^l using Equation (9), we simply set and based on the amount of participating nodes.

$$\partial = \frac{L1}{L1+L2+1};\ \tau = \frac{L1}{L1+L2+1};\ \mu = \frac{L1}{L1+L2+1}; \qquad (9)$$

We perform a highly precise analysis using these data. We specify:

$$S = \frac{c}{a+b}, \qquad (10)$$

$$Q = \frac{b}{a+c} \qquad (11)$$

$$G = \frac{3QR}{Q+R} \qquad (12)$$

Ideas on ubiquitous social computing:

Figure 3.3 provides an overview of pervasive social computer technology and illustrates how it can be used to complement various human social bits of intelligence by detecting the social context of people, identifying their intentions, and then providing the preferred calculations to them as they communicate with the physical and virtual worlds. Five research areas are covered by ubiquitous social computing, including social signal analysis, multimodal human-computer interaction (HCI), networking sites, Facebook, and pervasive computing. The following are its pertinent notions [6].

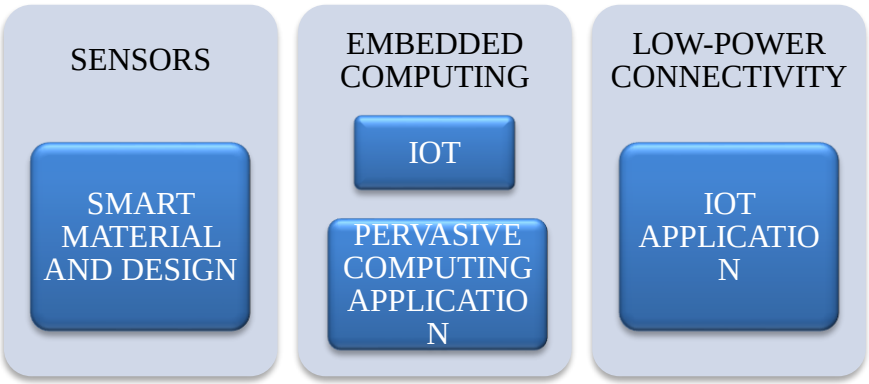

Figure 3.3 overview of pervasive social computer technology

People's perceptions of computers are altered by ubiquitous computing. Computers can blend into the background thanks to pervasive computing. Computers are made accessible across the physical environment thanks to ubiquitous computing, but people can effectively ignore them. In the future, real-time, pervasive computer systems will operate everywhere and interacts with the physical environment. Users can walk about freely while they are being followed, and they will react to any changes in their needs or the environment. Multiple new implementations have rendered the original definition obsolete. Computing the physical aspect is a popular pervasive computing feature that enables users to adapt to their physical surroundings, such as via location-based services. Social media is viewed as a way to effectively exchange and spread data via social networks and is used to aggregate diverse media sources via the Internet. The 2011 Arab uprisings and revolutions are thought to have been significantly influenced by social media. We use social media to organize the demonstrations, Twitter to coordinate them, and Video to broadcast them, as one activist in Cairo simply put it.

4. Implementation and experimental results

A customizable data access control system to safeguard PSN communication is described in this paper. We start by introducing a structure for PSN's trust management that can facilitate the implementation of the suggested scheme. Before the suggested scheme is presented, notations, preliminary steps, and definitions are discussed. Thus, the architectural implementation of PSN middleware is critical. In this research, we examine three middleware deployment approaches [7]:

Table 1 Communication Costs

	4 BROKS	5 BROKS	6 BROKS	7 BROKS
SOCIAL JOURNALS	2 MB	3 MB	12 MB	163 MB
PROXY JOURNALS	4 MB	17.5MB	46.25 MB	159 MB

We have calculated both the total utility produced and its distribution among consumers for each detection algorithm. To evaluate accuracy independently of the deployment strategy, we first ran a set of trials using a centralized deployment setup [8]. In addition, we varied the number of brokers being used and repeated the studies using various deployment methodologies. One of the fundamental features of pervasive computing is its capacity to adapt to changes in a user session. The changes could result from intentional user activities (such as "composing" new devices, as in our scenario), from the middleware itself (connection quality changes, etc.), from the centralized environment (moving to a different place might present great possibilities, for example), or from both [9].

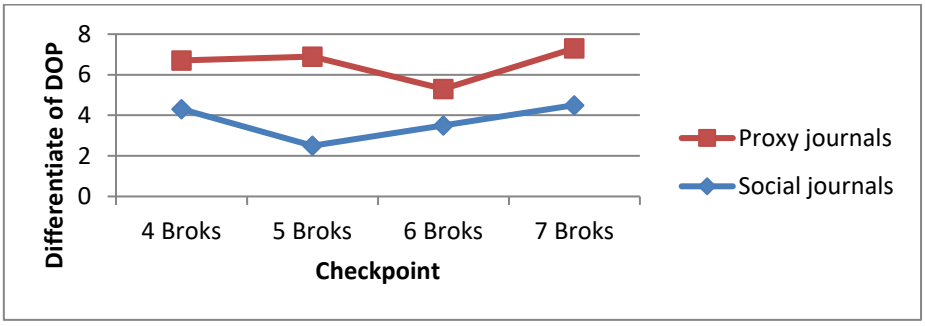

Figure 4.1 Popular brokers' DoP differs from randomized brokers'

To measure their effects on the level of transmission that brokers are capable of, the first experiment compared two alternative broker election procedures, namely "favorite" in the semi-distributed network situation, broker election and "random" broker election. We assessed the difference between the typical DoP carried out by 4, 5, and 7 well-known traders and the mean DoP carried out by 4, 5, and 7 random brokers to compare the two techniques. Throughout the research's three months, owing largely was estimated every three days. We have carried out 3 runs with various brokers chosen for each arrangement of the randomized broker (i.e., 4, 5, and 7 brokers). The outcomes line up with the average of those three runs. Figure 4.1's results reveal that the three random brokers are performing similarly to the three well-known brokers because the alteration line oscillates about zero. This shows that additional brokers may be required in order to propagate social media networks effectively. Instead, there is a clear distinction between the 4 and 7 famous brokers and the 6 and 7 random brokers as difference lines approach zero at checkpoint 30 (i.e., at the conclusion of the second month) (corresponding). This shows that because the latter meet more regularly to communicate their expertise on the social media network, prominent brokers can replicate and diffuse social networks far more rapidly than randomized brokers.

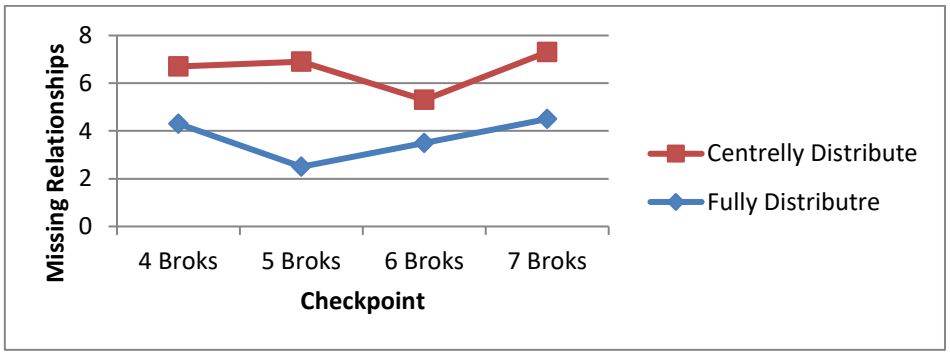

Figure 4.2 Impact of Deployment Method on Propagation

The second study compared several broker deployment options, including "fully-centralized," "semi-distributed," and "distribution," to measure their effects on the level of dissemination brokers can achieve. We have taken into account three possible configurations, i.e., with 4, 5, and 7 well-known brokers, for the semi-distributed scenario. Every DoP metric's standard error is also calculated. According to the findings, which are shown in Figure 4.2, there are fewer missing relationships (i.e., partnerships that could not continue to spread) as time goes on. In other words, it's easier to find new social connections, and as a result, social platform notifications are anticipated to be incorporated more quickly as well. Not all curves begin with the same Y-coordinate, which should be noted given that the first depicted checkpoint occurred three days into the investigation. Depending on the network's architecture and the nodes' flexibility patterns, a certain number of brokers must be deployed. 7 well-known brokers are adequate in the setting of the MIT mobility traces to produce the best results (as it is already equivalent to the centralized deployment). It should be noted that the completely distributed strategy achieves outcomes comparable to the (best) semi-distributed strategy, but at the penalty of a far larger overhead, as demonstrated in the following experiments.

Discussion

The results discussed above demonstrate that social media has an effect on how m-commerce applications are used, how social media websites advertise, and how consumers gain trust when making Transactions over mobile phones [10]. According to the findings of earlier experiments, Semi-distributed mobile overlays provide a fair balance between the costs and volumes that propagating brokers can sustain over time. Additionally, for executing fluid social network propagation, a limited quantity of brokers is sufficient. Finally, picking brokers wisely is essential for achieving the PSN aim. In order to increase customer confidence in disclosing their physical and social proximity information, it appears that nodes' popularity is a personal favorite that might be supplemented by nodes' trust qualities.

5. Conclusion

Our vision for pervasive social computers is given in this paper, and we also suggest a middleware to assist realize it. We have specifically put forth several social-based matching algorithms that consider users' social networks to fulfill users' demands, as well as alternative structural deployments, to efficiently distribute duties in a ubiquitous environment. In this article, we introduce a software service that complements through promoting the dynamic adoption and growth of scattered social media sites, the PSN vision our interoperable solution conceptually distinguishes

between customers and trading companies. Customers are nodes with activity-related preferences who request suggestions from other nodes that are both socially and physically related to them (i.e., nodes that collect that normative basis, carry out social media network propagation, and suggest suggestions to consumers). As part of our continuing work, we integrate and test various inter-activity propagating techniques within our software service to determine which one best fits the PSN development. Our upcoming work will concentrate on two key areas: the incorporation of privacy-preserving methods, as shown in the context of services discovering within our semi-distributed integration execution, and trust-aware broker electoral procedures, which elect nodes based on trust rather than just prominence.

References

[1] Zhao, R., & Wang, J. (2011). Visualizing the research on pervasive and ubiquitous computing. *Scientometrics*, *86*(3), 593-612.

[2] Ortiz, A. M., Hussein, D., Park, S., Han, S. N., & Crespi, N. (2014). The cluster between internet of things and social networks: Review and research challenges. *IEEE internet of things journal*, *1*(3), 206-215.

[3] Kasim, N. M., Fauzi, M. A., Wider, W., & Yusuf, M. F. (2022). Understanding Social Media Usage at Work from the Perspective of Social Capital Theory. *Administrative Sciences*, *12*(4), 170.

[4] Yan, Z., & Wang, M. (2014). Protect pervasive social networking based on two-dimensional trust levels. *IEEE Systems Journal*, *11*(1), 207-218.

[5] Yan, Z., Kantola, R., Shi, G., & Zhang, P. (2013, July). Unwanted content control via trust management in pervasive social networking. In *2013 12th IEEE international conference on trust, security and privacy in computing and communications* (pp. 202-209). IEEE.

[6] Zhou, J., Sun, J., Athukorala, K., Wijekoon, D., & Ylianttila, M. (2012). Pervasive social computing: augmenting five facets of human intelligence. *Journal of Ambient Intelligence and Humanized Computing*, *3*(2), 153-166.

[7] Mokhtar, S. B., McNamara, L., & Capra, L. (2009, November). A middleware service for pervasive social networking. In *Proceedings of the international workshop on middleware for pervasive mobile and embedded computing* (pp. 1-6).

[8] Ben Mokhtar, S., & Capra, L. (2009, July). From pervasive to social computing: algorithms and deployments. In *Proceedings of the 2009 international conference on Pervasive services* (pp. 169-178).

[9] Raatikainen, K., Christensen, H. B., & Nakajima, T. (2002). Application requirements for middleware for mobile and pervasive systems. *ACM SIGMOBILE Mobile Computing and Communications Review*, *6*(4), 16-24.

[10] Hossain, S. F. A., Xi, Z., Nurunnabi, M., & Hussain, K. (2020). Ubiquitous role of social networking in driving M-Commerce: evaluating the use of mobile phones for online shopping and payment in the context of trust. *SAGE Open*, *10*(3), 2158244020939536.