COVID-19 Patient Care: A Content-Based Collaborative Filtering Using Intelligent Recommendation System

B. D. Deebak[1](✉) and Fadi Al-Turjman[2]

[1] Schoool of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
deebak.bd@vit.ac.in

[2] Department of Artificial Intelligence Engineering, Research Center for AI and IoT, Near East University, Nicosia, Mersin 10, Turkey

Abstract. COVID-19 is a more transferable illness caused by a new novel coronavirus. It is highly emerging with efficient biosensors such as sensitive and selective that afford the diagnostic tools to infer the disease early. It can maintain a personalized healthcare system to evaluate the growth of disease under proper patient care. To discover as a personalized technology, the healthcare system prefers collaborative filtering. It can effectively deal with cold-start and sparse-data to conduct useful extensions. Due to the continuous expansion of scaling data in a medical scenario, content-based, collaborative filtering, and similarity metrics are preferred. It relies on the most similar social users or threats when the information is large. Many neighbors gain importance to obtain a set of users with whom a target user is likely to match. Forming communities reveal vulnerable users and also reduce the challenges of collaborative filtering like data-sparsity and cold-start problems. Thus, this framework proposes content-based collaborative filtering using intelligent recommendation systems (CCF-IRS) based on high correlation and shortest neighbor in the social community. The result is shown that the proposed CCF-IRS achieves better accuracy than the existing algorithms.

Keywords: COVID-19 · Healthcare · Content-based · Collaborative filtering · Recommendation systems · Accuracy

1 Introduction

A novel coronavirus known as SARS-CoV2 has widely been transferred across Wuhan to other parts of the country. This transferrable infection was unacquainted until it had been a chain of occurrences at Wuhan in early December 2019 [1]. In the past nine months, it has been widely dispersed that reports 27 million as reported case, 18 million as recovered case, and 881,000 as the death case [2]. In general, it has some common symptoms such as fever, loss of strength and energy, nasal clog, sore throat, and dry cough. An elderly person with medical complexities such as diabetes, heart disease, and

S. Paiva et al. (Eds.): SmartCity360° 2020, LNICST 372, pp. 31–44, 2021.
https://doi.org/10.1007/978-3-030-76063-2_3

hypertension are bearing with a continual illness, whereas an individual with deprivation, cough, and fever must inquire for a proper health checkup [3]. This infection is so viral among the people when they are closely contacted. On the other hand, the people should keep up a minimum distance of 3 feet to control the spread out during sniffing or talking. This infectious virus may survive up to 72 h on the contact surfaces. Therefore, a protective system is recommended to measure the safety precautions including a face mask, handwash, and sanitization [4].

This has led to several strategical approaches such as self-isolation, lockdown, risk assessments, transport containment, and closure of provisional necessities. The SARS-CoV2 has been dominated as a global threat that affects thousands of people in various forms such as chest pressure, fatigue, repeated shaking with chills, and loss of taste. The healthcare and respiratory monitoring form a drone-based platform to meet the objectives of the defense department such as sensing temperature, crowd distancing, workforces, heart, and respiratory assistance [5]. A drone is generally represented as the aerial vehicle that aviates over a region like an aircraft without human intervention. It has specific hardware and embedded system to design a suitable aerial vehicle that tracks the payload to improve the information efficiency and accuracy [6]. It may be modernized to visualize the sourcing model that explores the concept of crowdsourcing to perform several societal activities such as work, information, opinion. In this pandemic, it is widely used to monitor the system functionalities including thermal scanning, food supply, alter system, and medication [7].

Any form of personal data may result in the outcome of electronic activities to categorize the information as personal or professional. It may protect the sensitive data of the people to preserve privacy rights. Of late, SARS-CoV2 has caused several causalities that is nowadays growing exponentially across the globe. World Health Organization (WHO) has declared the disease as a pandemic outbreak that essentially demands technological tools, intellectual mechanisms, and network resources to save the human's life [8]. It is severely affecting people living in terms of fever, dry cough, and tiredness. Approximately, 80% of people have developed a mild infection and recovered without hospitalization. However, the symptoms such as chest pain, pressure, suffocation, loss of moment are found to be more vulnerable. In addition, people with medical ailments namely diabetes, cancer, respiratory issue, and cardiovascular disease may have a severe illness causing sudden death. Unfortunately, this disease does not have any proper treatment or vaccination to examine potential threats. Due to a lack of medical procedures and treatment, people should proactively prevent the infection by frequent hand-wash, wearing-mask, and stay-home [9].

The drone-based system integrates the distinct features of mission-centric regions such as red, orange, and green zone to deploy thermal screening, sanitization, contact tracing, and patient tracking. A smart healthcare system collects the medical data to observe patient conditions using a recommendation system that uses the information filters to provide a better-personalized recommendation [10]. It can be available as a search engine that periodically examines the input queries to process a set of contextual information of the users. Accordingly, it can generate a ranking list for the precaution measures that suit the standard requirement of the public or government. Since the treatment case may grow exponentially due to more public threats, a suitable recommender is highly necessitated to maintain the threat list in terms of region-wise or state-wise. However, the online database should be properly handled to solve the issue of overloading and network mapping. To determine the relevant information in the massive dataset, a suitable strategy such as collaborative filtering may be applied. It allows the recommendation system to filter the relevant information quickly that improves the application loyalties to save human life.

It is intended to offer a suitable web forum or intelligent application that acts as a real-time entity to monitor the activities of the patient. This system may widely be implemented to serve the purpose of public communities including schools, colleges, airports, transport, shopping malls, government, and industrial sectors. It has a product of an intelligent recommendation system (I-RS) to motivate the researchers to categorize the filtering methods into content-based, collaborative-filtering, and hybrid. These methods rely on the personal information of the patient that has a problem of privacy leak to ensure a feature of credible preference to the medical analysis. It may demand a mutual trust to prevent the data leakage containing the collaborative filter that protects the identities of the patient and the systems. Thus, this paper presents content-based collaborative filtering using intelligent recommendation systems (CCF-IRS) to offer data privacy and confidentiality. The proposed CCF-IRS mitigates the error deduction rate to measure the data trust in terms of similarity and trusted-criterion.

The remaining sections are as follows: Sect. 2 discusses the similar collaborative techniques to signify the use of similarity models. Section 3 shows a drone-based smart intelligence to signify the essential characteristics of three computing platforms including edge, fog, and cloud. Section 4 presents content-based collaborative filtering using intelligent recommendation systems. Section 5 shows the examination results of the proposed CCF-IRS and other collaborative techniques. Section 6 concludes the research work.

2 Related Works

To support data confidentiality and reduce the system error rate, various solutions have been proposed. Generally, it can categorize the recommendation systems into five types such as cryptographic, perturbation, data mining, and trust-based in social communities. Erkin et al. [11] introduced a cryptographic algorithm to privatize data access. It uses a data encryption technique including public and private keys to protect data confidentiality. It relies on trusted third parties to generate a reliable private and public key to the users. As each user requires a unique public and private to generate a reliable key pair, it is consuming more time to complete the process of key generation. Ma et al. [12] designed a new Applet framework to preserve the user information that obtains the user status from the cloud environment. It uses Paillier encryption to calculate and store the user ranking in text format. However, this designed strategy cannot be more reliable to produce a key pair of public and private keys. Liu et al. [13] designed a homomorphic algorithm using elliptic-curve cryptography that generates public and private keys through trusted third parties to preserve data privacy. However, this technique is consuming more time to compute the complex operation. Shieh developed homomorphic encryption to generate a key pair between the real-time entities. Unfortunately, this method is consuming more time to deal with the error rate.

Soni and Panchal [14] introduced homomorphic encryption to preserve data privacy in the recommendation system. This mechanism uses trusted third parties to produce the key pairs that ensure data confidentiality. Patil and Jadhav [15] use collaborative-based homomorphic encryption to protect the privacy of the recommendation system. Kaur et al. [16] introduced a homomorphic method to generate the public and private through the knowledge of trusted third parties. Chen et al. [17] utilized a field of cryptography to create public and private keys. However, it could not be more reliable to cite in the referral systems. Li et al. [18] developed a randomized perturbation technique to offer privacy-preserving that demands the expectation levels of the recommendation systems. It uses noise-based perturbation to form collaborative filtering that generates a random number using perturbation to enhance the prediction rate. Dou et al. [19] introduced a privacy-preserving method that uses a perturbation technique to meet the requirements of the social networks. It has a core aspect of user activities to define the raging matrix that predicts the ranking of multimedia resources. It applies a perturbation function to guess the adversary activities. However, it cannot achieve a better privacy-preserving to improve system performance. Polatidis et al. [20] designed a multi-level method to preserve user privacy using collaborative filtering. It uses randomized perturbation to rate the server access in-network domains.

It is worthy to note that the randomness provides better security protection, but the rate prediction is a bit complex to penetrate the rating process. Liu et al. [21] and Xiong et al. [22] utilized differential privacy and randomized perturbation that uses a perturbation technique to release the private data. These methods apply a privacy-preserving technique to increase the accuracy rate of user privacy. Goyal et al. [23] combined classification and clustering to improve rating efficiency, but cannot protect user privacy. Ma et al. [24] proposed a lightweight privacy-preserving technique that applies a random trust relationship to analyze the attributes of the social network using the KNN algorithm. Heidari et al. [25] use a clustering method to categorize the attributes of the big data. It can reduce the error rate efficiency, but does not affect the data confidentiality.

3 Drone-Based Smart Intelligent Systems

This section presents a drone-based smart intelligence system that integrates artificial intelligence to include learning techniques such as machine learning and deep learning to analyze the real-time data effectively. The service-based networking includes the Internet of Things (IoT), Internet of Medical Things, Internet of Vehicle, and Internet of Drone that uses AI technology to process the data efficiently. Besides, it has network computing resources such as fog, cloud, and edge to functionalize data storage, location tracking, distance tracing, face mask, etc. The smart-driven technology associates with user profiling to monitor the commuter movement that cautiously analyses the activities such as testing, tracing, observing, treating, recovering, and monitoring during this pandemic situation. Figure 1 shows the proposed architecture of drone-based smart intelligence that regulates three key factors such as control, monitoring, and analytics to meet the objectives of the mission-intelligent systems. This smart system architecture has six technological components, which are as follows:

Thermal Imaging: It is an alternative strategy to deploy the sensory platform to examine the collective information. It uses a drone-based camera to capture and analyze people's information including thermal reading and distance measurement.

Wearable Sensory System: This architecture deploys the sensory platform to observe commuter environments including public transport, shopping mall, school, and college. It uses a wearable sensor or ground movement detector to examine the surveillance areas. It uses interconnected networks such as the wearable body area network, Internet of Things, and the Internet of Medical Things to collect, observe, and analyze the statistical data. A patient under observation can be regulated using a wearable sensory system. In specific cases, a drone-navigator can be deployed to collect the patient's movements including tracking, tracing, treating, and observing the activities of the patients. On the other hand, the patient movements are continuously monitored using multiple servers to store the activities in big data. It uses computing platforms such as edge, fog, and cloud to maintain data modeling, profiling, processing, and analyzing the real-time data. The collective data are regulated under the government policies to operate any system procedures in the medical boards. The proposed strategy endures to tackle the pandemic situation to govern the people activities such as person profiling, location tracking, and data observation that integrates the wearable sensory system to formulate the design strategy of Industrial IoT. It can interconnect the sensory systems with medical intelligence to process the clinical trails such as drug supply, patient tracking, consulting, storage, and analysis.

Edge Networking: This system standardizes the data modeling and decision-making process that saves the computing resources to maintain the collection of medical data. It uses a drone network to handle discrete decisions in real-time. It is more useful to operate the system instruction to address the key challenges such as time stipulation, system interconnection, and computing tasks. The proposed system considers the data transfer cost to increase the feature of scalability that requires system intelligence and network resources to transfer the network costs.

Fog Networking: The proposed system incorporates the system intelligence to handle user profiling that executes decision-making and data monitoring to maintain the patient profile including commuter trajectory.

Cloud Networking: The proposed system applies application-level to pattern the regulation policies such as patient recognition, tracking, decision making, distance measuring, and sanitization. It can handle high-end computing systems to provide a comprehensive analysis.

Drone System: It uses a closed-circuit television (CCTV) to cover the surveillance areas including thermal screening, drug delivery, scanning, and sanitization. It can integrate the resources such as biosensors, accelerometers, and microelectromechanical systems to constitute a large data transfer and analysis. There are few important drones such as Parrot Mambo and DJI Phantom 3 Pro to navigate the indoor hospital system. It may also use radar or optical system to avoid collision avoidance that has a large number of aerial vehicles or drones to regulate various computing services such as public movement, transportation, aviation, etc.

Control Room and Covid-19 Monitoring: This system regulates the data observation to monitor the hotspots remotely that executes the necessary actions to control the individual's movements.

Data Processing, Capturing, and Analytical Flow: The proposed system uses drone-based intelligence to monitor or capture the patient information. However, it is still challenging to address privacy and security concerns.

Confidence-Based Trust Model: It considers patient profiling and trusted network groups to design a trust model that assigns different trust values to the patients according to the risk of region vulnerabilities. To group the trusted users in any network, the trusted values play a crucial role that infers the nature of user vulnerability in terms of risk ranking. It is typically based on the community networks to represent whether the trusted users are known to each other or not.

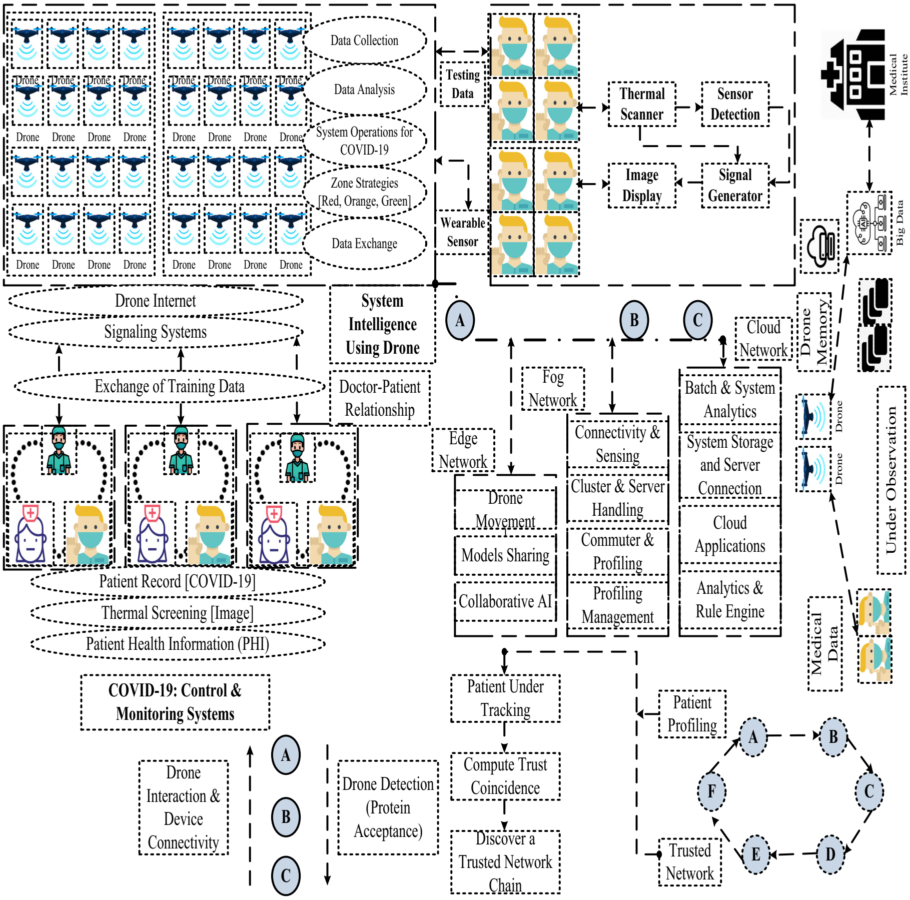

Fig. 1. Proposed architecture of drone-based smart intelligence

4 Proposed CCF-IRS

This section presents content-based collaborative filtering using intelligent recommendation systems with the detection of threat rates. The proposed CCF-IRS discusses content-based recommendation and collaborative filtering to mine the network communities in the trusted networks.

4.1 Content-Based Trust Recommendation

A content-based trust recommender has its own root to find the relevant information retrieval that applies a searching technique of information filtering. It can recommend similar items to the one that the user tries to prefer in the past. Most of the existing recommender systems focus on textual information including books, news, and documents. In any intelligent system, the content is generally labeled with keywords, thus informativeness of any keywords is measured using the weight of term frequency-inverse document frequency (TF-IDF). Any profiling document weights a keyword that denotes the term frequency (TF), while the weight of a keyword is defined as the inverse document frequency (IDF). However, content-based recommender has several limitations that are as follows:

Limited Content Analysis: The systems have difficulty applying the inherent problems with automatic feature extraction such as user profiling.

Overspecialization: The system has the recommended items to find the limitation of similar items, which are already rated by the users.

New User Problem: The content-based recommender uses preference settings to rate sufficient user profiling, hence it cannot recommend any user profiles with few user ratings.

4.1.1 Algorithm 1: Content-Based Rating, Offering by Social Community S_C for a Common Person P

In content-based vectorization, the social threats or items represent a rating mechanism that aims at user ranking r_u of a given user-item offering by S_C which is yet to rate in social networks. The formulation utilizes TF and IDF to recommend the nature of user profiling. It has a set of user items su and social threats $T^{'}_{su}$ to rank the social user su, which is yet to rate. While a score s is computed for the given unrated items u_i, Algorithm 1 gives careful consideration to two scoring strategies:

1. Firstly, it applies the cosine similarity score of all the social items in $T^{'}_{su}$. It can aggregate k social items enduring the cosine similarity in the highest form. Later on, p is a parameter of the contention model to denote the approach as '$p - Approach$'.
2. Secondly, a single vectorization is represented to obtain a key parameter $T^{'}_{su}$ that achieves the $n - dimension$ vector to represent the social threat $T^{'}_{su}$. It has an $n - dimensional$ vector centroid $T^{'}_{su} = \langle vc_1, vc_2, vc_3, \ldots\ldots, vc_n \rangle$ in which each user entry defines its own relevance score to the corresponding term T_d averaging over the social items in $T^{'}_{su}$:

$$T_d = \frac{1}{\left|T'_{S_u}\right|} . \sum\nolimits_{i \in T'_{S_u}} v_{id} \tag{1}$$

Then, the assigned score i defines the cosine similarity between vector i and centroid T'_{su}. It utilizes the relevance score to evaluate whether the representation of the individual items in T'_{su} adds a reasonable value over a reduced error rate.

4.2 Collaborative Filtering Techniques

This technique is widely used to build recommender systems that classify into memory-based and model-based approaches. In the former approach, the user-item matrix is applied to signify input and predicted user interest that directly uncovers the complex and unpredicted patterns from the past behavior of the recommended items. The users with similar interests and profiling preferences have a perfect combination to explore network communication in a social environment. It can find whether any user coincides with similar profiling agreed with each other in the past or not.

Table 1. Merit and key issues in memory-based approach

Name	Merits	Key Issues
User-based	• No content analysis • Domain-independent • Quality improves • Bottom-up approach • Serenity	• New user problem • New item problem • Popular taste • Scalability • Sparsity • Cold start problem
Item-based	• Focus on items; assume that the items rated similarly are probably similar. • It recommends items with the highest correlation	• New item problem • Popular taste • Sparsity • Cold start problem

It is more likely to agree with each profiling that randomly chooses the users in the future as well. The memory-based approach is typically divided into a user-based and item-based method. The former predicts the unknown threat rating from similar user profiling over the weighted average, whereas the latter predicts the threat rating from the user profiling over the average weighted rating by the same communities. However, it has some significant issues to tabulate (see Table 1). On the other hand, the item-based technique correlates the social threats using mining or similarity ratings before any threat is recommended newly (see Fig. 2). This technique deals with the ‘cold start’ problem because it is depended on sufficient user behavior from the past. When the systems execute the collaborative filtering technique for a while, this problem endures to emerge the rating when new users or items are newly added. On the one hand, the new users should give sufficient ratings for the social items in order to provide an accurate recommendation based on the user-based method. On the other hand, the new items should rate with a sufficient number of community users when any social items are under community threats. Additionally, it deals with the ‘sparsity’ upon the user action taken on the networks. Since these filtering techniques rely on community-driven information, community threats are supposed to be more common across the regions. The learners with an unusual threat may have less qualitative recommendations, while the learners with common threats are unlikely to classify the highly vulnerable threats.

Hence, the common problem of the filtering technique is scalability, thereby it cannot deal with large amounts of data to provide a proper recommendation to the global communities in real-time exceeding in 27.4 million.

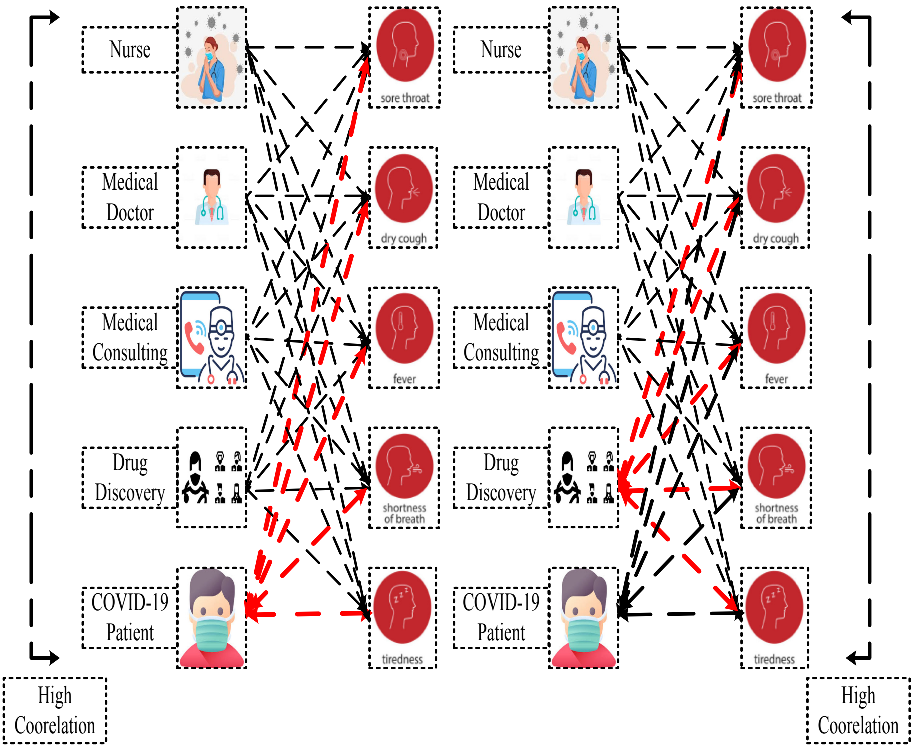

Fig. 2. User-based and item-based methods

To measure the correlations, several similarity measures are available listed below. It is assumed that $su = \{su_1, su_2, su_3, \ldots\ldots, su_N\}$ and $t = \{t_1, t_2, t_3, \ldots\ldots, t_M\}$ are the set of social users and threats respectively. The rating matrix of social-user-threat is denoted by $R = \left(r_{ij}\right)_{NxM}$, where $i = 1, 2, 3, \ldots\ldots, N$ and $j = 1, 2, 3, \ldots\ldots, M$. The Pearson correlation coefficient (PCC) and cosine (CoS) similarities are the most widely used to measure the similarities in collaborative filtering. The formulas are defined as follows:

$$(su, v)^{PCC} = \frac{\sum_{t\in I}\left(r_{su,t} - \overline{r_{su}}\right).\left(r_{v,t} - \overline{r_v}\right)}{\sqrt{\sum_{t\in I}\left(r_{su,t} - \overline{r_{su}}\right)^2}.\sqrt{\sum_{t\in I}\left(r_{v,t} - \overline{r_v}\right)^2}} \tag{2}$$

$$(su, v)^{cos} = cos\left(\overrightarrow{su}, \overrightarrow{v}\right) = \frac{\overrightarrow{su}\,.\,\overrightarrow{v}}{\|\overrightarrow{su}\|.\|\overrightarrow{v}\|} \tag{3}$$

where I defines the set of common social rating threats by the social users su, $v.\overline{r_{su}}$, $\overline{r_{su}}$ and $\overline{r_v}$ are the average rating values of su and v respectively. $r_{su,t}$ and $r_{v,t}$ defines the rating of the social threats t given by su and v respectively. $\overrightarrow{su}$ and $\overrightarrow{v}$ are the rated social vector su and v respectively. $\|\,\|$ is the vector magnitude vector. However, few shortages exist in both PCC and CoS to improve similarity measures. In general, the scale of social ratings is unqualified to analyze the metrics in recommender systems. The system infers the social ratings as positive or negative to determine the social impact in any social community. Hence, the Constrained Pearson correlation coefficient (CPCC) is defined as follows:

$$(su, v)^{CPCC} = \frac{\sum_{t\in I}\left(r_{su,t} - r_{med}\right).\left(r_{v,t} - r_{med}\right)}{\sqrt{\sum_{t\in I}\left(r_{su,t} - r_{med}\right)^2}.\sqrt{\sum_{t\in I}\left(r_{v,t} - r_{med}\right)^2}} \tag{4}$$

where r_{med} defines the rating scale median. To find a similarity the user profiling, $(su, v)^{CPCC}$ is utilized. It can predict the profiling on social items using the average ratings defined in Eq. (1).

5 Proposed CCF-IRS

This section shows the process of the proposed CCF-IRS that includes content-based rating and collaborative filtering to analyze the rating of active users.

We prefer to use the available social threats which are primarily focused as a pandemic threat of COVID-19. It is attracting global attention as it is being viewed as a serious threat to the socio-economic impacts. The infection is so common across the globe with some cautious symptoms such as dry cough $\langle 1\rangle$, fever $\langle 2\rangle$, fatigue $\langle 3\rangle$, sore throat $\langle 4\rangle$, conjunctivitis $\langle 5\rangle$ that gradually develops from mild to moderate illness ≈ 5 to ≈ 9 days. However, the infectious cause may even take up ≈ 14 days to mutate its form as S and L type. The mutation process may change from asymptomatic to severe pneumonia that reviews with some typical symptoms such as headache, nausea, congestion, and vomiting. Thus, the clinical presentation considers some universal precautions to prevent further transmission. This transferable disease demands the use of a face mask to reduce the transmission rate across the various communities and workplaces. To provide an effective measure, a preprocessing strategy is applied with a scale of 5-threats. Each social user experiences at least some threats to define the set of social users as communities. The social user rates the infectious rate to represent the sequence of events that represent the correlation between the infection rate (see Fig. 3).

It has two basic assumptions to visualize the quality measurement that performs the maximum modularity using the Gephi tool.

1. Social user su_1 rates social threat I_1 with 4
2. Social user su_2 rates social threat I_2 with 3

A total of 56 communities has been identified with maximum modularity of $Q = 0.549$. The quality metric such as modularity is considered to analyze the library function using igraph in R. The proposed CCF-IRS considers the analytical dataset to determine the impact of the training sets that recommend the qualities of the original samples. It uses a cross-validation technique to partition the dataset into $k - samples$. It considers one subsample to validate the testing model that has two scenarios such as 90% of social user ratings and 40% of rating instances to test the real-time scenario.

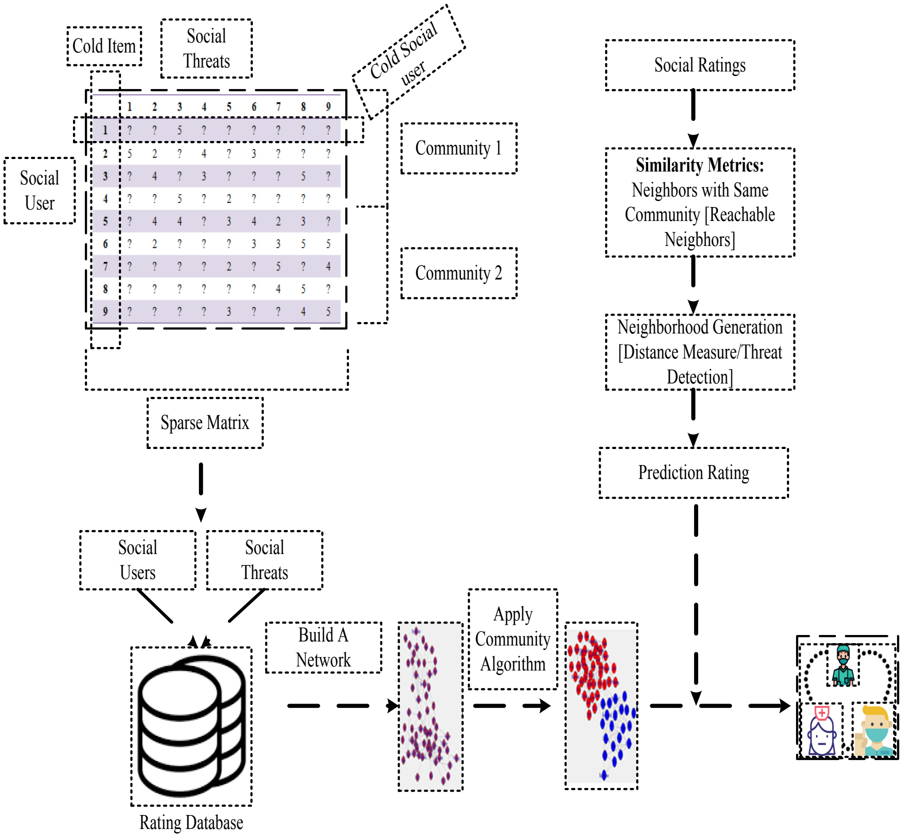

Fig. 3. Social communities and threats based collaborative recommendation system

In R Programming, the library known as recommender lab uses content-based collaborative filtering using intelligent recommendation systems that apply the quality metrics such as mean absolute error (MAE), root mean square error (RMSE), precision, coverage, and F-Measure to examine the prediction accuracy of the proposed CCF-IRS. The metrics are defined as follows:

$$MSE = \frac{1}{t}.\sum\nolimits_{Su,v} \left| R_{su,v} - \overline{R_{su,v}} \right| \tag{5}$$

$$RMSE = \sqrt{\frac{1}{t}.\sum\nolimits_{su,v} \left(R_{su,v} - \overline{R_{su,v}} \right)^2} \tag{6}$$

$$Precision = 1 - \frac{(RMSE)}{4} \tag{7}$$

$$Coverage = \frac{su}{N} \tag{8}$$

$$F - Measure = \frac{\langle 2 * Precision * Coverage \rangle}{\langle Precision + Coverage \rangle} \tag{9}$$

where $R_{su,v}$ represents the rating provided by social users over su and v, $\overline{R_{su,v}}$ represents the prediction rating, and t represents the cumulative tested ratings. Table 2 estimates the performance efficiencies of different quality metrics such as mean absolute error (MAE), root mean square error (RMSE), precision, coverage, and F-Measure. The examination reveals that the proposed CCF-IRS achieves better performance efficiency than other collaborative techniques.

Table 2. Performance of different quality metrics

Algorithms	*RMSE*	*MAE*	*Precision*	*Recall*	*F − Measure*
Item-based CF	1.271	0.942	0.844	0.7264	0.756
SNCF	1.254	0.887	0.896	0.742	0.796
Proposed CCF-IRS	1.243	0.872	0.912	0.889	0.861

6 Conclusion

In this paper, a typical drone-based smart intelligence has been proposed for COVID-19 patient care. It can mainly investigate some quality measures such as face masks, social distancing, sanitization, statistical analysis, and report analysis to control the infection rate. This framework gathers the sensitive data of the patient using wearable or movement sensors in any targeted area through thermal image-screening. It may apply a multi-layered architecture to examine the statistical data and to make any decision-making. Moreover, it has an edge, fog, and cloud computing to build technological intelligence before any decision is made. To improve the preferential measurement and quality recommendation, this paper has proposed CCF-IRS. It uses similarity models to validate the effectiveness of quality measures. The proposed CCF-IRS integrates content-based and collaborative filtering to resolve the issues of cold-start and sparsity-data. It can explore user profiling to infer the difficulties of the user communities that typically view the systematic flows of social threats. The experimental result reveals that the proposed CCF-IRS achieves better performance measures than other collaborative techniques. In the future, we will explore the similarity computation of trusted users pertaining to the same communities.

References

1. Suliman, K., et al.: Emergence of a novel coronavirus, severe acute respiratory syndrome coronavirus 2: biology and therapeutic options. J. Clin. Microbiol. **58**(5) (2020)
2. Kumar, A., Sharma, K., Singh, H., Naugriya, S., Gill, S., Buyya, R.: A drone-based networked system and methods for combating coronavirus disease (COVID-19) pandemic. Future Gener. Comput. Syst. **115**, 1–19 (2021). https://doi.org/10.1016/j.future.2020.08.046
3. Singer, M., Baer, H., Long, D., Pavlotski, A.: Introducing medical anthropology: a discipline in action. Rowman & Littlefield (2019)
4. World Health Organization. Water, sanitation, hygiene, and waste management for SARS-CoV-2, the virus that causes COVID-19: interim guidance, 29 July 2020 (No. WHO/COVID-19/IPC_WASH/2020.4). World Health Organization (2020)
5. Kuula, J.: The hyperspectral and smartphone technology in CBRNE countermeasures and defence. Jyväskylä Stud. Comput. **256** (2016)
6. Meier, L., Tanskanen, P., Heng, L., Lee, G.H., Fraundorfer, F., Pollefeys, M.: PIXHAWK: a micro aerial vehicle design for autonomous flight using onboard computer vision. Auton. Robot. **33**(1–2), 21–39 (2012)
7. Liang, T.: Handbook of COVID-19 prevention and treatment. The First Affiliated Hospital, Zhejiang University School of Medicine. Compiled According to Clinical Experience, 68 (2020)
8. Jeffery Reeves, J., et al.: Rapid response to COVID-19: health informatics support for outbreak management in an academic health system. J. Am. Med. Inform. Assoc. **27**(6), 853–859 (2020). https://doi.org/10.1093/jamia/ocaa037
9. Fong, S., Dey, N., Chaki, J.: Artificial Intelligence for Coronavirus Outbreak. Springer Singapore, Singapore (2021)
10. Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P.M., Sundarasekar, R., Thota, C.: A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. Future Gener. Comput. Syst. **82**, 375–387 (2018)
11. Erkin, Z., Veugen, T., Toft, T., Lagendijk, R.L.: Generating private recommendations efficiently using homomorphic encryption and data packing. IEEE Trans. Inf. Forensics Secur. **7**(3), 1053–1066 (2012)
12. Xindi, M., et al.: APPLET: a privacy-preserving framework for location-aware recommender system. Sci. China Inf. Sci. **60**(9), 092101 (2017)
13. Liu, K., Giannella, C., Kargupta, H.: A survey of attack techniques on privacy-preserving data perturbation methods. In: Aggarwal, Charu C., Yu, Philip S. (eds.) Privacy-Preserving Data Mining, pp. 359–381. Springer US, Boston, MA (2008). https://doi.org/10.1007/978-0-387-70992-5_15

14. Soni, K., Panchal, G.: Data security in recommendation system using homomorphic encryption. In: Satapathy, S.C., Joshi, A. (eds.) ICTIS 2017. SIST, vol. 83, pp. 308–313. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-63673-3_37
15. Patil K., Jadhav N.: Multi-layer perceptron classifier and Paillier encryption scheme for friend recommendation system. In: International conference on computing, pp. 1–5. IEEE (2017)
16. Kaur, H., Kumar, N., Batra, S.: An efficient multi-party scheme for privacy preserving collaborative filtering for healthcare recommender system. Future Gener. Comput. Syst. **86**, 297–307 (2018)
17. Chen, S., Rongxing, L., Zhang, J.: A flexible privacy-preserving framework for singular value decomposition under internet of things environment. In: Steghöfer, J-P., Esfandiari, B (eds.) IFIPTM 2017. IAICT, vol. 505, pp. 21–37. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59171-1_3
18. Li, D., et al.: An algorithm for efficient privacy-preserving item based collaborative filtering. Future Gener. Comput. Syst. **55**, 311–320 (2016)
19. Dou, K., Guo, B., Kuang, L.: A privacy-preserving multimedia recommendation in the context of social network based on weighted noise injection. Multimedia Tools Appl. **78**(19), 26907–26926 (2017). https://doi.org/10.1007/s11042-017-4352-3
20. Polatidis, N., Georgiadis, C.K., Pimenidis, E., Mouratidis, H.: Privacy-preserving collaborative recommendations based on random perturbations. Expert Syst. Appl. **71**, 18–25 (2017)
21. Liu, X., Liu, A., Zhang, X., Li, Z., Liu, G., Zhao, L., Zhou, X.: When differential privacy meets randomized perturbation: a hybrid approach for privacy-preserving recommender system. In: Candan, S., Chen, L., Pedersen, T.B., Chang, L., Hua, W. (eds.) DASFAA 2017. LNCS, vol. 10177, pp. 576–591. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-55753-3_36
22. Xiong, P., Lefeng, Z., Tianqing, Z., Gang, L., Wanlei, Z.: Private collaborative filtering under untrusted recommender server. Future Gener. Comput. Syst. (2018). https://doi.org/10.1016/j.future.2018.05.077
23. Goyal, N., Aggarwal, N., Dutta, M.: A novel way of assigning software bug priority using supervised classification on clustered bugs data. In: El-Alfy, E.-S.M., Thampi, S.M., Takagi, H., Piramuthu, S., Hanne, T. (eds.) Advances in intelligent informatics. AISC, vol. 320, pp. 493–501. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-11218-3_44
24. Ma, X., Ma, J., Li, H., Jiang, Q., Gao, S.: ARMOR: a trust-based privacy-preserving framework for decentralized friend recommendation in online social networks. Future Gener. Comput. Syst. **79**, 82–94 (2018)
25. Heidari, S., Alborzi, M., Radfar, R., Afsharkazemi, M., Rajabzadeh Ghatari, A.: Big data clustering with varied density based on MapReduce. J Big Data **6**(1), 1–16 (2019). https://doi.org/10.1186/s40537-019-0236-x
26. Al-Turjman, F., Deebak, B.D.: Privacy-aware energy-efficient framework using the internet of medical things for COVID-19. IEEE Internet of Things Mag. **3**(3), 64–68 (2020)
27. Deebak, B.D., Al-Turjman, F.: A novel community-based trust aware recommender systems for big data cloud service networks. Sustain. Cities Soc. **61**, 102274 (2020)