ISSN : 0973 - 8355

www.ijmmsa.com

IJMMSA

INTERNATIONAL JOURNAL OF MATHEMATICAL, MODELLING, SIMULATIONS AND APPLICATIONS

E-MAIL
editor.ijmmsa@gmail.com
editor@ijmmsa.com

INTERNATIONAL JOURNAL OF
IJMMSA MATHEMATICAL, MODELLING, SIMULATIONS AND APPLICATIONS

ISSN 0973-8355www.ijmmsa.com

Vol 8, Issuse3.Aug 2020

What are the applications, problems, and future prospects of blockchain-based recommender systems?

P.V.Sarath Chanda[1],N.Ch.Ravi[2],Dr.G.S.S.Rao[3],Dr.M.Sreenivasulu[4]

abstract

Recommended systems are extensively utilised in a variety of fields, including as in energy conservation, e-commerce, health care and social networking sites, among others. In order to construct precise and effective recommender systems, such applications need the analysis and mining of enormous volumes of different sorts of user data, including demographics, preferences, social interactions, etc. Datasets containing sensitive information are common, however recommender systems tend to prioritise accuracy above security and privacy concerns. As a result, no risk reduction strategy has been totally effective in maintaining cryptographic security and the protection of the user's private information. Blockchain technology has emerged as a viable technique to increase security and privacy preservation in recommender systems, not only because of its security and privacy salient aspects, but also because of its resilience, flexibility, failure tolerance and trust characteristics. An in-depth look into blockchain-based recommender systems, including problems, open issues, and solutions, is presented in this study. A well-designed taxonomy is provided to characterise the security and privacy concerns, review current frameworks, and evaluate their applications and advantages when utilising the blockchain before highlighting prospects for future study, as well.

Introduction

Recommendation engines, originally designed to improve customer experience and retention on e-commerce sites, have since become a common and anticipated feature of many online interactions, from movie and song recommendations [2] to applications for tourism, social networks, health and energy and smartcities [5–7]. Internet of things (IoT), Internet-connected gadgets (e.g. mobile phones, tablets, laptops and smartsensors, etc.), and sensors have resulted in massive volumes of data [7, 8]. The "five V's," meaning velocity, variety, veracity, volume, and value, characterise these enormous amounts of data [9]. Many facets of daily life, including as social network interactions, e-commerce, healthcare services, and energy, have been revolutionised profoundly by the capacity to create and analyse large amounts of big data [10].

Professor[1,2,3,4,] Assistant Professor[1,2,3,4], ,Associate Professor[1,2,3,4],
Department of CSE Engineering,
Pallavi Engineering College,
Mail ID:chandsarath70@gmail.com, Mail ID:ravi@saimail.com,
Kuntloor(V),Hayathnagar(M),Hyderabad,R.R.Dist.-501505.

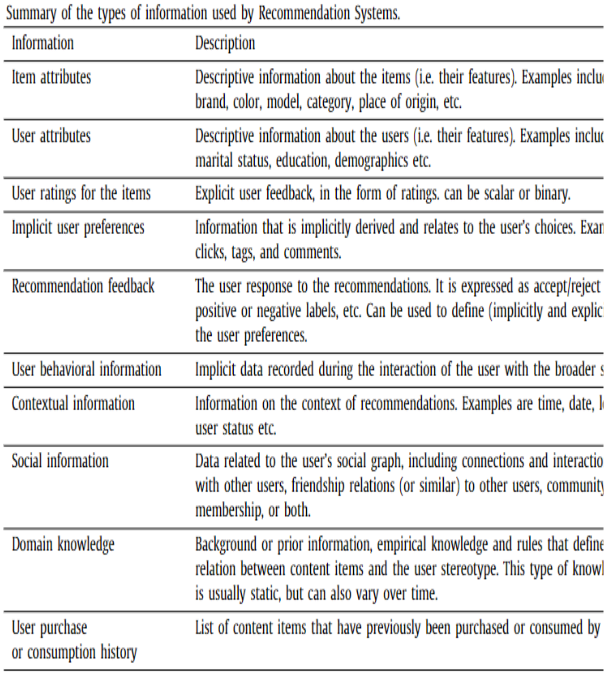
It is possible for people to get valuable information about their health, environment, and other factors by processing large amounts of big data properly [11]. Big data, on the other hand, makes it difficult to handle these applications because of their pervasiveness andubiquity. New, scalable RS algorithms that can handle varied kinds and enormous volumes of data have emerged, despite the fact that big data analytics have been utilised for many years to assist humans in processing such information and making judgments [12]. RSs have been able to progress from classic clustering, closest neighbours, matrix factorization, and collaborative filtering to a new generation of RSs driven bycomplex deep learning systems [15] and knowledge graphs [16] thanks to the substantial advancements in machine learning. A wide range of new applications for RSs have emerged as a result, including but not limited to e-commerce, social media, e-learning, social behaviour analysis, energy conservation, healthcare, the Internet of Things, tourism, fashion, and the food sector, to name just a few. Data sources that are utilised in RSs in addition to the conventional 'user, item and rating' triplets are included in Table 1, indicating the wide range of information that may be employed. Such user-related data has unquestionable relevance and sensitivity. Most research into establishing new algorithms and models does not include privacy and security while optimising for accuracy and/or scalability, despite the fact that some researchers [28] have looked into constructing privacy-preserving random number systems (RS). An further weakness of RSs is that they are open to attack from outside sources (such as injected or manipulated data used to train the models). In the era of cloud computing, securing and protecting data has become a considerably more difficult undertaking than it was in the past. Although numerous risk reduction approaches have been used, none of them have been totally effective, particularly in terms of cryptographic security and the protection of users' private information. Therefore, Blockchain technology has shown itself to be a successful decentralised method of protecting security and privacy over the last several years. There has been an increase in interest in this cross-domain topic among academics from both groups due to the potential of this technology to address one of the most pressing issues facing RSs. Building trust-based and secure systems employing the advantages of blockchain-supported secure multiparty computing is made feasible by integrating the blockchain into RSs.

Smart contracts are included into the RS pro-blockchain platform. Internet users may rest easy knowing that their personal information is secure because to the widespread adoption of the protocol. portals. This is because it makes use of a distributed ledger that provides the required mechanical support for storing and processing data transactions, as well as techniques for safeguarding and maintaining the integrity of data via the use of technology. Combined, they provide a full solution. In comparison to traditional storage techniques, the blockchain's complicated structure and algorithmic processes make it more difficult to corrupt and tamper with RSs based on the blockchain. They have put up their best efforts here, the first evaluation of RSs based on blockchain. As a consequence, Tocategorise the present state of technologyRSs based on the blockchain, we use a good taxonomy. We'll begin by discussing the issues of safety and privacy. issue areas, features and operational concepts of RSs as well as probable blockchain effect on RSs. Following an explanation of blockchain-based RS design, an example of the most typical RSs constructed on the blockchain is provided as an overall overview. Once we do it, we'll go on to the next phase. An RS built on the blockchain is described, along with numerous possible applications. There are a number of examples provided. After that, we'll conduct a thorough analysis. check to see if there are any present or prospective faults. Finally, we identify potential prospective research routes that are likely to draw a lot of attention in the near and medium term, as well as a lot of attention a long time in the future. The following are a few of the study's key findings: follows: Bridges two academic disciplines that may be utilised for research. the "blockchain," also known as a "recommender system," influence one another significantly (RSs). For each person, a unique map is constructed. researchers who are working on blockchain-based RSs This report focuses on problems, unanswered questions, and solutions that might be found. RSs will be used to inject the blockchain ledger with decentralised applications. By keeping your data in a different place, you can ensure its safety. In light of different characteristics, such as time, accuracy, and the eloquence of current suggestions, it rates the efficacy of a variety of commonly utilised frameworks. Scalability and other features of RSs are analysed. " distributed computing and load balancing It creates new problems for blockchain researchers. Users and developers As part of this approach, blockchain-based RSs and their performance will be improved, while some of the current issues will be addressed. In order to innovate in the field of blockchain-based RSs and provide the framework for their future growth, a specific process was followed for the objectives of this study. Figure 1 shows a group of divers out in the field. As a starting point, let's look at how blockchain compares to RSs and what it can accomplish to address those needs. Next, we'll talk about how blockchain technology complies with RS criteria by describing its most critical features. After that, the basic architectural plan is put forward. to learn more about the main implementation of blockchain-based RSs as well as other relevant features. The next phase is to examine the potential applications for the new solution and any unanswered questions that have arisen so far. Finally, there are a number of potential directions for further research.

presented.

Table 1

Summary of the types of information used by Recommendation Systems.



Information	Description
Item attributes	Descriptive information about the items (i.e. their features). Examples inclu brand, color, model, category, place of origin, etc.
User attributes	Descriptive information about the users (i.e. their features). Examples incluc marital status, education, demographics etc.
User ratings for the items	Explicit user feedback, in the form of ratings. can be scalar or binary.
Implicit user preferences	Information that is implicitly derived and relates to the user's choices. Exar clicks, tags, and comments.
Recommendation feedback	The user response to the recommendations. It is expressed as accept/reject positive or negative labels, etc. Can be used to define (implicitly and explic the user preferences.
User behavioral information	Implicit data recorded during the interaction of the user with the broader s
Contextual information	Information on the context of recommendations. Examples are time, date, l user status etc.
Social information	Data related to the user's social graph, including connections and interactio with other users, friendship relations (or similar) to other users, community membership, or both.
Domain knowledge	Background or prior information, empirical knowledge and rules that define relation between content items and the user stereotype. This type of knowl is usually static, but can also vary over time.
User purchase or consumption history	List of content items that have previously been purchased or consumed by

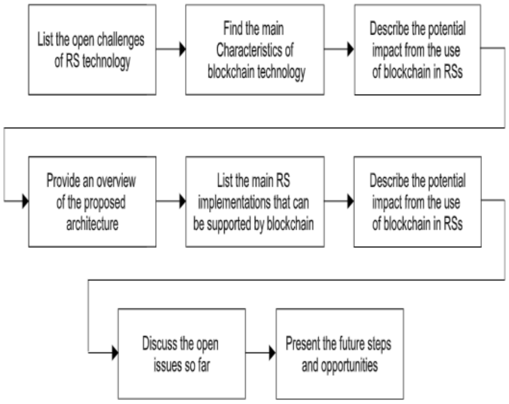

List the open challenges of RS technology
Find the main Characteristics of blockchain technology
Describe the potential impact from the use of blockchain in RSs
Provide an overview of the proposed architecture
List the main RS implementations that can be supported by blockchain
Describe the potential impact from the use of blockchain in RSs
Discuss the open issues so far
Present the future steps and opportunities

Fig: The main steps for introducing blockchain-based RS solutions and going beyond the current state of the art.

The rest of the paper is organized as follows: Section 2 pro-vides an overview of blockchain-based RSs, starting with themain challenges of RSs and the main blockchain features thatcan be of benefit to RSs, followed by a discussion on the impactof blockchain's use to future RSs, a presentation of the mainarchitecture of a blockchain-based RS, and the various types ofblockchain-based RSs and their applications. Section 3 includesa critical analysis that highlights the drawbacks and limitationsof the proposed technology and discusses the main open issues,whereas Section 4 provides the directions for future research onthe topic. Finally, Section 5 concludes the paper by highlightingthe importance of the proposed framework for the blockchain andRSs research community.

Overview of blockchain-based RSs

RSs' application of blockchain technology has just begun, with the first publication published in 2016 [29] and the bulk of related work published in the previous two years.. A thorough taxonomy is needed to identify the key research sub-areas and the current research subjects in each one of them, in order to offer a full overview of the field and identify the obstacles and potential for future study. Learn about the many application domains of blockchain-based RESTful services, as well as the unique features of the two domains (blockchain and RESTful services) and their obstacles. Research in blockchain-based RSs will be impacted by new technologies that are projected to emerge in the near future, and this will provide academics a better understanding of where future research should go. We used the taxonomy shown in Fig. to organise our survey of relevant work in the domain of blockchain-basedRSs.

2.2.1. Security and privacy challenges in RSs (C)

As in all machine learning algorithms, the success of RS modelsrelies on the quality and quantity of data. The more the systemknows about the past history of a user, the better the qualityof the recommendations. Moreover, when additional informationsuch as the one included in Table 1 is incorporated, and themore accurate and detailed it is, the more useful and personalized

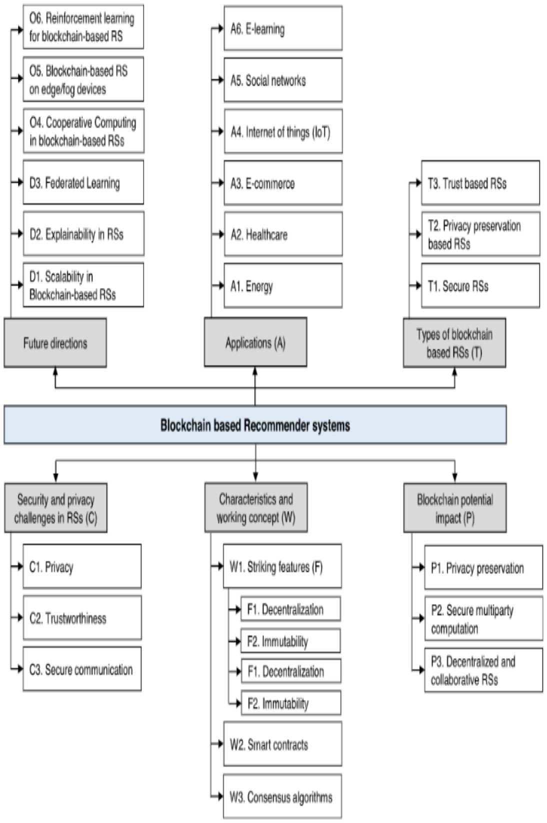

O6. Reinforcement learning for blockchain-based RS
O5. Blockchain-based RS on edge/fog devices
O4. Cooperative Computing in blockchain-based RSs
D3. Federated Learning
D2. Explainability in RSs
D1. Scalability in Blockchain-based RSs
Future directions
A6. E-learning
A5. Social networks
A4. Internet of things (IoT)
A3. E-commerce
A2. Healthcare
A1. Energy
Applications (A)
T3. Trust based RSs
T2. Privacy preservation based RSs
T1. Secure RSs
Types of blockchain based RSs (T)
Blockchain based Recommender systems
Security and privacy challenges in RSs (C)
C1. Privacy
C2. Trustworthiness
C3. Secure communication
Characteristics and working concept (W)
W1. Striking features (F)
F1. Decentralization
F2. Immutability
F1. Decentralization
F2. Immutability
W2. Smart contracts
W3. Consensus algorithms
Blockchain potential impact (P)
P1. Privacy preservation
P2. Secure multiparty computation
P3. Decentralized and collaborative RSs

Fig:Taxonomy of blockchain based RSs.

the user's suggestions are. Various security and privacy risks are raised as a result of unauthorised access to or susceptible handling of users' data in this scenario [30]. There is a greater risk of a user's privacy being compromised if more particular information about their preferences, habits, and behaviours is made available to the public. Although currentRS methods and implementations tend to overlook the danger of hostile attacks and the concerns they pose to user privacy, this is not always the case. The idea of trust is a closely connected one. Trust may signify several things in relation to RSs. In the first place, it has to do with the user's confidence in the RS's ability to safeguard their sensitive data and privacy. For the suggestions to be accepted, users need to have faith in the accuracy and correctness of the recommendations provided by the system. When it comes to making trust-aware recommendations, there is still another way to look at trust. This refers to social recommendation systems that employ the user's circle of trust to improve suggestion quality. That third interpretation will not be discussed any further since this study is focused on security and privacy-related trust.

C1. Privacy

Because RSs collect and retain a variety of sensitive data about a user's identification, utility consumption, preferences, and social networks, protecting the privacy of the user is critical [34]. For example, if an attacker obtains access to the RS engine, they might mine and steal important information about the user's habits and preferences. Data saved in healthcare apps may include even more sensitive information [35,36]. The first line of defence in the digital age is authentication, which is essential in almost any knowledge-based system. Furthermore, it contributes significantly to the development of a relationship of mutual trust between the RS and its users. An RS user must first connect to the RS network and then identify themselves on the RS platform, which checks the trustworthiness of claimed identities by comparing various user-related facts. However, since most RSs and their associated data are hosted on third-party cloud platforms, an additional level of risk has been established. A privacy breach might be a result of this. Studies on data encryption, distributed storage and processing, and other technological elements of privacy and security in RS have been conducted from a variety of perspectives [37].

C2. Trustworthiness:

The precision and correctness of the recommendations can deteriorate due to several reasons, and mainlydue to the training process itself. Even in cases where everythingis done properly, the quality and trustworthiness of the recom-mendations can be compromised, either due to bias existing inthe data, or due to malicious attacks. Despite the many and clearlydefined algorithms employed by the recommendation engines,users are generally not provided with enough data and conve-nient reasoning that will allow to comprehend precisely why andhow an item/action is being recommended to them. This leadsto ‘‘black-box’’ models, which may hide inherent biases in thetraining dataset or the overall design that might go undetected.Explainability of recommendations is a prevalent challenge notonly for RSs, but for all ML models in general [38,39].Finally, and most related to security and privacy, the datasetand/or the model might be compromised by malicious attacksaiming to achieve a particular outcome in the recommenda-tion process. RSs can suffer from different kinds of maliciousattacks launched by hackers who would try to leak the identi-ties of the authenticated users and bias the recommendations,such as shilling attacks [40,41], adversarial attacks [42,43], profileinjection attacks [44,45], and poisoning attacks [46,47].Informally, the robustness of a RS measures its ability to pre-vent attackers from manipulating its output. When such attacksare targeted to rating-based RSs, they usually include injection offake information on a user profile (e.g. fake ratings), generationof fake profiles that intentionally rate specific items higher thanothers (which are randomly assigned low ratings), or attacks tonuke specific items. To that end, robustness, which refers to delivering stable, secure and tailored recommendations, is becomingone of the most challenging security issue for RSs [48,49].A variety of strategies that can be employed to build RSsin a more robust way have been proposed. CAPTCHA has beensuccessfully used in several online systems to identify humansvs. robots and can be applied in the RS context as well [50].Social trust [51] has also been widely explored [52,53] as away to identify adversary behaviors. A variety of robust matrixfactorization methods for designing attack-resistant RSs have alsobeen proposed [54,55]. An overview of attack-resistant RSs canbe found in [56] while a very recent survey of attack-detectionapproaches for RSs has appeared in [57].

C3. Secure Communications

Security standards for communications between users and the RS engine should be as comprehensive as possible, even if RSs just need to meet the very minimal criteria. Sending and receiving various types of data is how RSs connect with their users. Furthermore, if the RS needs a significant amount of compute and storage, data may be sent to distant cloud servers [58]. It is thus presumed that all information sent between RS and users is verified and accurate. However, in practise, malevolent individuals may be able to tamper with the authentication information.

Blockchain-based RS: characteristics and working concept (W)

Many real-world applications of RSs have emerged since their inception as content customization tools for the Web. These include anything from health and well-being to tourism and energy efficiency. Many applications (in smart cities and homes, healthcare, and agriculture) have emerged in the past few years thanks to the Internet of Things (IoT). Further, the potential of IoT to act as or on behalf of human beings has widened the range of applications for IoT-based RSs and has enhanced human confidence in the produced (and directly actionable)recommendations. Because of the popularity of RSs as well as their potential profit for sellers, merchants have become more interested in manipulating RSs in their favour [60]. In order for RSs technology to be accepted, it is critical to build confidence in both the information sources (such as users, sensors, etc.) and the recommendation algorithms so that they can withstand adversarial assaults [61, 30]. Blockchain is a decentralised, tamper-resistant ledger that records all transactions in a distributed network, ensuring the privacy, integrity, and security of all data. For RS development, where privacy and trust are crucial values for the decision-making process, its qualities may be employed, and may go beyond existing protocols for privacy-preserving data collecting. When it comes to health care, for example, patients want to disclose their personal information in order to get better medical advice, but they also want to ensure that their data is safe from unauthorised access and alterations [63]. Also, in social networking RSs, users can be concerned about the privacy of their context or preferences (such as not wanting their precise location or the specific goods they browsed) being revealed to others.

W1. Striking features

In contrast to conventional servers, the blockchain is almost never interrupted by breakdown or maintenance. If a transaction does not go through, the system provides an explanation for why it did not go through as expected. In the blockchain, no single user or machine is identified. Open and transparent rules are in place to govern transactions on the blockchain, which uses trusted mathe-matical formulas to govern the conduct of transactions. There is no need for mutual trust to exchange information between nodes in the blockchain networks. While this feature is dependent on the type of blockchain, three main scenarios are identified: I public blockchain, which is completely open; (ii) consortium blockchain, which is open to specific groups or organisations that have been granted permission to access it; and (iii) private blockchain, which is only open to an entity or a specific user with complete internal control. At the transaction level, blockchain guarantees that the property remains and is transferred to the correct people. The whole system is protected against theft, illegal access, duplicate spending, and fraudulent transactions because of the blockchain's decentralised nature. Decentralized ledger based on encryption, consensus, and decentralisation. Each block contains a single transaction (or bundle of transactions). Using a cryptographic chain, all previous blocks are connected to each new block, making it almost hard to break the chain. Even more important is the need for a consensus method to verify that all transactions inside the blocks are valid and genuine. The "public key" and the "private key" are the two asymmetric cyphers that are used in the blockchain to complete the encryption/decryption process. Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC) are two of the most often utilised asymmetric encryption methods in blockchain. In the face of adversity, the blockchain is able to authenticate and transfer ownership of its data in a secure manner, while being immune to a variety of threats. From a variety of viewpoints, the final stability may be observed. Yes, there are instances when the system's responses aren't consistent, however over time the system as a whole finally produces steady answers because of how the blockchain works Furthermore, stability refers to an environment in which blocks are arriving at a steady pace and may be accepted by a fixed peer-to-peer network (P2P). An external observer may determine, indefinitely, which blocks will be authorised by a blockchain-based RS with this kind of stability.

Conclusion

A complete review of blockchain-based RSs is presented in this article. In this paper, we describe current blockchain-based RS frameworks in terms of security and privacy problems, features and working concepts, the possible influence of blockchains, and various forms of blockchain-based RSs and applications. Before determining a set of future paths for increasing the quality of blockchain-based RSs, we explore the limits and outstanding challenges. It's conceivable to create efficient decentralised RSs with comparable accuracy to centralised ones, thanks to blockchain's remarkable properties, which will protect sensitive data and maintain anonymity. It was thus necessary to outline how to construct recommendations engines in accordance with user privacy and security, as well as to increase the user's confidence in RSs. Typically, blockchain has been promoted as a potential solution that may be integrated with RSs to provide answers to unanswered problems, particularly those relating to the protection of security and privacy. Blockchain has been incorporated in Consequently, blockchain may considerably improve recommendation frameworks by assuring the security, integrity of data, confidentiality, and accessibility of the data that is stored on the blockchain. Some problems may arise while constructing blockchain-based RSs, such as in the event of conflicts or misconduct amongst users. This is something to keep in mind. As a result, it is imperative that methods to establish fair procedures, such as atomic swaps inherited from the blockchain, be researched in the near future.

References

[1] J.B. Schafer, J. Konstan, J. Riedl, Recommender systems in e-commerce, in:Proceedings of the 1st ACM Conference on Electronic Commerce, 1999,pp. 158–166.

[2] Y. Deldjoo, M. Schedl, P. Cremonesi, G. Pasi, Recommender systemsleveraging multimedia content, ACM Comput. Surv. 53 (5) (2020) 1–38.

[3] M. Hong, J.J. Jung, Multi-criteria tensor model for tourism recommendersystems, Expert Syst. Appl. 170 (2021) 114537.

[4] S.M. Ghafari, A. Beheshti, A. Joshi, C. Paris, A. Mahmood, S. Yakhchi, M.A.Orgun, A survey on trust prediction in online social networks, IEEE Access8 (2020) 144292–144309.

[5] J. Saha, C. Chowdhury, S. Biswas, Review of machine learning and deeplearning based recommender systems for health informatics, in: DeepLearning Techniques for Biomedical and Health Informatics, Springer,2020, pp. 101–126.

[6] L. Quijano-Sánchez, I. Cantador, M.E. Cortés-Cediel, O. Gil, Recommendersystems for smart cities, Inf. Syst. 92 (2020) 101545.

[7] R. Katarya, N. Verma, Automatically detection and recommendation incollaborative groups, in: 2017 International Conference on IntelligentSustainable Systems, ICISS, IEEE, 2017, pp. 218–222.

[8] B. Deebak, F. Al-Turjman, A novel community-based trust aware recom-mender systems for big data cloud service networks, Sustainable CitiesSoc. 61 (2020) 102274.

[9] G. Gupta, R. Katarya, A study of recommender systems using Markovdecision process, in: 2018 Second International Conference on IntelligentComputing and Control Systems, ICICCS, IEEE, 2018, pp. 1279–1283.

[10] R. Katarya, O.P. Verma, Recommender system with grey wolf optimizerand FCM, Neural Comput. Appl. 30 (5) (2018) 1679–1687.

[11] M. Fu, H. Qu, Z. Yi, L. Lu, Y. Liu, A novel deep learning-based collaborativefiltering model for recommendation system, IEEE Trans. Cybern. 49 (3)(2018) 1084–1096.

[12] H. Zhang, Y. Sun, M. Zhao, T.W. Chow, Q.J. Wu, Bridging user interestto item content for recommender systems: An optimization model, IEEETrans. Cybern. 50 (10) (2019) 4268–4280.[13] R. Katarya, Reliable recommender system using improved collaborativefiltering technique, in: System Reliability Management, CRC Press, 2018,pp. 113–119.

[14] G. Gupta, R. Katarya, Recommendation analysis on item-based and user-based collaborative filtering, in: 2019 International Conference on SmartSystems and Inventive Technology, ICSSIT, IEEE, 2019, pp. 1–4.

[15] G. Gupta, R. Katarya, EnPSO: An AutoML technique for generatingensemble recommender system, Arab. J. Sci. Eng. (2021) 1–19.

[16] Q. Guo, F. Zhuang, C. Qin, H. Zhu, X. Xie, H. Xiong, Q. He, A survey onknowledge graph-based recommender systems, IEEE Trans. Knowl. DataEng. (2020) 1, http://dx.doi.org/10.1109/TKDE.2020.3028705.
[17] K.R. Jerripothula, A. Rai, K. Garg, Y.S. Rautela, Feature-level rating systemusing customer reviews and review votes, IEEE Trans. Comput. Soc. Syst.7 (5) (2020) 1210–1219.

[18] A. Anandhan, L. Shuib, M.A. Ismail, G. Mujtaba, Social mediarecom-mender systems: Review and open research issues, IEEE Accessfuture research possibilities.6 (2018)15608–15628.

[19] M. Eirinaki, J. Gao, I. Varlamis, K. Tserpes, Recommender systems forlarge-scale social networks: A review of challenges and solutions, FutureGener. Comput. Syst. 78 (2018) 413–418.[20] D. Wu, J. Lu, G.