Artificial Intelligence, Deep Learning and Blockchain Based Secure Collaborative Recommender System

C. Jayapratha[1], D. Saravanan[2], R. DelshiHowsalya Devi[3] , T. Sangeetha[4], AB. Hajirabe[1]

[1]Master of Computer Applications, KarpagaVinayaga College of Engineering and Technology, India
Pin: 603 308

[2]Department of Mathematics, KarpagaVinayaga College of Engineering and Technology,
Madhuranthagam - 603 308, Tamil Nadu, India.

[3]Department of Artificial Intelligence & Data Science, Karpaga Vinayaga College of Engineering & Technology, Chengalpattu, India
[4]Department of Biomedical Engineering, Karpaga Vinayaga College of Engineering and Technology, Chengalpattu, India

ABSTRACT

Decentralized recommender systems (RSs) are an attempt to solve the problems that are inherent in centralised RSs by endowing users with an increased level of autonomy and accountability in the decision-making process. This raises a lot of concerns regarding disagreements and inappropriate behaviour, and these are substantial issues. It is essential to both anticipate problems and anticipate solutions that can create a fair process by identifying potential unfair exchanges that could occur during the activity between two or more users. This can be done by identifying potential unfair exchanges that could occur during the activity between two or more users. This can be accomplished by preparing for potential challenges and preparing for potential solutions that can produce an equitable procedure. Deep learning (DL), artificial intelligence (AI), and blockchain technology are the three pillars upon which the secure collaborative recommender system that is provided in this paper.

Keywords: Artificial Intelligence, Deep Learning, Blockchain, Recommender System

1. INTRODUCTION

Recommender Systems (RSs) were initially developed to increase customer satisfaction and repeat business on online shopping sites [1], recommender systems have since expanded into virtually every aspect of online life, including travel itineraries, health monitoring, and smart city infrastructure. RSs are now able to provide recommendations for a wide variety of topics, ranging from films and music to vacation destinations and health monitoring.

It is impossible to deny either the worth of such information about customers or their sensitivity to the matter. Although several studies have investigated the possibility of developing RSs that protect user privacy [2], Most studies that concentrate on developing new algorithms [11] and models ignore privacy and security in favour of improving things like precision and scalability. several studies have investigated the possibility of developing RSs that protect user privacy, [3] Most studies that concentrate on developing new algorithms and models. In addition to this, RSs are susceptible to attacks that are launched from untrusted sources located in the outside world.

Since the advent of cloud computing, protecting sensitive information has become a task that is significantly more difficult to accomplish. This is especially important to keep in mind when thinking about issues relating to privacy and safety. There have been many attempts made to implement various risk reduction techniques; however, none of them have been entirely successful, particularly in the areas of cryptographic security and the protection of the user private information [4].

Despite these numerous attempts, none of the risk reduction techniques have been completely successful. It is common knowledge that blockchain technology has been effective over the course of the past few years in its role as a decentralised technique for maintaining the data integrity of individuals while also protecting their confidentiality. Because this technology has the potential to be used to solve one of the most urgent problems in RSs, researchers from both groups have begun to focus their attention on this inter-disciplinary space. The reason for this shift in attention is since this technology has the potential to be used to solve the problem [5].

It paves the way for the development of distributed RSs, which will use the blockchain database to store data in a safe environment while also isolating it from services. This will be made possible because of the preparations made by this [6]. To determine the current state of the art, it evaluates the relative benefits of several different existing frameworks based on several different metrics, such as the amount of time needed for computation and the level of accuracy of recommendations.

2. RELATED WORKS

RSs that incorporate blockchain have the potential to secure the control of user information by allowing safe data processing for users within online portals. This can be seen as a positive development for the cryptocurrency industry. The blockchain support for secure multiparty computation, which adds smart contracts to the main blockchain-based RS protocol, is what makes this feasible. In this manner, distributed storage solutions that incorporate blockchain have the potential to safeguard user information control.

This is because it uses encryption technologies to protect user data, uses a secure distributed ledger to record transactions, and provides the necessary mechanisms for protecting user data. Because of the combination characteristics along with the complex structure and protocols of blockchain, blockchain-based distributed storage systems are more resistant to manipulation and tampering than traditional storage systems. Conventional storage systems do not have this level of resistance [7].

The authors [8] developed a system that, by utilising smart contracts, permits many users to collaborate simultaneously on a dataset and to make changes to a machine learning model in real time. This system can be found in the paper. After that, the model is made accessible to the public and added to the distributed ledger so that anyone can reason based on it. to guarantee the model consistency about any test collection, it is possible to incentivize both monetary and non-monetary (Gamified) compensation mechanisms for the provision of excellent results. Gamification is one strategy that can be used to accomplish this goal. The distributed ledger technology that underpins Ethereum might be utilised as the fundamental structure for such an application.

A system that is capable of the decentralised generation of knowledge networks is described by [9]. to guarantee transparency, honesty, and auditability, they implement crowdsourcing strategies that are backed by smart contracts, which are made possible by blockchain technology. The efficiency of the system is evaluated using a variety of different case studies, and the decentralised knowledge graph that is generated because studies is used as the foundation for an in-depth recommendation structure. These authors hope that their work will clear the way for future research on the knowledge graph as well as practical applications of the knowledge graph in the real world by presenting an innovative and decentralised strategy for the construction of the knowledge graph.

The authors [10-13] present a data-sharing framework (DSF) scheme that makes use of a blockchain-based decentralised network. Every node in this network can establish direct connections with other nodes, which makes it possible for nodes to share data with one another. The plan also makes use of a data-sharing framework that operates since a decentralised network that is built on blockchain technology. A framework and a path have been established to facilitate the transfer of data between the different categories of nodes. The acquired knowledge is communicated to the user node by the server node in the form of information that was learned through the process of machine learning after the server node has successfully obtained destination assessment data from the user node. The generation of recommendations is dependent upon the successful completion of several steps, one of which is the transmission of data in real time from the sensor to the user router. Every computer that is a part of the blockchain network contributes to the dissemination of data in several different ways, such as by chaining blocks, hashing, and broadcasting. These are just some of the ways that a contribution can be made.

3. PROPOSED METHOD

The blockchain is a decentralised ledger that records all the transactions that take place within a peer-to-peer (P2P) network. Users of RSs no longer require the services of a third-party validator to validate the authenticity of transactions and recommendations made on the platform because the platform makes use of blockchain technology.

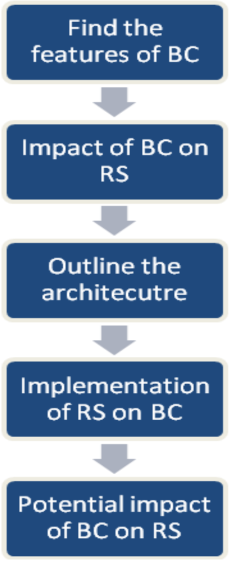

Figure 1: Process of RS

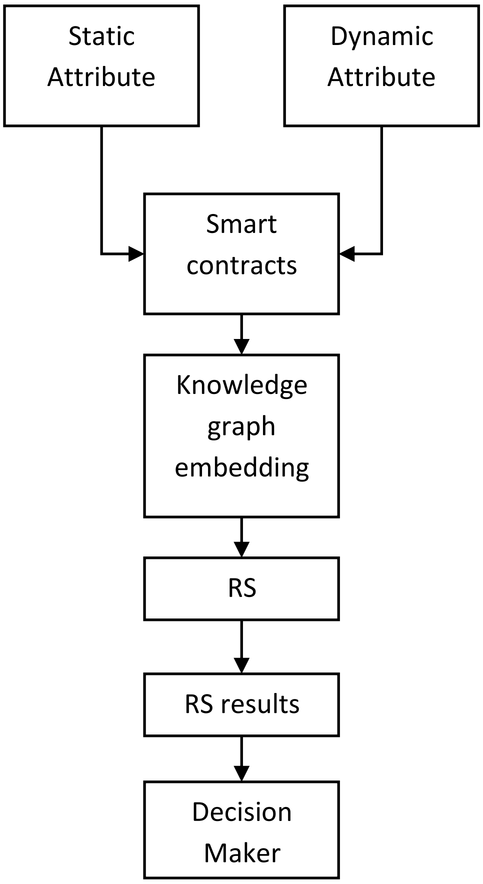

Figure 2: RS-BC architecture

A RS that is based on blockchain technology can be seen in Figure 1-2. Most recommendation systems place a significant amount of importance on the information that is provided by users or vendors in the form of profiles, descriptions, evaluations, ratings, and other information that is very similar. Users can have faith that sensitive data required by RSs, such as their preferences and products selected, digital transactions, special needs, personally identifying information, rating feedback, and so on, will be stored on the blockchain in a secure manner.

Examples of this kind of data include preferences and products selected, digital transactions, special needs, and rating feedback. The owner of the RS is the one who is accountable for gathering and storing any additional data that may be relevant in the blockchain network. This is done with the goal of preventing malware and other forms of vulnerability to the RS.

The utility matrix R, which is comprised of evaluations given by a group of customers U for a group of products This is the essential information that the algorithm in matrix factorization uses. Matrix factorization is the most advanced technique currently available for use in collaborative filtering algorithms for RSs. The technique that is utilised at this time is known as matrix factorization.

We factor the matrix R to acquire user and item profiles and to be able to make recommendations based on approximated ratings for items for which we do not have data. In addition to this, we carry out these steps to finish the matrix. The user evaluations that are submitted through blockchain are encrypted before they are sent to the recommendation engine; matrix derivatives go through a similar procedure through a crypto service provider (CSP).

Algorithm 1: BC-RS

```
Step 1:   Collect user rating
Step 2:   Encrypt the rating
Step 3:   Send the encrypted information to the RS
Step 4:   Mask the rating
Step 5:   Send the masked rating to CSP
Step 6:   Apply matrix factorization
Step 7:   Decrypt at CSP
Step 8:   Set the dimensional vector
Step 9:   Compute encryptions
Step 10:  Send encrypted information to the RS
Step 11:  Update rating matrix
Step 12:  Verify end condition
```

After the user assessments have been collected, the CSP public key is utilised to encrypt them so that they cannot be read. Before being sent back to the CSP, each assessment is first encrypted with a one-of-a-kind disguise that is produced by the recommendation engine. This step ensures that the assessments cannot be read by unauthorised parties.

After decrypting the masked ratings (i.e., rij+mij), the CSP, as a component of the matrix factorization phase, computes their d-dimensional vector representations, encrypts them, and then transmits them back to the RS. This process occurs after the CSP has decrypted the masked ratings.

After the rij and mij have been successfully deciphered, all this will take place. The RS decrypts the vectors that have d dimensions and then discards the mask vectors that correspond to those dimensions so that it can acquire the final approximations. Repeating the method until reaching a predetermined cutoff point is required to complete the process of approximating evaluations.

4. RESULTS AND DISCUSSIONS

The performance of the system is evaluated both before and after an attack to determine how the attack affects the system. the stability of the system investigates how the attack profiles influence the ratings that the system assigns to the object that is being attacked. Robustness measures the performance of the system both before and after an attack.

Experiments involving deep learning are carried out by utilising a software application that has been pre-installed on a computer that has a Core i7 processor. This allows for the experiments to be as realistic as possible. Because it contains 16 gigabytes of random-access memory (RAM) and four processors, each of which operates at 1.7 gigahertz, this machine can handle any kind of task. The overall dataset was subdivided into training, cross-validation, and testing sets so that multiple goals could be achieved. These sets were generated by partitioning off the overall dataset. K-Fold Cross-validation, which can be applied to both the training set and the testing set, was utilised in this examination. The training set consisted of 80% of the dataset.

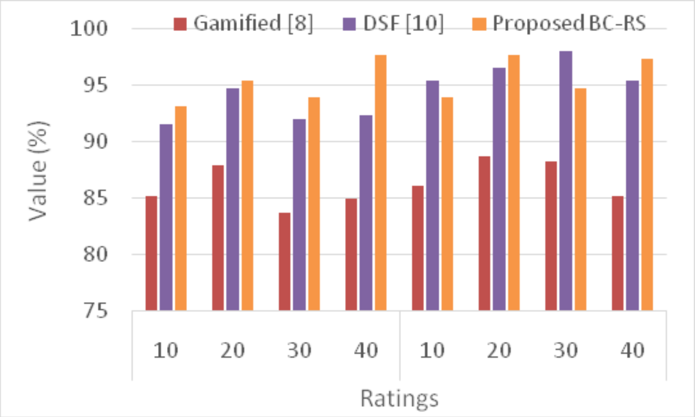

Figure 3: Recall

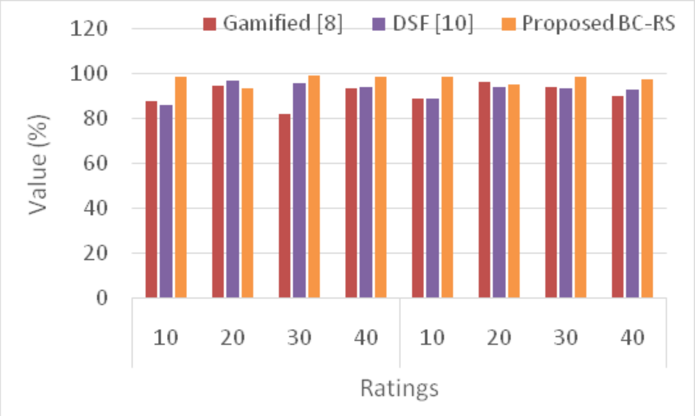

Figure 4: Precision

Figure 4 demonstrates the various metrics that are utilised to evaluate the efficacy of the recommended CF schemes. This is because different research concentrates on different aspects of shilling attacks. This is the case for the following reason: if we look at Figure 3-4, we can see that the training score for precision ultimately reached a maximum of 94% after 100 epochs, which is an increase from the beginning score of 90.5%. This shows that the score increased over time.

In addition, the performance started out at 93%, peaked at 92%, and then dropped all the way down to 85.8% in terms of how accurately the test outcome was predicted. It was found that the efficiency started out at 87.5% and continued to remain relatively constant until about 45 epochs later. This occurred after it had previously been unstable. The blue curve, which depicts the result of the test, also began at 87% and has remained there ever since it was drawn. This indicates that the result of the test was accurate. after 100 epochs it achieved its highest point of 912%, which was its highest point ever.

5. CONCLUSIONS

It has been demonstrated that BC-RS are susceptible to attacks of the type known as profile insertion attacks. These kinds of attacks involve the addition of several fictitious user accounts to the system to exert some sort of influence over the recommendations that are provided to the users. It is necessary to monitor the present state of shilling attacks to design and implement recommendation algorithms or attack detection schemas that are more robust.

REFERENCES

[1] Arora, M., Chopra, A. B., & Dixit, V. S. (2020). An approach to secure collaborative recommender system using artificial intelligence, deep learning, and blockchain. In *Intelligent communication, control and devices: Proceedings of ICICCD 2018* (pp. 483-495). Springer Singapore.

[2] Mantey, E. A., Zhou, C., Anajemba, J. H., Okpalaoguchi, I. M., & Chiadika, O. D. M. (2021). Blockchain-secured recommender system for special need patients using deep learning. *Frontiers in Public Health*, *9*, 737269.

[3] Himeur, Y., Sayed, A., Alsalemi, A., Bensaali, F., Amira, A., Varlamis, I., ... & Dimitrakopoulos, G. (2022). Blockchain-based recommender systems: Applications, challenges and future opportunities. *Computer Science Review*, *43*, 100439.

[4] Ghantous, N., & Fakhri, C. (2022). Empowering Metaverse Through Machine Learning and Blockchain Technology: A Study on Machine Learning, Blockchain, and Their Combination to Enhance Metaverse. *ScienceOpen Preprints*.

[5] Arora, M. (2022). The Latest Trends in Collaborative Security System. In *Recent Innovations in Computing: Proceedings of ICRIC 2021, Volume 2* (pp. 711-723). Singapore: Springer Singapore.

[6] Bosri, R., Rahman, M. S., Bhuiyan, M. Z. A., & Al Omar, A. (2020). Integrating blockchain with artificial intelligence for privacy-preserving recommender systems. *IEEE Transactions on Network Science and Engineering*, *8*(2), 1009-1018.

[7] Porkodi, S., & Kesavaraja, D. (2020). A Trust-Based Recommender System Built on IoT Blockchain Network With Cognitive Framework. *Recommender System with Machine Learning and Artificial Intelligence: Practical Tools and Applications in Medical, Agricultural and Other Industries*, 291-311.

[8] Liang, W., Xie, S., Cai, J., Xu, J., Hu, Y., Xu, Y., & Qiu, M. (2021). Deep Neural Network Security Collaborative Filtering Scheme for Service Recommendation in Intelligent Cyber–Physical Systems. *IEEE Internet of Things Journal*, *9*(22), 22123-22132.

[9] Hannah, S., Deepa, A. J., Chooralil, V. S., BrillySangeetha, S., Yuvaraj, N., Arshath Raja, R., ... & Alene, A. (2022). Blockchain-based deep learning to process IoT data acquisition in cognitive data. BioMed Research International, 2022.

[10] Patel, S. B., Bhattacharya, P., Tanwar, S., & Kumar, N. (2020). Kirti: A blockchain-based credit recommender system for financial institutions. *IEEE Transactions on Network Science and Engineering*, *8*(2), 1044-1054.

[11] Vilma Roseline J, **Saravanan D**, (2022), Hybrid Backward Production Scheduling for Manufacturing Systems, *Indian Journal of Natural Sciences, ISSN: 0976 – 099, Vol.13, Issue 75, PP 51559-51568*

[12] Vilma Roseline J, **Saravanan D**, (2019), Crossover and Mutation Strategies applied in Job Shop Scheduling Problems, Journal of Physics: Conference Series(JPCS), 1377 (2019) 012031 doi:10.1088/1742-6596/1377/1/012031Conference Proceedings.

[13] Uma Sankar G, **Saravanan D**, (2018), Single Objective for an Integer Partial Flexible Open Shop Scheduling Problem Using Developed Ant Colony Optimization, International Journal of Mechanical and Production Engineering Research and Development (IJMPERD) ISSN(P): 2249-6890; ISSN(E): 2249-8001 Vol. 8, Issue 3, Jun 2018, PP 1121-1132.