Journal of Convergence for Information Technology
Vol. 11. No. 8, pp. 36-41, 2021
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2021.11.08.036

Explanable Artificial Intelligence Study based on Blockchain Using Point Cloud

Sunghyuck Hong
Associate Professor, Division of Smart IT, Fintech major, Baekseok University

포인트 클라우드를 이용한 블록체인 기반 설명 가능한 인공지능 연구

홍성혁
백석대학교 스마트IT공학부, 핀테크 전공 부교수

Abstract Although the technology for prediction or analysis using artificial intelligence is constantly developing, a black-box problem does not interpret the decision-making process. Therefore, the decision process of the AI model can not be interpreted from the user's point of view, which leads to unreliable results. We investigated the problems of artificial intelligence and explainable artificial intelligence using Blockchain to solve them. Data from the decision-making process of artificial intelligence models, which can be explained with Blockchain, are stored in Blockchain with time stamps, among other things. Blockchain provides anti-counterfeiting of the stored data, and due to the nature of Blockchain, it allows free access to data such as decision processes stored in blocks. The difficulty of creating explainable artificial intelligence models is a large part of the complexity of existing models. Therefore, using the point cloud to increase the efficiency of 3D data processing and the processing procedures will shorten the decision-making process to facilitate an explainable artificial intelligence model. To solve the oracle problem, which may lead to data falsification or corruption when storing data in the Blockchain, a blockchain artificial intelligence problem was solved by proposing a blockchain-based explainable artificial intelligence model that passes through an intermediary in the storage process.

Key Words : Artificial Intelligence, Explanable Artificial Intelligence, Point Cloud, Blockchain, Oracle Problem

요 약 인공지능을 이용하여 예측이나 분석하는 기술은 지속적으로 발전하고 있지만, 의사결정 과정을 명확히 해석하지 못하는 블랙박스 문제가 존재한다. 따라서 인공지능 모델의 의사결정 과정에서 사용자의 입장에서 해석이 불가능하여 결과를 신뢰할 수 없는 문제가 발생한다. 본 연구에서는 인공지능의 문제점과 이를 해결하기 위한 블록체인을 활용한 설명 가능한 인공지능에 대해 연구를 진행하였다. 블록체인을 이용해서 설명 가능한 인공지능 모델의 의사결정 과정에서의 데이터를 타임스탬프 등을 이용하여 부분별로 블록체인에 저장한다. 블록체인을 이용하여 저장된 데이터의 위변조 방지를 제공하고 블록체인의 특성상 사용자는 블록에 저장된 의사결정 과정등의 데이터를 자유롭게 접근할 수 있다. 설명 가능한 인공지능 모델의 구축이 힘든 것은 기존 모델의 복잡성이 큰 부분을 차지한다. 따라서 포인트 클라우드를 활용해서 3차원 데이터 처리와 가공과정의 효율성을 높여서 의사결정 과정을 단축해 설명 가능한 인공지능 모델의 구축을 원활하게 한다. 블록체인에 데이터 저장과정에서 데이터 위변조가 발생할 수 있는 오라클 문제를 해결하기 위해 저장과정에 중간자를 거치는 블록체인 기반의 설명 가능한 인공지능 모델을 제안하여 인공지능의 블랙박스 문제를 해결하였다.

주제어 : 인공지능, 설명 가능한 인공지능, 포인트 클라우드, 블록체인, 오라클 문제

*This research was supported by 2021 Baekseok University Research Fund.

*Corresponding Author : Sunghyuck Hong (shong@bu.ac.kr)

Received July 6, 2021
Revised July 31, 2021
Accepted August 20, 2021
Published August 28, 2021

1. Introduction

Recently, artificial intelligence technology has been used in various industries, such as natural language processing translation, autonomous driving, medical care, business, and defense, and is now affecting our lives. The basis of this evolution of artificial intelligence technology can be traced to the development of machine learning technologies such as Deep Learning, where artificial intelligence learns on its own based on Big Data. However, there are limitations to the perfect application of this advanced form of artificial intelligence in the real world. Deep Learning, where artificial intelligence learns based on Big Data, has advanced techniques to diagnose, predict and make decisions on complex problems. However, there is a black-box problem that cannot be interpreted by users, including designers, in the decision-making process of artificial intelligence. Thus, problems arise in which the results derived by artificial intelligence are completely unreliable [1-3].

2. Related Work

2.1 Explainable Artificial Intelligence Model

However, this only reduces the gap between humans and artificial intelligence in terms of resulting values and does not solve the black box problem. Therefore, different models have been presented to implement explainable artificial intelligence. In the general classical machine learning artificial intelligence models, a decision tree structure is introduced to infer features based on information such as presented images and pictures and compare the Euclidean distances in the structure with reference features. Based on the compared data, block matrices are created to divide the features into low and high levels, and the artificial intelligence itself is evaluated and referenced. Finally, by combining block matrices with high scores by the artificial intelligence, a judgment base And-Or-Template (AOT) of the decision tree model is created. This allows the user to intuitively understand the decisions made by the artificial intelligence [4]. The optimal question for branching each node in the decision tree is that the information gain (IG) value has a maximum value. When distinguishing from a particular node to the number m of subordinate nodes, the expression for information gain is represented as follows [5,6].

$$IG(D_p, f) = I(D_p) - \sum_{j=1}^{m} \frac{N_j}{N_p} I(D_j) \tag{1}$$

f is the feature value of the data for the branch, D_p is the record on the parent node, and D_j is the record present on the j-th child node. $I(D_p)$ and $I(D_j)$ refer to the data contamination of each record. Nj and Np refer to the number of data in D_j and D_p, respectively. There are three methods to measure data impurity: genie index, entropy and classification error. In the presence of data classified into the number c of classes, the data impurity I(s) can be represented as the genius index when the ratio of data to type i satisfying $1 \le i \le 2$ of of the data present in node s is expressed as p(i/s) [7].

$$I_G(s) = 1 - \sum_{i=1}^{c} p(i/s)^2 \tag{2}$$

In entropy, I(s) is expressed as follows.

$$I_H(s) = -\sum_{i=1}^{c} p(i/s) \log_2 p(i/s) \tag{3}$$

$I_E(s) = 1 - \max p(i/s)$ In classification error, I(s) is expressed as follows.

2.2 Prunning Method

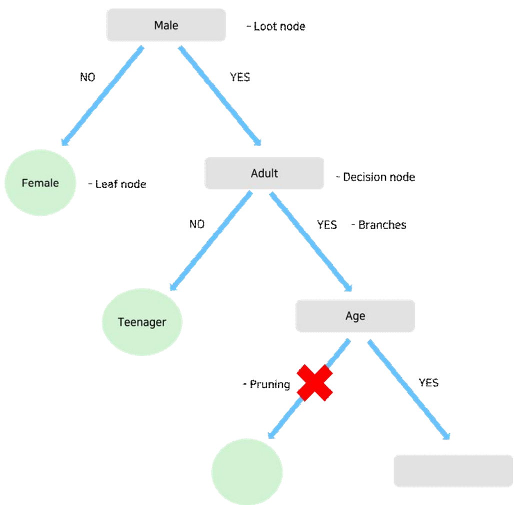
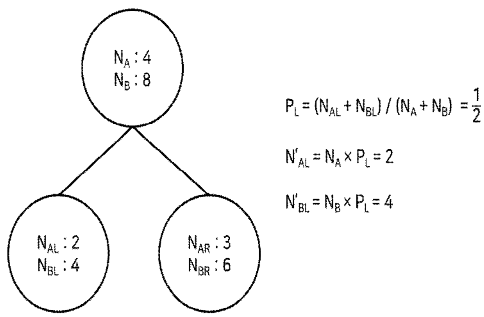


Fig. 1. Decision Tree Model Basic Structure

Fig. 1 is a visualization of the underlying structure of the decision tree. Pruning is performed because increasing the number of branches in the decision tree increases the overfitting rate of the artificial intelligence learning data. When the number of branches increases, the misclassification rate for new data decreases, but when the number of quarters exceeds a certain level, the misclassification rate increases, so pruning of the concept is performed to combine the correct branches instead of discarding the branches. Some examples of pruning methods are creating a whole tree before pruning and evaluating its performance by repeatedly removing branches from leaf nodes. In addition, there is a method for performing pruning based on the generated verification data [7,8].

Another method is the chi-square test. Fig. 2 is an explanation of the chi-square test. P_L represents the rate at which data goes to the left child node, while N'_{AL} and N'_{BL} refer to the expected value of the left child node. Finally, the value of the chi-squared test is determined using the above value. We set any value as the threshold that can be determined as statistically significant. It is considered as meaningful branch if the value of chi-squared is above the threshold value. However, if a value below the threshold is determined, even if the information gain is large, it is considered as a non-meaningful branch, so it does not need to be pruned and no branching is performed during the branching process [8].



$$\chi^2 = \frac{(N'_{AL} - N_{AL})^2}{N'_{AL}} + \frac{(N'_{BL} - N_{BL})^2}{N'_{BL}} + \frac{(N'_{AR} - N_{AR})^2}{N'_{AR}} + \frac{(N'_{BR} - N_{BR})^2}{N'_{BR}} = 1$$

Fig. 2. Example of a Chi-square test

2.3 LIME and Saliency map

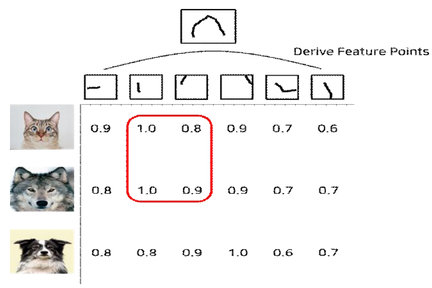


Fig. 3. Decision Tree

Fig. 3 describes the construction of a block matrix divided into low and high levels by deriving feature points from the input images and comparing the Euclidean distances with the reference data. In general, we infer deep networks with a large number of operations. Therefore, it is necessary for Deep

Learning-based artificial intelligence to find ways to reduce the fundamentally complex computations to explain the decision-making process. For proxy models that can mimic the computational processes of Deep Learning, they are structurally simpler than traditional Deep Learning models, making them easier to explain. For linear proxy models (LIME), it is explainable because the process of changing inputs in the decision process is traced. Data is used to construct local linear models that simply serve as proxies for the composition of the entire model. It is used to identify input domains that have the greatest impact on artificial intelligence decision making through different models and problem domains. The proxy model has predictable properties because it can be evaluated and executed by loyalty according to the original system [9].

By computing the input gradient, a saliency map is naturally created. In this process, important information may be overlooked. Therefore, models such as LRP, DeepLIFT, CAM, Grad- CAM, Integrated Gradients and SmoothGrad also consider factors that may carry information other than the gradient [9,10].

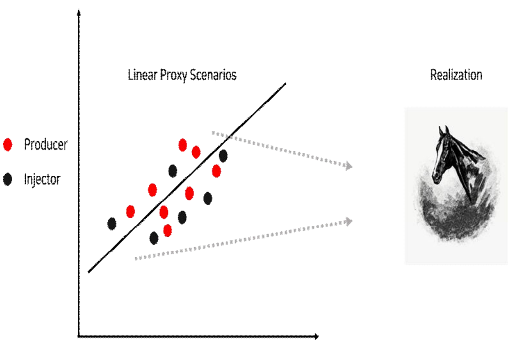


Fig. 4. Extract Linear Proxy Model

Fig. 4 is an illustration that outlines the process of extracting and materializing data through decision making in a linear proxy model. The tracing is intuitive as the results are represented by the input values. Fig. 5 is a figure illustrating the generation of saliency maps that highlight only feature parts except the background by a method that highlights operations related to important parts in general data.

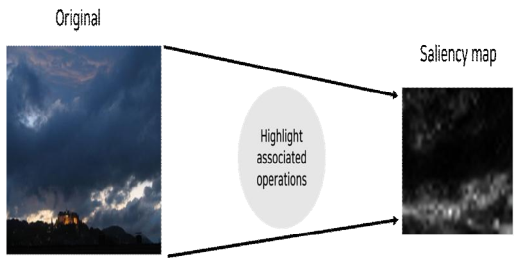


Fig. 5. Saliency Map Extraction

3. Blockchain-based explainable artificial intelligence using point clouds

3.1 Blockchain-based explainable artificial intelligence

Blockchain technology can be used to solve the black box problem, which is an artificial intelligence problem discussed in Chapter 1. Various data, such as input and output data from artificial intelligence models and computational data used in the decision-making process and processed by each node of the neural network, are stored in blocks on the blockchain, sometimes using timestamps. This allows data processed by artificial intelligence to be stored and managed in real time via Blockchain. Blockchain stores and connects data in blocks and can prevent data forgery through user verification, ensuring data integrity. In addition, its decentralized nature allows individual users free access to data. These advantages of blockchain allow users to provide reliability for the decision-making process, which is a description of the results derived from artificial intelligence, and provide transparency and integrity of data [11].

3.2 Take advantage of Point Cloud

A point cloud is a set of points representing information distributed in a three-dimensional space, such as the shape and color of an object, each of which has different properties. Artificial Intelligence basically goes through the process of producing meaningful results through Big Data. Artificial Intelligence can produce incorrect results if there is unverified or meaningless information in a large amount of information. When results are derived from too much data, the efficiency of data processing is reduced and the decision process of the model becomes complex. The more complicated the models become, the more difficult it becomes to build models for explainable artificial intelligence. Point clouds are a set of points with only three features in the form of three-dimensional data, which allows efficient use of storage space and makes it easier to add feature points of objects such as colors and materials. Use point clouds to increase the efficiency of data processing. Accordingly, it increases the efficiency of the decision-making process and the derivation of results, reducing the complexity of the model and facilitating the construction of explainable artificial intelligence models [12,13].

3.3 Oracle Problems on Blockchain

Data that exists outside the blockchain is called on-chain data that exists inside the off-chain. Data that is stored in the blockchain from off-chain to on-chain is called oracle. For data that exists within the blockchain, it is impossible to falsify the data. Data must be stored in the blockchain in order to be managed. Therefore, it is difficult to establish trust when data is not stored on the Blockchain or when data forgery occurs during the storage process. In the process of IoT devices consisting of various sensors collecting data and storing it in the Blockchain, errors or inaccurate data measurements in the device can lead to hardware oracle issues where inaccurate data is stored in the Blockchain. This can lead to errors or inaccurate results in deep learning models. To solve this problem, there is a method using intermediaries that provide reliable data between external and blockchain, such as sensors. For example, organizations or companies with appropriate size and structure, such as data providers Oracle Rise and ChainLink, can play the role of intermediary and first collect data and then provide it to blockchain networks in a stable and systematic way[14,15]. Fig. 6 is a picture of Blockchain-based explainable artificial intelligence.

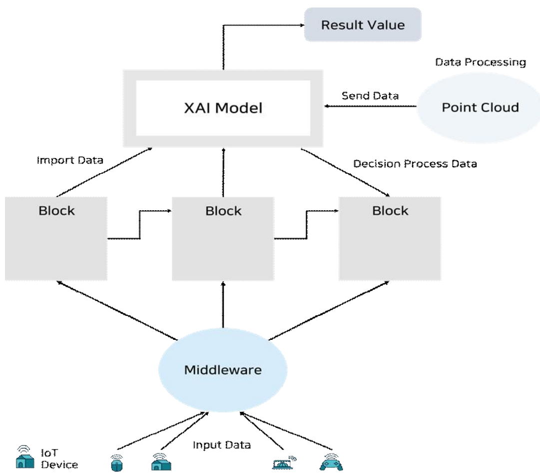


Fig. 6. XAI Model Based on Blockchain with Point Cloud

4. Conclusion

The development of deep learning artificial intelligence has led to superior performance of the model, but there is a black-box problem that makes it impossible to interpret the decision-making process from the user's perspective. Explainable Artificial Intelligence is what enables human users to understand and trust the output of artificial intelligence. Explainable artificial intelligence enables users to understand how the model works and can solve problems in the decision-making process and improve the model. Moreover, explainable artificial intelligence will be a prerequisite for implementing responsible artificial intelligence in the future.

This paper presents a blockchain-based explainable artificial intelligence model that uses point clouds. This ensures prevention of data falsification, which is the advantage of Blockchain, and free access for users by storing operational data of models, etc. in Blockchain.

REFERENCES

[1] M. Ridley. (2019). Explainable Artificial Intelligence. *Ethics of Artificial Intelligence, (299),* 28-46. DOI : 10.29242/rli.299.3

[2] A. Ignatiev. (2020). Towards Trustable Explainable AI. *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence.* DOI : 10.24963/ijcai.2020/726

[3] S. Mahamood. (2019). Explainable Artificial Intelligence and its potential within Industry. *Proceedings of the 1st Workshop on Interactive Natural Language Technology for Explainable Artificial Intelligence* (NL4XAI 2019). DOI : 10.18653/v1/w19-8401

[4] A. Holzinger. (2018). From Machine Learning to Explainable AI. *2018 World Symposium on Digital Intelligence for Systems and Machines (DISA).* (pp. 55-66). IEEE. DOI : 10.1109/disa.2018.8490530

[5] B. S. Miguel, A. Naseer & H. Inakoshi. (2020). Putting Accountability of AI Systems into Practice. *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence.* DOI : 10.24963/ijcai.2020/768

[6] E. Dağlarli, (2020). Explainable Artificial Intelligence (xAI) Approaches and Deep Meta-Learning Models. *Advances and Applications in Deep Learning.* 79. DOI : 10.5772/intechopen.92172

[7] Jo, T. (2020). *Decision Tree.* Machine Learning Foundations, 141-165. DOI : 10.1007/978-3-030-65900-4_73.

[8] F. Mahan, M. Mohammadzad, S. M. Rozekhani & W. Pedrycz. (2021). Chi-MFlexDT: Chi-square-based multi flexible fuzzy decision tree for data stream classification. Applied Soft Computing, 105, 107301. DOI : 10.1016/j.asoc.2021.107301

[9] L. H. Gilpin, D. Bau, B. Z. Yuan, A. Bajwa, M. , Specter & L. Kagal. (2018). Explaining Explanations: An Overview of Interpretability of Machine Learning. *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA).* DOI : 10.1109/dsaa.2018.00018

[10] M. Langer et al. (2021). What do we want from Explainable Artificial Intelligence (XAI)? - A stakeholder perspective on XAI and a conceptual model guiding interdisciplinary XAI research. *Artificial Intelligence, 296,* 103473. DOI : 10.1016/j.artint.2021.103473

[11] M. Nassar, K. Salah, M. H. ur Rehman & D. Svetinovic. (2020). Blockchain for explainable and trustworthy artificial intelligence. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10(1),* e1340. DOI : 10.1002/widm.1340

[12] Z. Zhang, Y. Dai & J. Sun. (2020). Deep learning based point cloud registration: an overview. *Virtual Reality & Intelligent Hardware, 2(3),* 222-246. DOI : 10.1016/j.vrih.2020.05.002

[13] H. J. Kim, K. H. Han & S. S. Shin. (2021). Hash-based SSDP for IoT Device Security. *Journal of the Korea Convergence Society, 12(5),* 9-16.

[14] G. Caldarelli & J. Ellu. (2021). The blockchain ORACLE problem in Decentralized finance - A Multivocal Approach. DOI : 10.20944/preprints202107.0231.v1

[15] G. Caldarelli. (2020). Understanding the Blockchain Oracle Problem: A Call for Action. *Information, 11(11),* 509. DOI : 10.3390/info11110509

홍 성 혁(Sunghyuck Hong) [종신회원]

· 2007년 8월 : Texas Tech University, Computer Science (공학박사)
· 2012년 3월 ~ 현재 : 백석대학교 스마트IT공학부 핀테크 전공 주임
· 관심분야 : 핀테크, 딥러닝, 블록체인, 사물인터넷 보안, 경량보안프로토콜
· E-Mail : shong@bu.ac.kr