applied sciences

MDPI

Article

Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments

Jinsu Kim [1] and Namje Park [1,2,*]

[1] Department of Convergence Information Security, Graduate School, Jeju National University, 61 Iljudong-ro, Jeju-si 63294, Korea; kimjinsu@jejunu.ac.kr
[2] Department of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si 63294, Korea
* Correspondence: namjepark@jejunu.ac.kr

Received: 6 May 2020; Accepted: 7 July 2020; Published: 8 July 2020

Abstract: Artificial intelligence (AI) has a limitation in that it is only in the passive cognition area, so its operating process is not transparent; therefore, the technology relies on learning data. Since raw data for AI learning are processed and inspected manually to assure high quality for sophisticated AI learning, human errors are inevitable, and damaged and incomplete data and differences from the original data may lead to unexpected outputs of AI learning for which processed data are used. In this context, this research examines cases where AI learning data were inaccurate, in terms of cybersecurity, and the need for learning data management before machine learning through analysis of cybersecurity attack techniques, and we propose the direction of establishing a data-preserving AI system, which is a blockchain-based learning data environment model to verify the integrity of learning data. The data-preserving AI learning environment model is expected to prevent cyberattacks and data deterioration that may occur when data are provided and utilized in an open network for the processing and collection of raw data.

Keywords: blockchain; data-preserving; AI; learning; cybersecurity; IoT

1. Introduction

With machine learning and deep learning technologies, artificial intelligence (AI) has been developed at a fast pace to the extent that it can be used commercially, and it has been leading innovation in various fields, including the medical, finance, robot, and culture sectors. Google has been researching to cure incurable diseases through the AI Calico Project by using genetic data and genealogy to extend people's average life span. Besides this, Korea has adopted AI Doctor to control and diagnose diseases. As such, AI technology has been realized not only at a corporate level, but at a national level.

The Ministry of Science and information and communications technologies (ICT) mentioned that obtaining sufficient quality data in the relevant field is crucial for the development of AI algorithms, and they published a dataset establishment plan in many quarters through AI learning data establishment challenges 10. To increase AI's capability to identify hazardous materials, building AI capacity for disease diagnosis, detecting abnormal behaviors from a community, and collecting data from many fields including industry, distribution, medical, history, and culture, the government has been promoting "multi-modal" video data establishment to support the development of AI with integrated cognitive ability and with translation, situation and movement cognition, object and risk element identification, and disease diagnosis data.

The existing AI has not been able to provide sufficient evidence of the results when presenting information on cognition, decisions, and prediction; therefore, explainable AI is required to overcome the limitations of AI, which is restricted to the passive recognition area. EU has increased the demand for an explainable AI algorithm through the General Data Protection Regulation (GDPR), and in 2017, Defense Advanced Research Projects Agency (DARPA) promoted the development of an explainable AI algorithm through the XAI (explainable AI) project. Deep learning has a problem in that transparency of its operating process is not guaranteed due to such functions as the black box of an artificial neural network. To solve this reliability issue, relevant policy and technology are required. In particular, to adopt everyday life AI such as for medical diagnosis and autonomous driving, algorithm verification should be reinforced and data should be accurately used regarding the uncertainty of judgment on the result of the AI's action. It is necessary to conduct technology development for the AI system itself and to minimize errors, while adopting a structure where malicious attacks can be defended against.

In this context, this research examines the need to manage learning data before machine learning by analyzing cases where inaccurate AI learning data were used and cybersecurity attacking methods in terms of cybersecurity, to improve the reliability of AI. We also intend to propose the direction of establishing a data-preserving AI system, which is a blockchain-based learning data environment model for the verification of learning data integrity.

2. Related Research

2.1. AI Cyberthreats

This section describes the need for cybersecurity of AI by examining forgeries or errors in AI learning data. First of all, accidents that have occurred in AI learning data are as follows [1].

AI chatbots' malicious learning: In 2016, Microsoft presented AI chatting robot Tay, but the learning was closed in 16 h because of intentional messages of racial and sexual discrimination included in the learning. Microsoft-made AI chat robot Zo also showed similar problems despite precautions having been taken [2].

Adversarial patch-based attacks: Google Research Group announced the Adversarial Patch, which can make the image recognition AI algorithm malfunction. Adversarial patch, a patch with round-shape abstract images, caused malfunction in the AI algorithm, which recognized an image when the printed patch was stuck to an object [3].

Error in pre-qualifying the recidivism rate in Brown County of Florida, USA: The COMPAS (Correctional Offender Management Profiling for Alternative Sanctions)'s prediction of recidivism for 7000 arrests over the two years of 2013 and 2014 was racially biased, with a 44.9% chance that African Americans would not repeat crimes, about twice as much as 23.5% of whites. It was also incorrectly predicted that white people, repeat offenders, had a 47.7% chance of not re-offending, while African Americans had a 28% chance of not re-offending [4].

Forgery of medical records through deep learning: The AI research group of Ben-Gurion University of the Negev in Israel conducted an experiment where malware generated through deep learning technology was used to manipulate patients' 3D scan images, deceiving all of three doctors. At that time, the problem that 3D CT (Computed Tomography) images, X-ray, and MRI were distributed without a security system was raised [5].

Deepfake using AI: In late 2017, fake videos appeared on the U.S. social news website Reddit through Deepfake, which changes faces using a swapping algorithm, and it was difficult to winnow the truth from falsehood. At that time, it was claimed that responses to the leakage of AI learning data from AI technology platforms should be prepared [6].

The above cases revealed that AI processing myriad data is vulnerable to inappropriate or incomplete data, and when malignant data are applied, incorrect and wrong outputs can be derived regardless of the AI functions and performance. There is a security risk that an attacker may exploit AI based on its efficiency and dissemination by using data or carrying out attacks disturbing the AI

system. In other words, when data forgery occurs due to cyberattacks, the effect of AI learning and learning concepts can be damaged, so data control is required before providing AI learning data.

2.2. Trends in Related Research

With the importance of AI learning data increasing, services to collect and process learning data are increasing; recently, research on the convergence of blockchain and AI has been underway. This section introduces related research on the link between AI data and blockchain, the base technology of the AI learning data environment model that is proposed in this research.

Kim (2019) made blocks directly collect data in parallel in the blockchain structure, compared data collected by each block with data of other blocks to sort out high-quality data only, and eventually established a learning dataset with data selected through comparison [7].

Aum (2019) established a stable data storage system in preparation for hacking, through the AI learning data productivity improvement system and method, which is based on labeled data management using blockchain [8]. He proposed a blockchain-based data management method and device which helps in the effective utilization of the storage resources of blockchain nodes [9].

Research conducted by Asaph (2016) proposed a data sharing mechanism based on blockchain for medical research purposes.

3. Proposed Method

3.1. Characteristics of AI Learning Data

Various types of AI technology, including deep learning, are composed of analysis and learning algorithms, computing systems, and data learning directly related to the sophistication of algorithms. For AI learning, data examples are needed, and to develop an AI model with a specific feature, an appropriate dataset should be established for learning. The learning flow of AI machine learning is as shown in Figure 1, and generally, data to be applied to the AI model follow the process below.

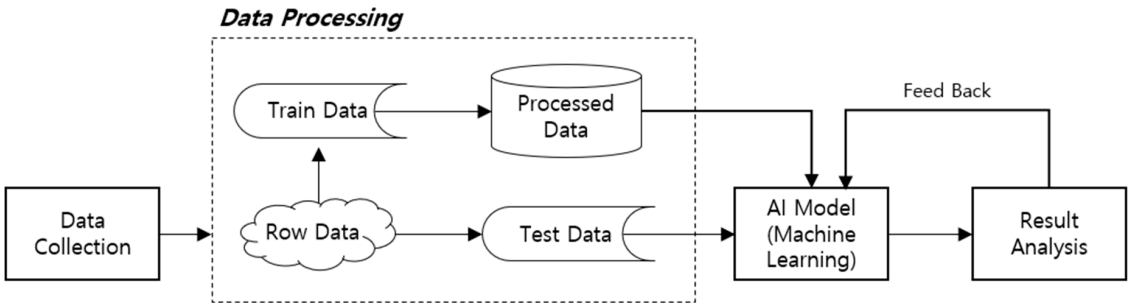

Figure 1. Artificial intelligence (AI) machine learning flow.

Data Collection: This is a stage for collecting non-structured data, including images, texts, and voice. In this stage, the first preprocessing is carried out, which is extracting data fit for the purposes and functions of the AI to be developed.

Data Preprocessing: In this stage, the collected data are converted in order to enter them in the machine learning model, including filling or deleting missing values, selecting or deleting data properties, combining existing data properties, and converting raw data into a designated type as needed.

Data Analysis: In this stage, data are analyzed to be applied to AI, including exploring standardized data patterns, data mapping, extracting data based on exploration and inference, and data learning using some of the data.

Raw data in the course of data collection have some noise, have no consistency, and are often repeated, so they are not suitable for application to AI algorithms. To ensure high quality, reliability, accuracy, and performance, a stage for improving the quality of data is necessary; in this stage,

data analysis and organization is conducted with professionalism and insight, including modification of data errors, elimination of overlapping data, deletion of inconsistent data, and coordination of data conflicts. Preprocessing of data accounts for 80% of the entire process [10–14]. Obtaining a sufficient amount of high-quality data is crucial for the development of AI, and quality assurance of AI learning data is required.

3.2. Requirements for AI Learning Data

Currently, AI technology is not able to provide sufficient grounds for results, and its operating process is not completely transparent and is limited to the passive recognition area. Due to these limitations, AI has come to have a vulnerability in that it is dependent on the data it learns. Also, there is a concern over AI security threats to vulnerabilities caused by AI's duplicity—helpful and hazardous—and its black box structural feature. Table 1 outlines the attack techniques against machine learning.

Table 1. Attack techniques applicable to AI.

Attack Method	Description
Poisoning attack	A type of adversarial attack that injects a hostile sample (completely new malicious learning data) into a training data set, disrupting the availability and integrity of a machine learning model.
Evasion attack	Attacks that significantly reduce the overall security of the target system by generating some hostile samples (some malicious data within normal learning data) so that an attacker can evade detection.
Impersonation attack	Generating specific hostile samples so that existing machine-learning-based systems use a different label than the impersonated sample to misclassify the original sample.
Inversion attack	An attack that collects some basic information about the target system model by using the API (Application Programming Interface) provided by the machine learning system and reversely analyzes the basic information to steal sensitive information.

Table 1 shows attack techniques applicable to AI and which use AI's vulnerability to malignant data. Data integrity is thus required for AI learning [15–20].

In particular, raw data need manual processing and inspection to secure data quality for sophisticated AI learning; therefore, human errors are inevitable. Damaged and incomplete data, as well as differences from raw data, may lead to unexpected outputs when the AI learns the processed data. In other words, in the course of establishing an AI model, the processed learning data need to be monitored to verify the AI's different outputs, and at this time, the integrity of the raw data should be guaranteed [21–24].

There are various services of collecting and processing data to be applied to AI, but the reliability of information is still an issue. The source of copious unreliable data uploads for malicious purposes needs to be analyzed and identified, and a traceable learning data collection environment is required. In general, the central server exists to control open data, so if an intermediary server stops or is modulated, many security threats can occur, including degradation of information reliability and availability. In addition, AI learning data present a type of big data in the course of collection, so the stability of a big data server is required [25–29].

To prevent data forgery and assure data integrity, in this research we propose a blockchain-based learning data management method.

3.3. AI Learning Environment Model

When an AI learning model learns using raw data as they are or data processed for learning, data forgery caused by a third party's malicious attack must be prevented. Particularly, when collecting raw data from a number of data providers through an open network and using them as learning data, personal information must be protected through encryption of the raw data [30].

The proposed learning environment model for data-preserving AI based on blockchain satisfies the integrity requirements of raw and processed data for AI learning using the structure of blockchain, and it ensures that AI learns with data that are not modulated before AI learning data are provided [31,32].

Figure 2 shows the structure proposed in this research, where raw data received from at least one data provider and the hashcode of the raw data are stored in blockchain, the stored raw data are provided to the AI learning model, and then the hashcode of the data used for AI leaning model is compared with the hashcode of the raw data stored in blockchain to verify data integrity. Raw data for AI learning enable the fundamental prevention of raw data forgery and accurate tracking of the data provider in an open network environment.

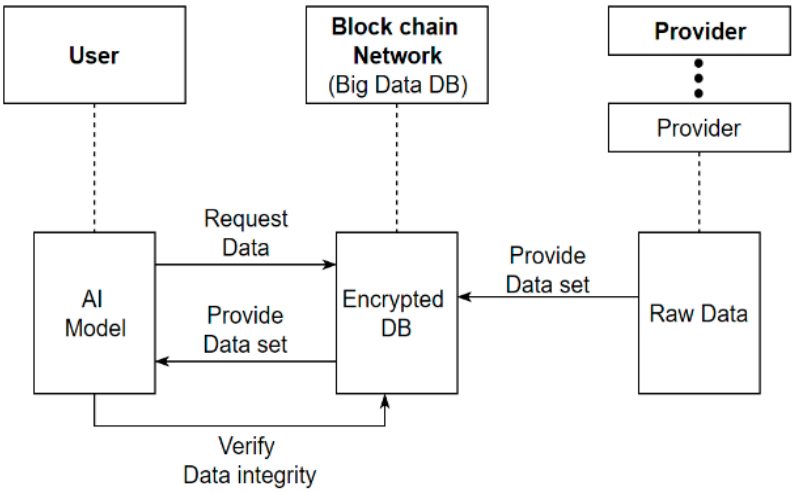

Figure 2. Blockchain-based AI learning data open network.

Blockchain stores raw data by encrypting the block data of the raw data received from the data provider, along with the hashcode, in a block composed of a block header and block data, or separately forms block data storing the hashcode of raw data to ensure convenience at the time of processing raw data according to the characteristics of the AI model.

The application of block chain in this research can ensure data integrity with the fact that AI learning data are not forged according to inflexibility. Furthermore, it provides safety against malicious attacks and incapacitation of the server, such as DDoS (Distributed Denial Of Service), and prevents manipulation by an insider. In addition, it is free from data leakage thanks to block encryption of the learning data and enables tracking of data for AI outputs.

3.4. AI Verification Environment Model

In the AI learning environment, data should be verifiable through tracking of raw data and processing data. Figure 3 shows the configuration to verify the integrity of AI learning data. The verification node of the system connected with the AI server over wired and wireless networks conducts verification of the data through connection with the blockchain server. The verification node receives data from the data provision node and stores it in blockchain, and upon the AI server's request for data, the data stored in blockchain are provided to the AI server. This process forms a verification environment for AI learning. The data provider layer in the verification environment model transmits raw data and their hashcode to the data layer. The data layer for data management and collection

encrypts the data and hashcode received from the provider layer and stores them in blockchain. The AI machine learning layer receives the data and encrypted hashcode from the data layer, teaches the AI, and derives results through learning patterns for model management.

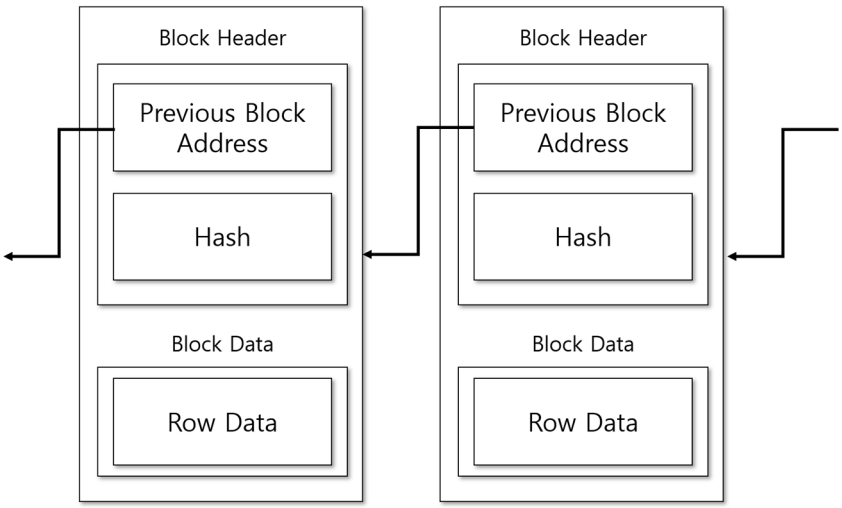

Figure 3. Proposed block configuration.

The verification node encrypts and stores data received from the data provision node in blockchain with the encryption key and decryption key, or encryption and decryption keys created in the verification node can be received by the data provision node to enable the data provider to provide data after encryption using the encryption key received at the time of data provision. This allows data encryption using the same encryption key for a number of data users in an open network, which has the effectiveness of managing only a single decryption key.

Table 2 shows components in the AI Verification Environment Model and consists of storage, providers, and validation.

Table 2. Construct of verification.

Scope	Description
Storage	Save data hashcode with data storage. Store hashcodes together in one blockchain or save each one separately.
Provider	When requesting data from AI server, it is transmitted to the data server and stored in blockchain. Provided after decrypting the encrypted data in data encryption mode.
Verification	Integrity verification using the hashcode of data stored in blockchain. Compare the hashcode of data received from the AI server to the hashcode of data stored in blockchain.

Figure 4 shows the overall structure of the AI environment for verification of the proposed model.

Upon request for the verification of data and its hashcode being received from the AI server, the encrypted hashcode of the corresponding data is transmitted to the provision module from the block chain ledger in the data storage module. In the provision module, the encrypted hash value is decrypted and transmitted to the verification module. In the verification module, the decrypted hashcode and the hashcode of the data received from AI are compared to verify whether it is forged.

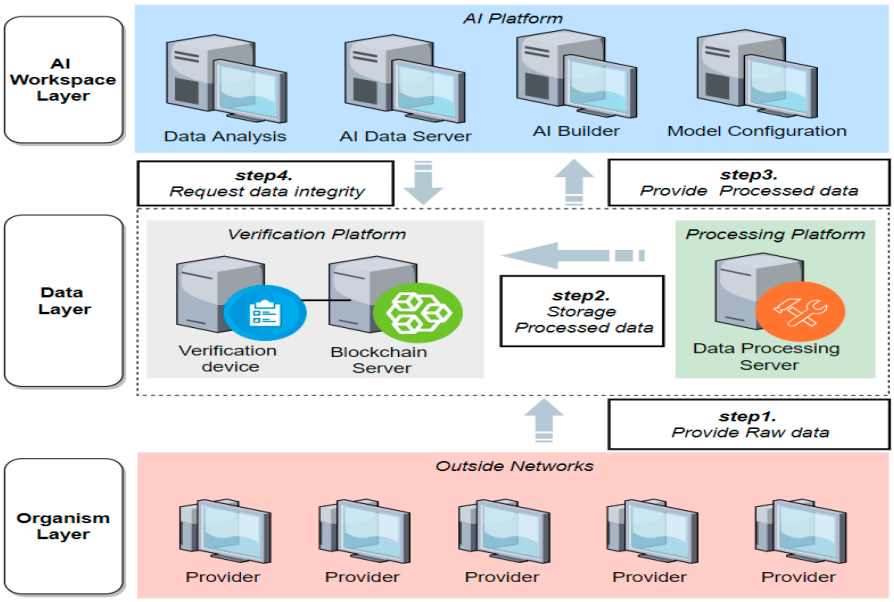

Figure 4. AI environment structure for verification.

3.5. Comparative Analysis with the Existing Research

Research on AI learning data focuses on the provision of quality learning datasets for the service of collecting and processing data required for the development of AI models, as well as on the development of processing and inspection processes and AI-based automated tools. Moreover, research on compensation methods for the collection of AI learning data is increasing, for example, in the decentralized data exchange protocol and network that induces the disclosure of personal data used for AI models, there is a system where a person uploading data is rewarded with cryptocurrency, and a framework where an interactive interface developer or a data holder provides value for the network and is compensated.

The AI learning environment model proposed in this research collects and stores learning data for AI machine learning through blockchain to assure data integrity as well as confidentiality through encryption. This enables for tracking and verifying AI learning data and securing the reliability of AI models. In addition, when providing and utilizing data on an open network for data processing and the collection of raw data, cyberattacks, damage of data, and other threats can be prevented. In short, this research emphasizes the need for security in the AI environment, and we propose an environment model to guarantee the integrity of learning data by focusing on securing reliability for sophisticated AI learning, which is a difference from other previous research. The studies have something in common in that they are AI learning about low data, but in the case of existing AI learning, they aim to generate higher-quality information through processing and compensation for the collected data, but collected on public networks. It is difficult to ensure the integrity of these data. On the other hand, the proposed methodology ensures the integrity of the collected data through blockchain and allows us to track the process when malicious AI learning is induced. Figure 5 shows how the AI server and provider server are applied to the block structure.

A typical AI learning model is often configured on a single server, so it is difficult to ensure the integrity of the collected data, and the data collected and recorded on the server are learned by the learning model. At this time, the integrity of data collected for use in learning cannot be ensured in the server record before they are processed for learning. In this case, the AI learning model assumes that no forgery has been carried out for the learning environment, and in the event of forgery, it is difficult to determine when or why it occurred. In response to these problems, the architecture of the linked list in which the blocks of data are generated one by one increases the difficulty of falsifying the data and further enhances the integrity of the data by applying a distributed ledger structure in which the block

data are shared by network participants to recognize more than half of the data as the ledger. This can provide more stable learning data in the AI learning environment. Figure 6 illustrates the difference between the general AI learning environment model and the proposed AI learning environment model.

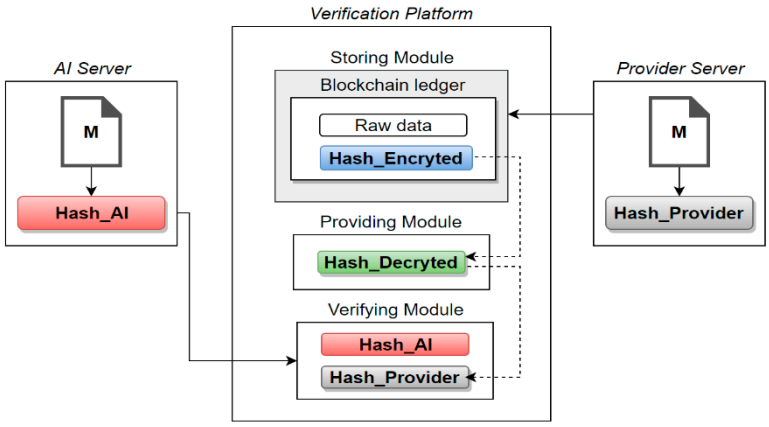

Figure 5. Process of verification for AI data.

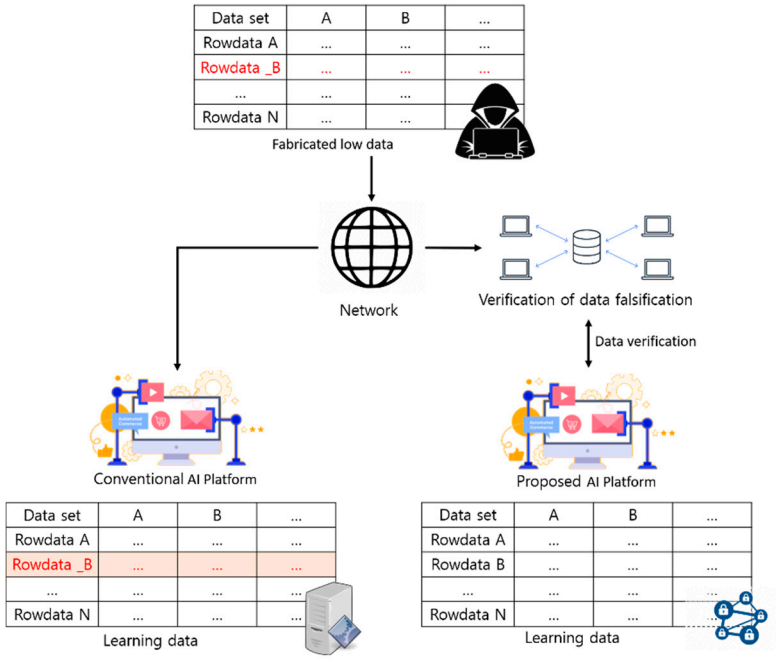

Figure 6. Comparing common AI learning models with the proposed AI learning model.

The model proposed in this paper is based on a distributed and open-source system through a peer-to-peer (P2P) environment that enables data recording by various participants on the network without applying a separate trust organization by instead applying a blockchain. Scalability can be guaranteed, and the contents of each block can be shared by all participants in the transaction records to provide transparency of raw data for learning. Also, since information about data is shared with all users on the network, it is difficult to manipulate data by consensus algorithm, thereby enhancing security, and unlike a normal network, failure on one node has no absolute effect on the system.

Based on the above characteristics, it is possible to highlight the difference from the general system.

Dispersibility: The generally applied network has a single server and aims to provide a server-dependent service. In this way, error in the server can be solved at a single point, and since the service provider has authority for the server, it is free to modify. However, the integrity of the data cannot be guaranteed, and the data of a system for which integrity is not guaranteed cannot

be trusted. In this regard, a blockchain that applies a distributed network to a system where data integrity is prioritized over ownership of the system can provide improved services when compared to a general network.

Scalability: In the case of the general network service, the axis, connection, and expansion of the service can be performed by the provider that provides the service. This may be more effective in services that do not need to be modified externally. Scalability through the use of open source in a distributed network can be proposed by various participants, and it is possible to provide an environment in which flexible services can be created, but a method to limit services by untrusted proposers is required.

Transparency: Data of general network services depend only on the data recorded on the server and are not shared with participants. This method can be applied as a more effective method for personal information. However, in the case of blockchain, since the recorded data are shared by all participants, the shared data can be transparently provided to all participants; it is thus possible to guarantee transparency of the data, but it is necessary to study security measures to protect information.

Security: General network services tend to rely on a single server, which presents a problem in that integrity can be compromised through forgery and alteration of the server. For such a problem, the strategy of the learning environment that applies blockchain is to ownership the data by a majority of users who share the data, and some errors can be corrected by having a large number of data. However, there is a possibility that the collected data may not have been provided in a reliable environment, and research on a mechanism for reliably collecting the data is required.

Stability: In the case of a network service that relies on a single server, the service may be stopped due to a fatal error of the central server, which degrades system availability. In this regard, the learning environment using blockchain has a minimal impact on service due to fatal error of a single node in the distributed network and can thus provide stable services. Table 3 shows a comparative analysis of the learning model in the existing general learning environment and the learning environment model using blockchain.

Table 3. Comparative analysis with existing research.

	Conventional AI Learning Environment Model	**Proposed AI Learning Environment Model**
Research element	Raw data for AI learning	
Purpose	- Collect and process data for AI models - Compensation through decentralized data collection	- Ensure AI learning data integrity - Prepare for AI environmental infringement accidents from cyber attacks
Characteristic	- Providing and processing high-quality datasets - Interface environment with data providers and AI model developers	- Verifiable data audit through AI training data tracking - Traceable when there are unintended AI results due to processed data

3.6. AI Learning Environment Module Case Study

For current AI learning environment modules, learning data are usually added by learning guides, or data on the network are automatically collected for use in learning modules. As such, various studies are being conducted that apply a combination of block chain and AI learning systems, and many of them are being applied to IoT systems with enhanced convenience. The paradigm shift to smart cities, a new target created by advances in digital technology, is taking place; in such a society, block systems have demonstrated the potential for convergence between blockchains and AI, noting that they can be a solution to solve problems in various areas of the public and society [33]. In addition, AI, which is used as a powerful tool for big data analysis, has problems such as centralized architecture and security of personal information, resource constraints, and insufficient training data [34]. AI's learning environment should establish the overall direction of the system, and being able to lead the system to the wrong environment by an act of integrity infringement by outsiders on the learning environment, as a major environment, has a significant impact on the final outcome. We can provide a more stable AI learning environment by ensuring the integrity of the learning environment.

In general, the learning environment of artificial intelligence can be attacked externally, and attacks on the learning environment are largely adversarial attacks, poisoning attacks, and evasion attacks.

In the case of adversary attack, incorrect data are injected into the learning environment; this attack changes the appearance of the data being learned so that the AI does not properly understand the original target. These attacks have been applied to Tesla's automatic control system. This was achieved by the Keen Security Lab in Tencent, China, where three dots were painted on the road and driven on using Tesla's electric vehicle self-driving system, which mis-recognized lanes and began reverse-driving them [35]. The adversary attack is difficult to resolve in the proposed mechanism, which allows an attacker to compromise the data collected in the learning environment to reach a different conclusion from the data learned in artificial intelligence.

Poisoning attack is a prime example of an attack that intentionally allows an attacker to proceed with the intended learning from the beginning of the learning process, and Microsoft's chatbot Tay was quickly completed by learning malicious comments by some malicious users, resulting in problems such as abusive language, sexism, racism, and excessive use of provocative political remarks. Poisoning attack is an example of how to attack the learning model itself, which shows that filters are required for early learning data, and it is difficult to resolve under the proposed mechanism because it is not an attack that undermines the integrity of the entered learning data.

The evasion attack is not easily distinguishable in the eyes of a typical person by the way in which an attacker tampers with learning data to attack a learning model, and it can be perceived as modulated learning data as a result of learning. One study produced hostile examples of images and conducted evasive attacks, and they found that from a typical human perspective, they were successful with a 93% chance [36]. Such an attack can be prevented by preventing the forgery of entered data in the mechanism proposed due to tampering with learning data.

The proposed mechanism may, through the above examples, enhance the integrity of the entered data, but it is difficult to ensure the integrity of the data before they are entered, and further research is required on ways to enhance the integrity of the data before input.

4. Conclusions

To resolve the problem of uncertainty of determination in AI results, it is necessary to develop technology embedded in the system, for example, for the strengthened verification of the algorithm and the use of accurate data, while minimizing errors and defending against malicious attacks. In this context, in this research we examined the need for the management of learning data before conducting machine learning, by analyzing cases of the use of inaccurate AI learning data and cyberattack techniques in terms of cybersecurity, ultimately to improve the reliability of AI. We also proposed a data-preserving AI system configuration, which is a blockchain-based learning data environment model to verify the integrity of learning data. The framework proposed in this research collects and stores the blockchain structure of learning data, which is a base for AI machine learning, ensures data confidentiality through encryption and data integrity, and also secures the reliability of the AI model through monitoring and verification of AI learning data. Overall, it is expected to contribute to preventing threats such as cyberattacks and data deterioration that can occur at the time of data processing or data provision and utilization in open networks for the collection of raw data. The proposed AI learning environment model treats data as normal data in a block chain environment, a learning environment recorded for learning. However, the collected data not only contain data by legitimate users, but may also contain data collected by third parties. Future research is required on how to collect reliable data in unreliable network environments.

Author Contributions: Conceptualization, methodology, investigation, writing—original draft preparation, project administration, J.K.; validation, formal analysis, data curation, writing—review and editing, supervision N.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) [2019-0-00203, The Development of Predictive Visual Security Technology for Preemptive Threat Response]. This work was also supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5C2A04083374).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Moon, Y. *The Malicious Use of Artificial Intelligence Forecasting, Prevention, and Mitigation*; NIA Special Report, 2018-12; National Information Society Agency (NIA): Seoul, Korea, August 2018.
2. Fuchs, D.J. The Dangers of Human-Like Bias in Machine-Learning Algorithms. *J. Mo. ST's Peer Peer* **2018**, *2*, 1.
3. Brown, T.B.; Mané, D.; Roy, A.; Abadi, M.; Gilmer, J. Adversarial patch. In Proceedings of the 31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA, 4–9 December 2017.
4. Dressel, J.; Farid, H. The accuracy, fairness, and limits of predicting recidivism. *J. Sci.* **2017**, *4*, eaao5580. [CrossRef] [PubMed]
5. Mirsky, Y.; Mahler, T.; Shelef, I.; Elovici, Y. CT-GAN: Malicious tampering of 3D medical imagery using deep learning. In Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, 14–16 August 2019; pp. 461–478.
6. Güera, D.; Delp, E.J. Deepfake video detection using Recurrent neural networks. In Proceedings of the 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 27–30 November 2018.
7. Kim, Y.; Woo, J.; Lee, J.; Shin, J.S. High-quality data collection for machine learning using block chain. *J. Korea Inst. Inf. Commun. Eng.* **2019**, *23*, 13–19.
8. Aum, S. Artificial Intelligence Learning Data Productivity Improvement System based on Label Type Data Management Using Block Chain, and Method Thereof. KR Patent 1020180153330, 3 November 2018.
9. Aum, S. Automatic Inspection System for Label Type Data Based on Artificial Intelligence Learning to Improve Data Productivity, and Method Thereof. KR Patent 1020180153327, 3 November 2018.
10. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using blockchain for medical data access and permission management. In Proceedings of the Conference of Open and Big Data, Vienna, Austria, 22–24 August 2016; pp. 25–30.
11. Woo, Y.; Lee, S.; Choi, W.; Ahn, C.; Baek, O. Trend of Utilization of Machine Learning Technology for Digital Healthcare Data Analysis. *Electron. Telecommun. Trends* **2019**, *34*, 98–110.
12. Park, N.; Kim, B.; Kim, J. A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission. *Electronics* **2019**, *8*, 735. [CrossRef]
13. Kim, J.; Park, N.; Kim, G.; Jin, S. CCTV Video Processing Metadata Security Scheme Using Character Order Preserving–Transformation in the Emerging Multimedia. *Electronics* **2019**, *412*, 412. [CrossRef]
14. Park, N.; Sung, Y.; Jeong, Y.; Shin, So.; Kim, C. The analysis of the appropriateness of information education curriculum standard model for elementary school in Korea. In Proceedings of the International Conference on Computer and Information Science, Singapore, 6–8 June 2018; Springer: Berlin, Germany, 2018; pp. 1–15.
15. Lee, D.; Park, N.; Kim, G.; Jin, S. De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment. *J. Peer Peer Netw. Appl.* **2018**, *11*, 1299–1308. [CrossRef]
16. Lee, D.; Park, N. Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment. *J. Pers. Ubiquitous Comput.* **2018**, *22*, 3–10.
17. Lee, D.; Park, N. Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance. *Supercomputing* **2017**, *73*, 1103–1118. [CrossRef]
18. Park, N.; Bang, H. Mobile middleware platform for secure vessel traffic system in IoT service environment. *J. Secur. Commun. Netw.* **2014**, *9*, 500–512. [CrossRef]
19. Park, N.; Kang, N. Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle. *J. Sens.* **2015**, *16*, 1–16. [CrossRef]
20. Park, N.; Kwak, J.; Kim, S.; Won, D.; Kim, H. WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment. *J. AWNTA* **2006**, 741–748. [CrossRef]

21. Park, N.; Hu, H.; Jin, Q. Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT). *J. Distrib. Sens. Netw.* **2016**. [CrossRef]
22. Se, J. Business Value of Blockchain and Applications of Artificial Intelligence. *J. AJMAHS* **2018**, *8*, 779–789.
23. Ku, J.H. A Study on Adaptive Learning Model for Performance Improvement of Stream Analytics. *J. Converg. Inf. Technol.* **2018**, *8*, 201–206.
24. Choi, J. A study on the standardization strategy for building of learning data set for machine learning applications. *J. Digit. Converg.* **2018**, *16*, 205–212.
25. Frost, R.; Paul, D.; Li, F. AI pro: Data processing framework for AI models. In Proceedings of the IEEE 35th International Conference on Data Engineering (ICDE), Macau SAR, China, 8–11 April 2019; pp. 1980–1983.
26. Aoaddah, A.; Elkalam, A.A.; Ouahman, A.A. FairAccess: a new Blockchain-based access control framework for the Internet of Things. *J. Secur. Commun. Netw.* **2017**, *9*, 5943–5964. [CrossRef]
27. Lee, J.; Kang, S.; Kim, S. Study on the AI Speaker Security Evaluations and Countermeasure. *J. Korea Inst. Inf. Secur. Cryptol.* **2018**, *28*, 1523–1537.
28. Kim, J.; Kim, S.; Park, N. Face Information Conversion Mechanism to Prevent Privacy Infringement. *J. KIIT* **2019**, *17*, 115. [CrossRef]
29. Kim, J.; Park, N. Inteligent Video Surveilance Incubating Security Mechanism in Open Cloud Environments. *J. KIIT* **2019**, *17*, 105–116. [CrossRef]
30. Park, N.; Kim, M. Implementation of load management application system using smart grid privacy policy in energy management service environment. *Clust. Comput.* **2014**, *17*, 653–664. [CrossRef]
31. Lee, D.; Park, N. A Proposal of SH-Tree Based Data Synchronization Method for Secure Maritime Cloud. *J. Korea Inst. Inf. Secur. Cryptol.* **2016**, *26*, 929–940. [CrossRef]
32. Lee, D.; Park, N. A Secure Almanac Synchronization Method for Open IoT Maritime Cloud Environment. *J. Korean Inst. Inf. Technol.* **2017**, *15*, 79–90. [CrossRef]
33. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.-H. Convergence of Blockchain and Artificial Intelligence in IoT Network for the Sustainable Smart City. *Sustain. Cities Soc.* **2020**, *1*, 102364. [CrossRef]
34. Singh, S.K.; Rathore, S.; Parkm, J.H. BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. *Future Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
35. Eykholt, K.; Evtimov, I.; Fernandes, E.; Li, B.; Rahmati, A.; Xiao, C.; Prakash, A.; Kohno, T.; Song, D. Robust physical-world attacks on deep learning visual classification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Salt Lake City, UT, USA, 18–22 June 2018.
36. Qian, Y.; Ma, D.; Wang, B.; Pan, J.; Wang, J.; Chen, J.; Zhou, W.; Lei, J. Spot Evasion Attacks: Adversarial Examples for License Plate Recognition Systems with Convolutional Neural Networks. *Comput. Secur.* **2020**, *95*, 101826. [CrossRef]