Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9873156, 1 page
https://doi.org/10.1155/2023/9873156

Retraction

Retracted: Research on Machine Learning Algorithm for Internet of Things Information Security Management System Research and Implementation

Wireless Communications and Mobile Computing

Received 18 July 2023; Accepted 18 July 2023; Published 19 July 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] W. Jiang, "Research on Machine Learning Algorithm for Internet of Things Information Security Management System Research and Implementation," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 8933468, 6 pages, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8933468, 6 pages
https://doi.org/10.1155/2022/8933468

Research Article

Research on Machine Learning Algorithm for Internet of Things Information Security Management System Research and Implementation

Weixiang Jiang

School of Software and Big Data, Changzhou College of Information Technology, Changzhou Jiangsu 213164, China

Correspondence should be addressed to Weixiang Jiang; 1420110224@st.usst.edu.cn

Received 30 April 2022; Revised 14 May 2022; Accepted 23 May 2022; Published 10 June 2022

Academic Editor: Balakrishnan Nagaraj

To study in the Internet information security and privacy problem, a method based on IoT card monitoring technology based on machine learning, the technology can use fuzzy *c*-means algorithm for online business audit, using the Naive Bayes algorithm to classify Internet content and text messages, on the analysis of the comparison of the measurement method based on distance and based on the similarity. The concept of divergence in information theory is used to measure the difference between probability distributions. Finally, the feasibility of the proposed method is validated using the data from the machine learning database. The experimental results show that under the same privacy gain, the data availability relationship between the three anonymous protection methods is roughly satisfied as follows: when the privacy gain is less than 0.85, $U_{\text{dverity}} < U_{\text{emonymity}} < U_{\text{eclorenes}}$; when the privacy gain is greater than 0.85, $U_{\text{uxanaymiy}} < U_{\text{uiversriy}} < U_{\text{closencs}}$. And it proves that on the premise of ensuring efficiency and accuracy, the system can find a large number of illegal IoT cards and effectively guarantee the security of IoT.

1. Introduction

As an important information technology, the Internet of Things has been widely used in all walks of life, such as the power system, water supply enterprises, transportation departments, and intelligent life, all of which exist in the application of the Internet of Things technology [1]. At present, the Business of the Internet of Things develops very rapidly in China, and the scale of the card opening of the Internet of Things is also increasing day by day. For example, the scale of the users of the Internet of Things card of China Mobile has exceeded 500 million, and the users of the Internet of things involve dozens of industries. The continuous growth of Internet of Things card business brings more problems to the management and security supervision of Internet of Things card [2]. Illegal personnel may use the Internet of Things card for malicious resale, illegal embezzlement, and embezzlement, take advantage of the low charge of the Internet of Things card to use the Internet of Things card as a common user card for sale, illegal arbitrage, and even use it to make nuisance calls, and send illegal SMS, which seriously affects the normal business of users. Subjects subject to privacy threats in the Internet of Things mainly include two categories: data and node location [3]. In recent years, Internet technology and virtual reality technology are developing rapidly at home and abroad, by means of virtual reality technology to the real world simulation expression in recent years, Internet technology and virtual reality technology are developing rapidly, with the aid of the expression of simulation and virtual reality technology to the real world IoT front sensor network access to all kinds of information, the object of perceived virtual reconstruction and reproduction, and Geographic information engineering applications can be established with true Three-dimensional landscape description, real-time interaction, and spatial analysis and query, which will make qualitative changes in the perception and expression ability of the Internet of Things [4]. The integrated application of virtual reality and Internet of things has been a lot of research and application achievements in the field of the water conservancy industry application, with

the help of a professional hydrological process calculation model and flood calculation model, and based on virtual reality technology and the Internet of things technology of water conservancy engineering, a comprehensive simulation system can make the researchers for the loss caused by flood disasters quantitatively, intuitive evaluation [5]. By simulating the process of hydrology and engineering conditions under different hydrology and climate conditions, the simulation dispatching and effect demonstration of hydraulic engineering are carried out, which provides scientific basis for flood control decision-making [6].

Huang puts forward that in the Internet of Things, foreign intrusion poses a serious threat to network security, and the system must have a corresponding mechanism to deal with this security threat. The intrusion detection mechanism is a kind of protection mechanism for the system to deal with foreign intrusion [7]. Xin et al.'s technology in intelligent contract is with block chain, such as a way of digital contract, usually by program code into blocks in the chain, mainly through specific operation mechanism to ensure transaction, and the operation of the contract is not affected by external interference, intelligent way of contract first consultation by both sides of the contract content, if the two sides reach a consensus. The system will publish the contract content in the system according to the contract logic through the program code [8].

The analysis was compared based on distance and based on the similarity measurement method, based on the use of virtual reality and Naive Bayes algorithm for online content and message classification, based on distance and is based on the analysis comparison, and based on the similarity measurement method using the concept of information releasing degrees to measure the difference between the probability distribution.

2. Internet of Things Card Monitoring Technology Based on Machine Learning

The Internet of Things card business security risk monitoring system can realize the full flow detection of the Internet of Things cards in the whole network of Liaoning Province and find out the security risks and illegal use of industrial cards and Internet of Things cards. The module as a whole includes three levels.

(1) Basic data layer: this layer is used to collect and screen all traffic related to Internet of Things cards, including Internet log, DN log, call signaling data, suspected SMS data, contract data, and consumption data of Internet of Things card users. Based on the above data results, the important fields of data are extracted, the data of different data sources are normalized, and the calculated data is stored

(2) Intelligent analysis layer: this layer is used to analyze the data provided by the basic data layer based on artificial intelligence from the three aspects of business risk, network information security risk, and management risk and find out the suspected illegal use or security risks of industrial cards and Internet of Things card users

(3) Security visualization layer: this layer analyzes and displays illegal industry cards and Internet of Things card users from multiple dimensions such as user violation type and user risk type and can export display data, which is helpful for regulators to deal with illegal Internet of Things users offline [9]

The monitoring center platform is the integration of the functions of the whole application layer, and its function system includes an interactive sluice virtual simulation scene based on Unity3D engine, which supports *C#* Script and Java Script control. The data management module is responsible for receiving and storing the data uploaded by telemetry terminals, remote video management module of telemetry point, real-time monitoring module of water condition and working condition data, and the sluice remote scheduling module and several hydrology professional calculation models running in the system background as service.

2.1. Use FCM to Conduct Business Type Audit. The FCM algorithm is a data clustering method based on the optimization of the objective function, which can carry out multiclass clustering of data. The clustering result is the degree of membership of each data point to the clustering center, which is expressed by a numerical value. The algorithm allows the same data to belong to multiple different classes. And FCM is an unsupervised fuzzy clustering method, which does not need human intervention in the process of algorithm implementation. During the use of the Internet of Things card, the business behaviors and business types of the Internet of Things card are usually quite different from those of normal users. A normal user's plan starts from 58 yuan to 98 yuan and includes a certain amount of call duration (for example, 200 minutes) and a certain amount of Internet access traffic (for example, 20 GB). Therefore, for normal users, most services include SMS (currently receiving more, but sending less), MMS (currently receiving more, but sending less), traffic, call (calling and called), and value-added services. For users of the Internet of things card, the package fee is low, and users may only promise to use one or two services. For example, the Internet of Things card installed in the smart camera only needs traffic and SMS service, while the Internet of Things card installed in the smart meter only needs SMS service. In the training process of classification, we first prepared the business data of 100,000 normal users as a positive sample and then found the business data of 10 Internet of Things cards in different industries (10,000 samples for each industry) as a negative sample, a total of 11 categories. For the Internet of Things cards to be classified, the FCM algorithm can find out the probability (fuzzy value) that each sample belongs to different categories; so, we choose the FCM algorithm to classify business types.

For each of the above categories, calculate the center for each category c_j:

$$c_j = \frac{1}{n}\sum_{i=1}^{n} x_i, j = 1, 2, \cdots, 11. \quad (1)$$

Based on Equation (1), for the Internet of Things card users to be classified x_i, calculate the probability that the card belongs to different categories of IoT card, respectively μ_{ij}:

$$\mu_{ij} = \frac{1}{\sum_{k-1}^{c}} \left(\frac{\left\| x_i - c_j \right\|}{\left\| x_i - c_k \right\|} \right)^2. \quad (2)$$

Among them, $\|x_i - c_i\|$ according to the vector x_i Euclidean distance from center c_i of the class.

After calculating μ_{ij} by the above method, by constantly reviewing feedback to set category thresholds, we can identify IoT cards that are involved in business abuse (the use of the IoT card is similar to that of normal users) [10].

2.2. Measurement of Anonymity Protection Techniques. Aiming at the privacy protection technology of anonymity, this paper focuses on the measurement method of data accuracy, that is, the measurement of the difference of data availability before and after the addition of privacy protection method. The smaller the difference, the better the usability of the privacy protection method, and the worse the other way around. The quantification methods to measure the differences between individuals mainly include the quantification based on distance and the quantification based on similarity [11].

2.2.1. Distance-Based Quantization. Measure the distance between individuals in space. The farther the distance, the greater the difference between individuals. Distance measurement methods mainly include the following:

Euclidean distance, also known as Euclidean distance, refers to the distance between two points in n-dimensional space. The formula is as follows:

$$d(X, Y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}. \quad (3)$$

Euclidean measurements need to ensure that all dimensions are on the same scale level.

Manhattan distance, also known as urban block distance or L1 normal form distance, is the sum of projected distances generated by line segments formed by 2 points in Euclidean rectangular coordinate system on the coordinate axis. The formula is as follows:

$$d(X, Y) = \sum_{i=1}^{n} |x_i - y_i|. \quad (4)$$

Minkowski distance, also known as Minkowski distance, is a measure in Euclidean space and a generalization of Euclidean distance and Manhattan distance. The formula is as follows:

$$d(X, Y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p}. \quad (5)$$

The Manhattan distance for $p = 1$, the Euclidean distance for $P = 2$, and the Chebyshev distance for $p =$ infinity are as follows.

Chebyshev distance or L_∞ metric is a metric method in vector space. The formula of distance between 2 points is defined as follows:

$$d(X, Y) = \lim_{p \longrightarrow \infty} \left(\sum_{i=1}^{n} |x_i - y_i|^2 \right)^{1/p} = \max |x_i - y_i|. \quad (6)$$

Mahalanobis distance represents the covariance distance of data. Mahalanobis distance is an effective method to calculate the similarity of two unknown sample sets. Different from Euclidean distance, it takes into account the relationship between various properties. For two random variables X and Y that follow the same distribution, whose covariance matrix is diagonal, and whose standard variance is σ, the Mahalanobis distance formula is as follows:

$$d(X, Y) = \sqrt{\sum_{i=1}^{n} \frac{(x_i - y_i)^2}{\sigma_i^2}}. \quad (7)$$

2.3. Function Realization of the System

2.3.1. Implementation of Authentication Management Module. In the current Internet of Things system, the identity authentication of devices mainly has three modes, namely, static password authentication, dynamic password authentication, and biometric authentication. Static password authentication uses a preset password for authentication.

The password is static. If the user does not change it, the password will remain valid. The dynamic password is mainly calculated according to the built-in password chip. The password authentication must be completed together with the dynamic password and the built-in password chip. Biometric identification authentication is based on a certain feature of the human body, such as face recognition, fingerprint recognition, and expression recognition. According to the characteristics of the system, this paper designs a comprehensive identification method, which is mainly to send the manufacturer, type, and factory code of the equipment.

As the unique identification code for identity authentication, the structure of the authentication table mainly includes the device name, identification code, device characteristics, and remarks. When a device is connected to the network, the device obtains the three information and compares them with the data in the device access table. If the comparison is successful, the authentication succeeds.

2.3.2. Implementation of Operation Management Module. When the Internet of things to send information between devices and access to information, the receiving device information interaction system module, and send the request to the data transmission module, data transfer module sends authentication request to the block chain system, block chain contract application permission to verify the device automatically, and the verification results returned to the

data transmission module; if verification goes through, then the data transfer module sends the information to the interaction module; otherwise, the interaction module will not be notified. Similarly, the same principle is used to complete the operation and management of the device for information receiving.

2.3.3. Implementation of Security Detection Module. The security detection function is mainly realized by CIDF program, which mainly includes three subroutines, namely, event generation program, event analysis program, and data writing program. The system first monitors the running status of the sent information and then sends the test results to the event analysis program. The event analysis program compares the message behavior with the malicious event database. If the comparison is successful, it indicates that the message belongs to the malicious message, and the message is returned to the system to restrict the permission of the device.

2.3.4. System Technical Architecture

(1) Perception Layer. The sensing layer is mainly composed of a sensor network composed of water condition and engineering condition information acquisition sensor units and sluice control equipment sensor units distributed in the telemetry points of each monitoring section to realize the whole-process and all-weather collection of water quantity, water level, water quality, and sluice operation information. The water condition and working condition information collection and sensing unit mainly include water level, flow rate, and water quality sensors installed in the sluice and monitoring section. The sensor unit of the gate control equipment mainly includes the monitoring and sensing unit of the gate automatic control system (gate opening and closing state, opening, current, voltage, pressure, temperature, vibration, etc.).

(2) Transmission Layer. The remote monitoring sensor unit is connected to the monitoring center server through wireless transmission. At present, the available wireless data transmission networks mainly include the following: for China Mobile GPRS and China Unicom CDMA 1X, the peak rate of GPRS is 115.2 kbit/s, and the peak rate of CDMA1x is 153.6 kbit/s, which can meet the communication bandwidth requirements of sensing unit and monitoring center server.

2.4. Virtual Visualization Combined with Internet of Things. Virtual tour technology can bring a sense of three-dimensional experience, and the interactive operation realizes the leap of man-machine relationship, making the tour experience more real. The gradient lifting algorithm is similar to the similar lifting algorithm. Its idea is to use Taylor expansion, take the negative gradient value of the first derivative of the loss function to represent the real loss value, reduce the gradient as the goal to realize the optimization of the model, and finally achieve the purpose of reducing the loss value. The formula can be obtained:

$$f_m(x) = f_{m-1}(x) - \gamma_m \sum_{i=1}^{N} \nabla_f L(y_i, f_{m-1}(x)), \tag{8}$$

where $f_{m-1}(x)$ is the model learned when the tree of lesson M is generated, and γ_m is the learning rate. Generally, linear search can be used to obtain the best learning rate value.

$$\gamma_m = \arg \min_{\gamma} \sum_{i=1}^{N} L\left(y_i, f_{m-1}(x_i) - \gamma \cdot \nabla_f L(y_i, f_{m-1}(x))\right). \tag{9}$$

Based on the above introduction, if the number of decision trees is increased infinitely and the value of M tends to infinity, the fitting results of the model can approach the real distribution of data infinitely, and then a model with very high precision can be obtained. However, when the model becomes very complex, it conversely reduces the generalization ability of the model, resulting in overfitting problems. Therefore, in addition to the model itself, regularization techniques are generally required to reduce overfitting.

3. Experimental Analysis

Through the interactive script editing environment of Unity3D engine, the Internet of Things card monitoring technology is defined and implemented, and the integration of business application modules and simulation scenes based on J2EE architecture is realized by using the HTML interactive characteristics of Unity3D.

In this paper, the experiment uses the university (UCI) machine learning database, the adult. In the data set including 32561 records, the data set is commonly used in table item properties that include the following: age, education level, marital status, race, sex, and occupation. The experiment to the "professional" as the sensitive attribute, to adopt different kinds of anonymous protection technology before and after the data, is available to evaluate the performance differences of various anonymous protection technologies. There are 14 values for the "occupation" attribute in the database, and the number and proportion of records contained in each value are shown in Table 1. Because there are empty records and records in the table with an empty "class" attribute, the sum of all the "class" attribute record values counted in Table 1 does not equal 32561.

The use of anonymous protection technology will not only improve privacy but also reduce data availability. The following two concepts are described in this paper. Data availability is as follows: the degree to which an anonymous data set is similar to the original data set, as measured by divergence. The higher the similarity (that is, the smaller the divergence), the higher the availability of anonymized data. Privacy gain is as follows: the degree of privacy improvement of the original data after anonymous processing, that is, the probability difference between the original data set and the anonymous data set that can accurately locate a certain record through the same attribute value.

Table 1: Number and proportion of different occupational records.

Professional attributes	Record number	The proportion of
Tech-support	928	0.2315
Craft-repair	4099	0.1246
Other-service	3299	0.3569
Sales	2556	0.2456
Exec managerial	2398	0.3214
Prof-specialty	4056	0.1246
Handlers-cleaners	5026	0.1579
Machine-op-inspct	7	0.2013

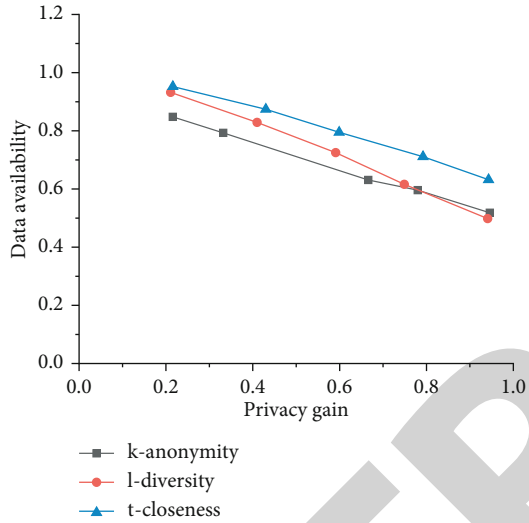

Figure 1: Privacy gains versus data availability.

Based on the two concepts above, this paper uses a measurement method based on divergence to compare the performance of three anonymous algorithms, which are K-anonymity, L-diversity, and T-closeness, with k values {10, 100,200, 500, 1000}, l is {3.0,3.5,4.0,4.5,5.0}, and T is {0.05,0.1,0.2,0.3,0.4}. The privacy gain and data availability relation of the three anonymous algorithms are compared as shown in Figure 1. The three solid lines in Figure 1, respectively, give the linear trend estimation of the three anonymous algorithms in the experimental environment. As can be seen from Figure 1, (1) when k, L, and t are different, the corresponding privacy gain and data availability are different. In addition, with the increase of k, L, and T, the privacy gain increases, and the similarity between the original data and anonymous data decreases, leading to the decline of data availability. (2) Under the condition of the same privacy gain, the data availability relationship roughly satisfied among the three anonymity protection methods is as follows: when the privacy gain is less than 0.85, $U_{\text{dverity}} < U_{\text{emonymity}} < U_{\text{eclorenes}}$; when the privacy gain is greater than 0.85,$U_{\text{uxanaymiy}} < U_{\text{uiversriy}} < U_{\text{closencs}}$.

In general, the default is standalone publishing. Clicking Unity's Build Setting will pop up a dialog box for client operating system to publish, and drag and drop the required scenes into current in order to realize the link jump. After clicking build button and setting resolution and rendering quality, generate an executable file in EXE format and a folder and keep the file and folder directory the same; otherwise, it will not run. After clicking Unity's Build Setting and selecting the Web Player option, build generates a web file and one. The Unity 3D file is then configured on the IIS server for web publishing. The server side will connect the web page and once the Unity 3D file is configured, the user can access it through a browser. Since Unity 3D publishing does not require an additional installer, it can be run directly by clicking on the EXE file after standalone publishing, and network publishing only needs to install a control of about 500 KB to run. After the platform is put into operation, it runs smoothly and has strong authenticity and interaction when operating equipment.

4. Conclusions

As the Internet of Things has been widely used in various industries, a large number of terminal devices are connected to the Internet of Things, which has brought great impetus to work and life. However, the information security problem of the Internet of Things has become increasingly prominent, especially in network management that is very difficult; for this, this paper puts forward the technology of information security platform based on block chain system design scheme, used to solve the technical problem, a certain scientific research achievements, but the system there has still some deficiencies; for the Internet of things system equipment, the lack of unified format of messages sent, every industry is fragmented, and message format cannot be unified. At present, there is no unified performance evaluation method and standard for anonymous privacy protection technology; so, it is necessary to develop a set of evaluation indicators and evaluation system to objectively and reasonably evaluate anonymous privacy protection technology. In the case of the same privacy gain, the data availability relationship roughly satisfied between the three anonymous protection methods is as follows: when the privacy gain is less than 0.85, $U_{\text{dverity}} < U_{\text{emonymity}} < U_{\text{eclorenes}}$; when the privacy gain is greater than 0.85,$U_{\text{uxanaymiy}} < U_{\text{uiversriy}} < U_{\text{closencs}}$.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that he/she has no conflicts of interest.

Acknowledgments

(1) General Program of Natural Science Research in Jiangsu University, Research on Key Technologies of Disaster Tolerant Mobile Data Collection for Underwater Acoustic Sensor Network, Project No: 19KJB520023. (2) Open Lab of Edge of

Computing for Smart Manufacturing, Changzhou College of Information Technology, Project No: KYPT201802Z. (3) The Scientific Research Project of Changzhou College of Information Technology in 2020, Digital Image Encryption Technology Based on Chaos Theory, Project No: XJ202001102.

References

[1] Q. Li, L. Zhang, R. Zhou, Y. Xia, and Y. Tai, "Machine learning-based stealing attack of the temperature monitoring system for the energy internet of things," *Security and Communication Networks*, vol. 2021, Article ID 6661954, 8 pages, 2021.

[2] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for internet of things," *International Journal of Machine Learning & Cybernetics*, vol. 9, no. 8, pp. 1399–1417, 2018.

[3] C. Yi, W. Zheng, A. Patil, and A. Basu, "A 2.86-tops/w current mirror cross-bar-based machine-learning and physical unclonable function engine for internet-of-things applications," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 6, pp. 2240–2252, 2019.

[4] H. Chen, C. Meng, and J. Chen, "Ddos attack simulation and machine learning-based detection approach in internet of things experimental environment," *International Journal of Information Security and Privacy*, vol. 15, no. 3, pp. 1–18, 2021.

[5] X. Gu, G. Liu, and B. Li, *Machine Learning and Intelligent Communications*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, 2018.

[6] A. Kulkarni, M. Mahajan, S. Mali, Y. Shelar, and M. Pradhan, "A study of use of internet of things and machine learning in smart waste management," *International Journal of Advanced Research*, vol. 9, no. 5, pp. 432–436, 2021.

[7] R. Huang, "Framework for a smart adult education environment2015," *World Transactions on Engineering and Technology Education*, vol. 13, no. 4, pp. 637–641, 2015.

[8] L. Xin, L. Jianqi, C. Jiayao, Z. Fangchuan, and M. Chengyu, "Study on treatment of printing and dyeing waste gas in the atmosphere with Ce-Mn/GF catalyst," *Arabian Journal of sciences*, vol. 14, no. 8, pp. 1–6, 2021.

[9] I. S. Thaseen, V. Mohanraj, S. Ramachandran, K. Sanapala, and S. S. Yeo, "A hadoop based framework integrating machine learning classifiers for anomaly detection in the internet of things," *Electronics*, vol. 10, no. 16, p. 1955, 2021.

[10] J. Jayakumar, S. Chacko, and P. Ajay, "Conceptual implementation of artificial intelligent based E-mobility controller in smart city environment," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5325116, 8 pages, 2021.

[11] C. Duan, *Design and Implementation of an Information Security Platform for the Iot Based on Blockchain*, Springer, Singapore, 2022.