Optimisation of Automation Devices Based on IOT Big Data Algorithms

Yike Xue*

School of Education, University of Sheffield, England, United Kingdom

Abstract. With the continuous development of communication, sensor and caching technologies, IoT technology has gained rapid opportunities for growth and a huge digital revolution has taken place at all levels of society. Blockchain technology has emerged rapidly in recent years and can be seen as a distributed, time-based ledger of distributed data. It utilises technologies such as consensus protocols, modern cryptography, P2P and smart contracts, which can provide a secure, stable, transparent, auditable and low-consumption system architecture that has a traceable, stable and efficient security management capability, and can provide a new solution to identity security for the Internet of Things. This paper absorbs the existing blockchain-based access management approach and improves it, proposing a new private chain-based security management approach that solves the problems of access dynamics, low intelligence and high overhead in the traditional access management approach. This paper designs a new control management architecture, the Novel-Capability-Based Access Control (NCBAC), which draws on the microkernel and microservice ideas of operating systems. Firstly, this paper abstracts the concept of management node to solve the problem of weak computing power and low storage performance of IoT devices that cannot meet the difficulty of direct communication between IoT devices and blockchain, and at the same time can reduce the network operation overhead; secondly, it constructs a multi-level smart contract system and designs three kinds of smart contracts, AC, ACC and AMC, to build a trusted and reliable access control entity model; finally, it adopts radial basis based (RBF) neural network and combines with access policy to dynamically generate the credit degree threshold of access nodes to build an intelligent access authority management model for IoT mass sensors. The model proposed in this paper designs a token mechanism based on the fact that IoT systems have multiple requests within a short period of time in a real production environment, which, according to experimental results, improves the performance of the system to a certain extent.

1. Introduction

With the rapid development of the digital economy, a new generation of information technology such as the Internet of Things (IoT) and other emerging technologies are developing rapidly. IoT technology is now widely used in many fields such as smart healthcare, smart homes and smart firefighting [1] [2]. The IoT infrastructure is a network for interconnecting things that completes data collection, fusion, processing and sharing. A huge amount of data is generated in the IoT, which contains a large amount of private data, and since IoT devices do not have high computing power resources, there is a great security risk in the exchange of information between things [3][4].

2. Smart Contract-Based Design for IoT Identity and Authority Authentication

One of the problems to be solved by the model proposed in this paper is how to make an otherwise centralised IoT system, improved to a decentralised system, so that the overall system is a distributed system [5]. The A3GM algorithm is used in the wireless sensor network in this model to ensure that the wireless sensor network is distributed and that some nodes rich in computational resources are selected to take on the role of communicating with the management nodes according to the algorithm [6].

2.1. System Architecture

The architecture of the NCBAC system proposed in this paper is shown in Figure 1 and consists of six main components: BlockChain, Management, Special Node, Wireless Sensor Networks (WSNs), Manager and Smart Contract Deployer [7] [8].

[*] xueyike1016@gmail.com

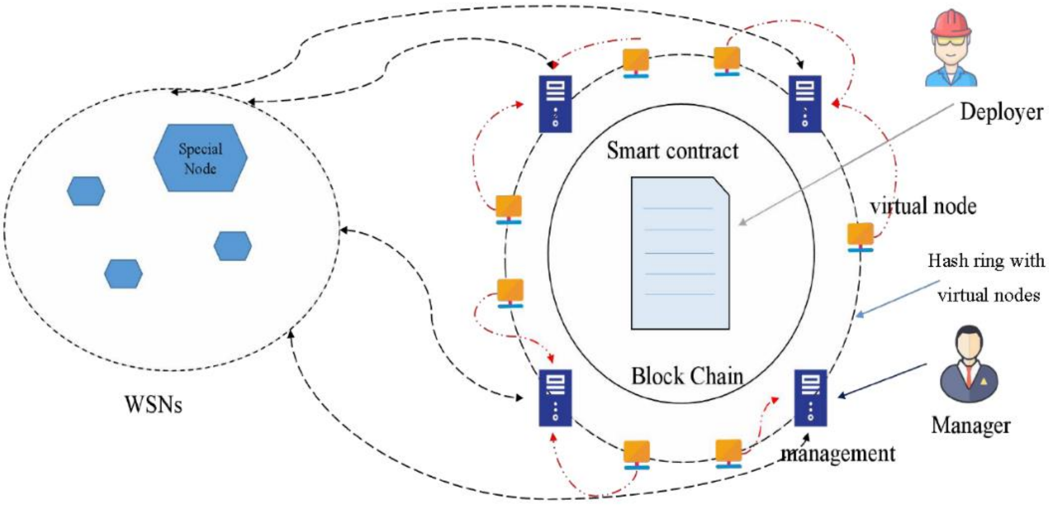

Figure 1. NCBAC system architecture diagram

Management node: It is part of the blockchain network and has two EOA accounts: normal account and special account. It performs the following functions: converting the information transmitted by the wireless sensors into JSON format based on the websocket protocol; obtaining the API interface exposed by the smart contract through the websocket protocol, and initialising and controlling access to the system based on these interface functions [9].

Special Node: Sensors and other devices in the IoT system are lightweight devices, many of which have limited computing resources and can only send and receive specific, simple communication information, and cannot perform the task of exchanging information with the management node, but there are still some devices with some computing resources [10].

Smart contract deployer: Smart contracts need to be written in the local compiler, however, the completion of the program does not mean that it can be run in Ether, it needs to generate EVM bytecode, and then the smart contract deployer uses his Ether account to deploy the EVM bytecode to the chain, the necessity of the smart contract deployer is because the smart contract is the "brain" of the whole system, all logical judgments are done by the smart contract, so it is necessary to abstract out the smart contract deployer, a clear division of authority can better ensure the security of the system.

2.2. Blockchain Network Construction

The actual function of the EVM is used to process transactions on Ether, and the business process is shown in Figure 2:

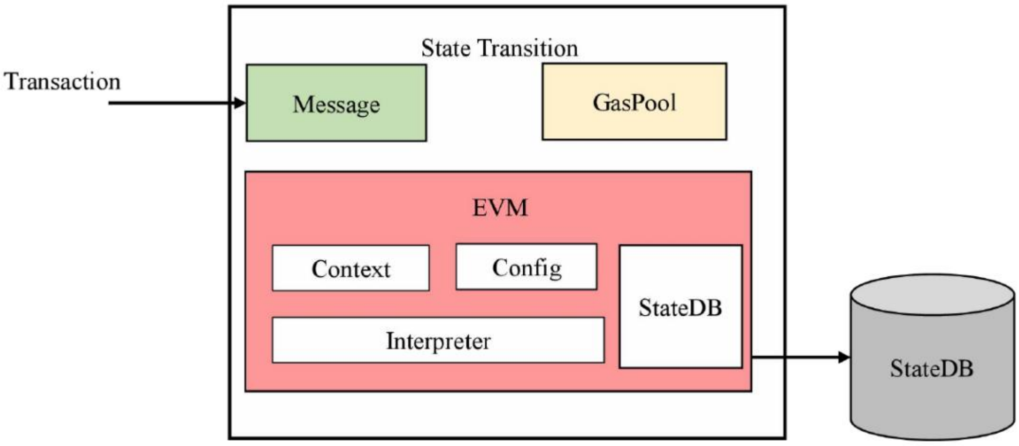

Figure 2. Ethernet virtual machine business process

Smart contracts compiled into EVM bytecode and entering the block are transformed into message body objects, as shown in Figure 3, and the message bodies are passed into the EVM for execution. If it is just a transfer of funds between two nodes in the system, the system only needs to directly modify the relevant data of the StateDB; whereas transactions generated by smart contracts require the EVM to run the relevant bytecode and then perform a series of query and modification operations on the StateDB.

The transaction is converted into an object with a message body and fed into the Ethernet virtual machine, which generates the corresponding contract object based on the message body for later execution.

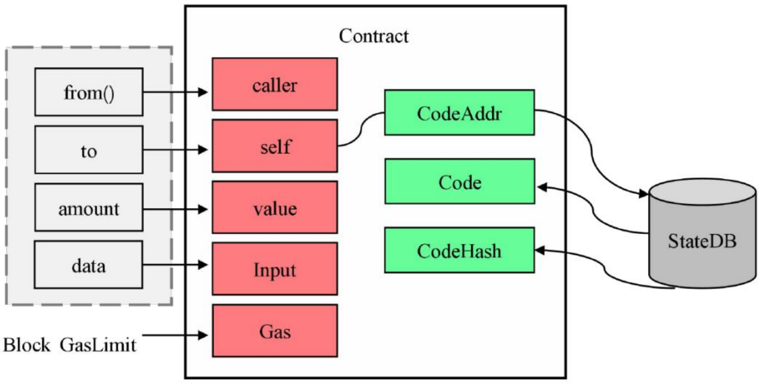

Figure 3. Transformation of a smart contract into a message body object

The blockchain module in the model proposed in this paper is required to deploy and run the three contracts AC, AMC and ACC. Successful deployment to Ethernet will automatically generate a binary specification interface to deploy the smart contract to the Ethernet private chain using an external account, and successful deployment will generate a contract account about that smart contract.

3. Dynamic Rights Management Modelling

3.1. Comparison of Dynamic Permission Management Models

With the continuous development of communication, storage and sensor technologies the scale of the IoT system continues to grow, and at this time there is a high demand for permission management in the IoT system, and how to achieve automated and intelligent permission management is a pressing challenge.

Prediction using linear regression models is a common and simple solution, and multiple linear regression models are an important mathematical tool in the field of statistics and analysis. Let the creditworthiness of the equipment be the dependent variable r and the set of parameters that will have an impact on the creditworthiness of the equipment be $s_1, s_2, s_3, \ldots\ldots, s_p$. Assuming that the size of the sample is W, the matrix of dimension $W * (p+1)$ is noted as $S = (1, s_1, s_2, s_3, \ldots\ldots, s_p)$, which is characterised by the first column having all values of 1, and whose augmentation matrix is $Z = (S, r)$. The multiple linear regression method, as well as the determination of the regression coefficients and the various parameters of the model, are calculated with the aid of the fork product array of the augmentation matrix $Z = (S, r)$, as shown in Eq. (1):

$$Z = \begin{pmatrix} S`S & S`r \\ r`S & r`r \end{pmatrix} \tag{1}$$

The key to multiple linear regression modeling is how to model the prediction of the fork product array. Let the point capacity of the sample be W, the dependent variable at moment t be r^t and the p independent variables be $s_j^t (j = 1,2, \ldots\ldots, p)$, then the linear regression model equation is obtained as Eq (2):

$$r_i^t = \beta_0 + \beta_1^t + s_{i1}^t + \cdots + \beta_p^t + s_{ip}^t + \varepsilon_i^t \tag{2}$$

Remember $r^t = \begin{pmatrix} r_1^t \\ r_2^t \\ \cdots \\ r_n^t \end{pmatrix} n \times 1, \beta^t = \begin{pmatrix} \beta_0^t \\ \beta_1^t \\ \cdots \\ \beta_p^t \end{pmatrix} (p+1) \times 1$

Its augmentation matrix is Eq. (3):

$$Z^T = \begin{pmatrix} (S^t)`S^t & (S^t)`r^t \\ (r^t)`S^t & (r^t)`r^t \end{pmatrix} = \begin{pmatrix} Z_{11}^t & Z_{12}^t \\ Z_{21}^t & Z_{22}^t \end{pmatrix} \tag{3}$$

The least squares estimator of the regression coefficient β^t is shown in Eq. (4):

$$\beta^t = (Z_{11}^t)^{-1} Z_{12}^t \tag{4}$$

The analysis of the construction of the multiple linear regression model shows that the linear characteristics of the model limit the fit of the model to complex problems, especially for this paper, which studies the permission problem of IoT devices, it is a complex non-linear problem, so a non-linear model needs to be constructed to solve the problem.

RBF neural networks are based on radial basis function neurons, which have outstanding properties for fitting to non-linear problems. The most critical point for RBF neural networks is the radial basis function. The most commonly used function for RBF neural networks is the Gaussian function, which completes the following non-linear mapping, as shown in Eq. (5):

$$R_1(X) = \exp\,[-\left||X - C_i|\right|^2 / (2\sigma_i^2)], i = 1,2, \cdots, Nr \tag{5}$$

Where X is the input variable is an N-dimensional vector $X = \{X_P | X_P \in R^N, p = 1,2, \ldots, K\}$, the range of the set of values taken is R^N, R^N Is the set of samples of the input; R_i(x) is the input unit of the hidden layer; C_i The centroid of the Gaussian function; 111 represents the parameter of the normalization of the nodes of the hidden layer, the magnitude of its value represents the number of layers of the hidden layer; Nr is the number of nodes representing the hidden layer; P denotes the number of samples.

RBF neural nets are effective neural nets that mimic the local response of neurons in the brain to external stimuli, allowing the network to be fast and still have the ability to fit non-linear problems well.

3.2. RBF-based Permission Management Design

The RBF neural network algorithm, which mainly uses the basis functions of the hidden layer to achieve a non-linear simulation, then performs a linear combination with the output layer as a way to complete the fitting of the non-linear problem. In view of the fact that the model proposed in this paper is based on blockchain technology implementation, the forward propagation logic of the RBF neural network needs to be expressed in the form of a smart contract. the input indicators of the RBF neural network are used in the contract and the algorithm for obtaining them.

4. Conclusion

The Internet of Things (IoT) technology continues to develop and advance, and its scale is growing, bringing convenience to people's lives while gradually revealing its shortcomings. As IoT technology continues to be integrated into our daily lives, traditional IoT technology architectures are no longer able to meet people's requirements as they become more aware of privacy and security. Traditional IoT C/S and B/S architectures require a centralized server to collect and process data and then provide services to the user layer. However, this architecture design has not only proven to have a single point of failure, but also cannot guarantee whether the third-party server is really safe and secure, especially since much of the data collected by the IoT system involves personal privacy data, which increases the danger of privacy data leakage. In this paper, we propose the organic combination of blockchain technology and IoT system to solve the problems in the process of continuous development of current IoT system, and combine with the current hot blockchain technology.

References

1. Chen Jian, Yan Kai, Gao Bangsheng. Common faults of automation devices in pumping stations and how to deal with them [J]. China Equipment Engineering, 2023(03):52-54.
2. Jia Shaohua. Analysis of the reliability improvement strategy of relay protection and automation device of power system [J]. Popular standardization,2022(22):158-160.
3. Sun J. Research on the reliability of relay protection and its automation devices in power systems [J]. Science and technology information,2022,20(21):39-42.DOI:10.16661/j.cnki.1672-3791.2205-5042-9281.
4. Zhang X, Zhang Chao. Analysis of operation and maintenance of relay protection and automation devices in photovoltaic power stations [J]. Light Source and Lighting,2022(09):51-53.
5. Fan Xiaowei, Xu Juan, Lu Yin. Reliability analysis of relay protection and automation devices[J]. DOI: 10.19339/j.issn.1674-2583.2022.09.132.
6. YANG Qingyun, MA Borong, MA Junpu, LUI Guanghui, ZHANG Zhiyuan, YU Yan. Automatic forming device design for marine copper-nickel alloy flanges [J]. Forging Equipment and Manufacturing Technology,2022,57(04):47-51.DOI:10.16316/j.issn.1672-0121.2022.04.010.
7. Siemens builds digital substation for Glitre Energi Nett to support power IoT applications [J]. Electrical Times,2019(11):41.
8. D J L S,F M L. [Ethical dilemma of big data in primary healthcare].[J]. Semergen,2022,48(6).
9. Laia S, Ismael V,Joan T, et al. La era del big data: análisis del lenguaje natural mediante la aplicación de folksonomía[J]. NEFROLOGÍA,2022,42(6).
10. S. J G, Wilfredo A,F. E C. A Data Analytics/Big Data Framework for Advanced Metering Infrastructure Data[J]. Sensors,2021,21(16).