Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2853821, 7 pages
https://doi.org/10.1155/2022/2853821

Research Article

Big Data-Based Access Control System in Educational Information Security Assurance

Zhong Peng, Feng Liang, and Lili Mu

Guilin Tourism University, Guilin, 541006 Guangxi, China

Correspondence should be addressed to Lili Mu; glmll@gltu.edu.cn

Received 18 November 2021; Revised 14 December 2021; Accepted 28 December 2021; Published 17 January 2022

Academic Editor: Deepak Kumar Jain

Access control is a key strategy to prevent and protect the network. The most important task is to ensure that visitors will not use network resources and will not conduct unauthorized access to them. This paper studies a number of information security issues in the process of education informatization, aimed at studying the application of access control systems based on big data in education information security. This article elaborates on the related concepts of access control and proposes an attribute-based encryption scheme. Based on this, an information system security system model with security strategy as the core content is constructed. The experimental results in this paper show that the improved access control system has the more efficient guarantee ability in education information security, which is about 47.3% higher than the traditional access control system.

1. Introduction

The provision of educational information is a comprehensive and in-depth process of application of modern information technology in education, it is a trend of the time and the inevitable result of the transformation and development of information technology in China, which has promoted educational reform and development from passive education to preventive and transformational studies; exam education is a quality education that cultivates talent that meets the needs of the knowledge economy of the new century and to enable educators to use information, networks and functions to carry out innovative activities that will advance the strategic talent goals of the new century in China and compete in the knowledge economy. It can not be denied that there are still many problems to be studied in the formulation process and that information security is a more real problem, especially in basic education where there is not enough research.

Providing educational information is an essential part of modernizing education and is an important step in modernizing it. The provision of educational information provides opportunities for all citizens to be educated and the provision of educational information is essential to improve the quality of all citizens. Educational information provides the environment, conditions, and quality assurance of innovative education and training. Students use the educational information environment to extract information, collect information, process information, and produce information to achieve discovery learning, problem solving, and exploration and discovery of knowledge, which are very important for the development of innovative skills. Providing educational information is a significant change in education and will effectively promote the development of educational theory. The educational information process is the process by which information technology and information machines are widely used in education; in this process, it has greatly promoted the development of the educational information industry. With the development of in-depth research data, the issue of information security is becoming more and more obvious and serious. Without security, it will not be used and without it, it will not be developed. Therefore, strengthening research on information systems access control mechanisms has significant theoretical value and wide application possibilities.

Thanigaivelan et al. introduced CoDRA, an access control system for Android, which provides context-based dynamic configurable restrictions, fine-grained policies, and the ability to enforce various policy configurations on different levels of system operations. CoDRA implements different policy configurations according to users by integrating multiuser support in Android. A simple graphical control panel is provided for strategy management. By testing 55 popular applications in Nexus 5 and 9 devices, the performance and overhead of CoDRA are analyzed. However, in the case of complete restrictions and higher policy granularity, the tested application will show some adverse effects during the execution process [1]. Konoplev and Kalinin propose an architecture of an access control system for user jobs to access computing resources in a grid distributed computing network. The architecture provides protection for the data being processed to prevent threats from exceeding user privileges. The developed system is compared with the available analogues, and the results of the efficiency evaluation of the developed system's performance are discussed. At the same time, Konoplev and Kalinin also reviewed the issue of providing information security for data and computing resources in grid networks. The specific characteristics of the distributed computing network architecture based on the grid platform are analyzed. The shortcoming of this research is that it is far from enough to describe the architecture of the access control system in theory, and it should be confirmed in practice [2]. Gruntz et al. proposed a smart phone-based physical access control system, in which the access point is not directly connected to the central authorization server, but uses the connectivity of the mobile phone to allow the central authorized online authorized user to access the request access server. The access point asks the phone whether a specific user can access it. The mobile phone then relays such requests to the access server or presents a ticket. However, in this case, in response to the access request, the access request is sent to the access point, and after the smart phone is connected, it will not be automatically updated regularly [3].

The innovation of this article lies in the following: (1) this article studies a number of information security issues in the process of educational informatization construction. It takes effectiveness and application as the leading factor, pays equal attention to management and technology, and starts from all aspects to build a complete basic education informatization Information security assurance system. (2) In-depth study of access control technology theory, standard-oriented, detailed analysis of the reference model of typical access control technology and its application advantages, the core of which is authentication and authorization technology.

2. Application Research Method of Access Control System Based on Big Data in Education Information Security Guarantee

2.1. Access Control

2.1.1. Basic Theory of Access Control. Access control technology refers to a security mechanism that controls the ability of objects to access object resources and their access scope according to specific security policies when the information resources exposed by the computer system are safe [4–6]. Execution without permission can provide reasonable control and preventive measures to protect the safety and correctness of resources. Preventing unauthorized users from accessing illegally protected resources and allowing legitimate users to access information resources is usually the main goal of access control, and it is also a function [7]. The two most basic principles in secure access control technology are the principle of least privilege and the principle of separation of duties [8]. The principle of least privilege requires the subject to be granted only the minimum set of privileges required for its operation during authorization. To ensure that the subject can complete the tasks that need to be completed under the privileges granted, while limiting the operations that the subject can perform, so as to minimize the loss caused by illegal or misoperation [9]. The principle of separation of duties, as a more advanced authority control mechanism, produces some mutually exclusive constraints based on the actual effect of authority. The use of certain authority can only be exercised under certain conditions, thereby reducing the subject's simultaneous use of multiple authorities to generate deceptive behavior possibility [10, 11]. This restriction ensures the security of permissions in application systems where role permissions are more sensitive. Access control first needs to verify the legitimacy of the user's identity and, at the same time, use the control strategy for selection and management. After the user's identity and access authority are verified, it is also necessary to monitor the unauthorized operation [12].

2.1.2. The Core Means of Access Control. Regarding the use of access control applications, first, the necessary authorization for valid users is required, and then, an access strategy is selected and implemented. Therefore, authentication and authorization are considered to be the two core means of access control [13, 14].

First, certification: authentication refers to the process of verifying whether a user has the declared identity based on the information provided by the user to prove his identity, and that is, verifying whether a user's identity is legal.

Second, authorization: authorization means that after the user is authenticated and becomes a valid user; it will verify whether it has the right to access specific resources according to the agreed access policy.

2.1.3. Basic Principles of Access Control. Access control mainly prevents illegal use of protected resources and defines the following four component roles: access initiator, access control enforcement function (AEF), access control decision function (ADF), and access target [15].

The principle of access control is shown in Figure 1: The access initiator represents the subject trying to access the protected resource, and the access target represents the protected resource object and the control decision function. Access is the realization of license-based access control authority [16, 17]. The agreed access control policy during the access process, the access initiator first sends the access

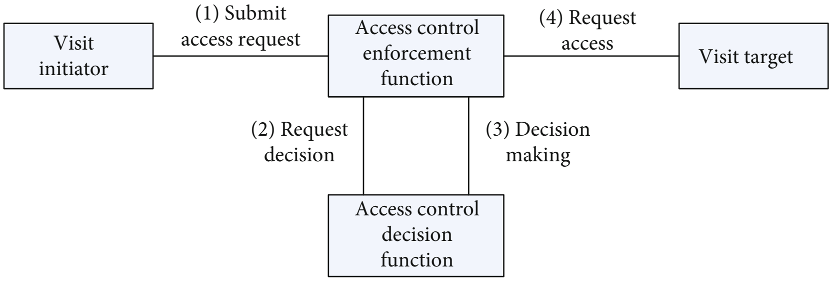
Visit initiator
(1) Submit access request
Access control enforcement function
(4) Request access
Visit target
(2) Request decision
(3) Decision making
Access control decision function

Figure 1: Schematic diagram of access control.

control request to the access control enforcement function (AEF), and then, the AEF item forwards the access request to the access control decision function (ADF). When deciding whether to allow the ADF component to allow access according to the access control policy, the request may eventually reach the protected access target. This can prevent the illegal access of legitimate users and the intrusion of illegal users, thereby reducing the security of system resources [18].

2.2. Identity Authentication. Authentication technology refers to technology that can verify the true identity of the sender and receiver. It is the first obstacle to protecting the security of network information resources. Its mission is to identify and verify the legality and validity of the user's identity in a networked information system and allow access to system resources and prevent illegal visitors. It can be seen that the authentication status of a security system is of great importance—it is the most basic security service and other security services depend on it. Factors such as environment, application environment, and employee quality are closely linked.

2.2.1. Common Mechanisms for Identity Authentication. Authentication technology is an effective means of achieving network security by closely integrating business processes to prevent unauthorized access to critical resources [19]. Authentication refers to a user's process that identifies a system. Authentication is the process by which the system checks for the user's identity, which is basically to determine whether the user has the right to store and use the requested resource. People often refer to proof of identity and act as a combination of identity verification (or authentication), which are two important links to identify and verify the true identity of a communications party. The authentication must be able to identify the other party accurately and at the same time require two-way authentication, that is, mutual authentication.

In the authentication mechanism, for security reasons, both parties communicating may require each other to digitally sign certain information, and signature verification requires the associated public key. Additionally, although the public key is not suitable for encrypting large amounts of data, the public key is generally used to encrypt session keys or master keys. Therefore, whether or not a user's public key is valid is a critical issue in the authentication of the information. To resolve the issue of whether the public key is valid or not, one way is to store all the public keys on the public key server, and each user can query the other user's public key through the public key server. Apparently, an attacker could put his own public key under a valid user ID, indicating that this method was not secure. Another way is to create a directory (database) to store each user's public key certificates. The user's public key certificate is generated by a trusted CA certificate authority and the certificate is stored in the directory. The implementation of the public key authentication mechanism that the certificate uses must involve the participation of the trusted authority. All CAs are contained in a hierarchical structure, and each CA has its own public key, which is signed with the CA certificate. However, since the CA root is at the top and does not have a top-level node, it is not subject to this restriction. Most public key management mechanisms include the generation of public and private key pairs. Downloading and issuing digital certificates used by the user downloads to verify the validity and validity of the other pair of public key certificates. This updates user keys and certificates, removes user certificates, and maintains functions such as certificate revocation list (CRL). Currently, most public key authentication mechanisms are used for internet authentication. Specifically, X.509 compliant digital certificates are used. The public key authentication system also has the following vulnerabilities: In public key authentication, the user is often required to validate the certificate. When issuing a certificate, the authentication center uses user authentication to make it inconvenient. Managing digital certificates and certificate revocation lists is complex. The cost of implementing an accreditation system is quite high.

2.2.2. PKI Technology. Modern encryption believes that algorithms can be made public. "All secrets are in one key." Encryption is a key technology for protecting information security. The PKI certification system is the one with the most thorough understanding of this theory. PKI is based on public key cryptography. As symmetric encryption systems have insurmountable drawbacks, such as exponential key increments and difficulty distributing keys, in the 1970s, Diffie and Hellman introduced a public cryptographic system. In this system, encryption and decryption use different keys and are interdependent, that is, data encrypted with one key can only be decrypted with another. The secret key is called the public key, and the secret key is called the private key. This allows the two parties to communicate secretly without having to exchange keys in advance. There are two basic models of public key encryption, encryption models, and authentication models.

Today, the most famous and widely used RSA public key system is asymmetric theoretical number encryption and belongs to the encryption block. It can be used for both data encryption and digital signatures. Most of the products and templates that use public key cryptography for encryption and digital signatures use the RSA algorithm. The main idea behind PKI is to use the RSA public key system to realize the validity, integrity, confidentiality, and disclaimer of information. The key is a way to verify that the user actually holds the public key. To ensure that user credentials match the keys, they hold, trusted, and independent third-party CAs which should act as a authentication center. The authentication center uses its own private key to add a digital signature to the digital certificate to verify that the certificate cannot be forged.

2.2.3. Identity Authentication Technology under the .NET Framework. Authentication is the process of identifying an application's clients. Clients here may include users of services, processes, or computers. Authenticated clients are called master. Authentication can occur on various application levels [20]. The end user is initially authenticated by the web application, usually based on a username and password. The end-user requests are then processed by the intermediate application server and the database server, and authentication is also performed in the verification and processing of these requests.

The .NET framework in Windows 2000 provides the following authentication: ASP.NET authentication, enterprise service authentication, and SQL server authentication.

2.3. Attribute-Based Encryption Scheme. The so-called fuzzy matching is not to strictly define each identity, but to classify all identities according to certain rules, and all identities in the same category are considered the same [21, 22]. According to the classification rules, identities belonging to the same category may have different attributes, and each category of identities is defined by the concept of attributes. Correspondingly, the file or data information in the cloud computing data service also restricts its visitors through attributes. If the attribute of the ciphertext is the set δ and the attribute of the visitor's key is the set ω, when the number of elements in their intersection meets the threshold t set by the system, the key matching is successful, which is

$$|\delta \cap \omega| \geq t, \tag{1}$$

define G_1, G_2 as the p-order cyclic group, which satisfies the bilinear mapping relationship, and its generator is defined as g. e is defined as a bilinear mapping relationship, namely,

$$e = G_1 \times G_1 \longrightarrow G_2, \tag{2}$$

define μ as the complete set of attributes, and the number of set elements is $|\mu|$ ($|\mu|$ is a positive integer). The attribute set of many entities in the system is a subset of the complete set.

Number each attribute in the system attribute as $1, 2, 3 \cdots, |\mu|$. Define Z_p as the certificate body in the security algorithm structure, and each attribute uniquely corresponds to the certificate in it. $t_1, t_2, \cdots, t_n$ is randomly selected in Z_p, and a value $y \in Z_p$ is randomly determined. Based on the above concepts, the PK of the system is defined as

$$T_1 = g^{t1}, T_2 = g^{t2}, \cdots, T_{|\mu|} = g^{t|\mu|}, Y = e(g, g)^y. \tag{3}$$

Among them, $t_1, t_2, \cdots, t_{|\mu|}$ represents the public key of the system.

2.3.1. Key Generation. The first step of the private key generation process of the entity $\omega \in \mu$ is to select a polynomial q of order $d - 1$ and satisfy the equation:

$$q(0) = y. \tag{4}$$

The private key can be expressed as

$$\{D_i\}, i \in \omega, \exists i \in \omega, D_i = g^{q_i/s_i}. \tag{5}$$

2.3.2. Encryption. For plaintext $M \in G_2$, the system randomly selects a positive integer and satisfies $r \in Z_p$ and uses the public key δ associated in the ciphertext to encrypt it:

$$E = \left(\delta, E' = MY^R, \{E_i = T_i^R\}, i \in \delta\right). \tag{6}$$

2.3.3. Decryption. If the attribute set of the visitor key ω can meet the threshold condition $|\delta \cap \omega| \geq t$, the ciphertext formed by the encryption of its corresponding public key δ can be decrypted. Arbitrarily, we select t attributes in the $|\delta \cap \omega|$ set to form an attribute subset R and complete the following decryption process:

$$\frac{E'}{\prod_{i \in R}[e(D_i, E_i)]^{\Delta_{i,R(0)}}} = \frac{Me(g, g)^{sy}}{\prod_{i \in R}[e(g^{q_i/s_i}, g^{rs_i})]^{\Delta_{i,R(0)}}} = M. \tag{7}$$

After the above formula is successfully solved, the value M obtained by the solution is the password information of the account.

3. Application Research Experiment of Access Control System Based on Big Data in Education Information Security Guarantee

3.1. Test Preparation

3.1.1. Hardware Test Environment. The environment consists of (1) two layer switch equipment and one layer three switch, (2) two PCs, (3) portal server, (4) display, and (5) several network cables.

3.1.2. Software Testing Environment. The environment consists of (1) test cases, (2) unit test tools, (3) simulation software, and (4) equipment configuration test tools.

3.2. Test Method Description. System debugging is to test the overall system of the equipment and the system on the equipment to check the undiscovered errors in the system and the positions that conflict with the user's requirements

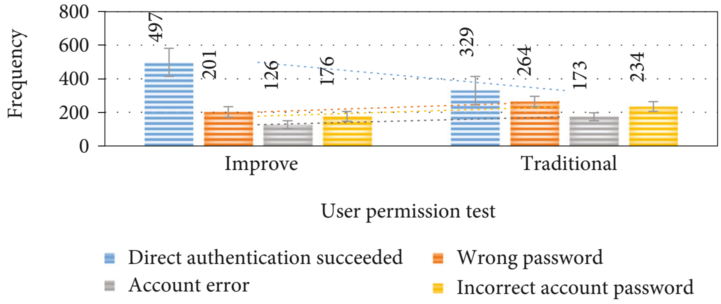

Figure 2: Test result of user permission test.

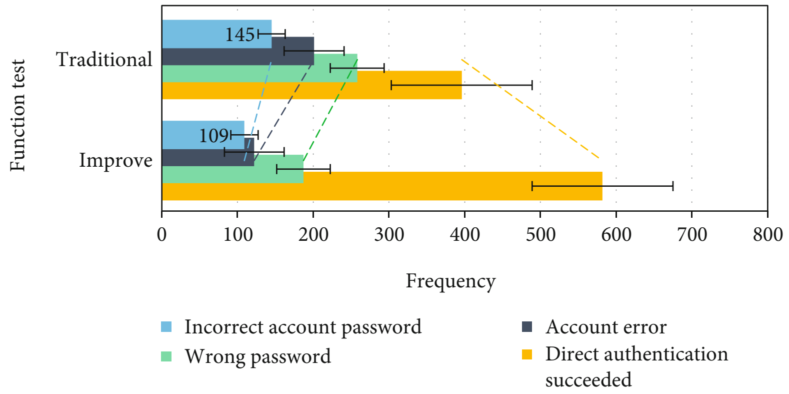

Figure 3: Test result of functional test.

and correct them in time. The correct system solution program most tests of this system use device simulation software to observe the test results and detect errors in the running program. Before the experimental test officially starts, some correct access codes and some wrong access codes are used to test the system to ensure that the system is tested under a condition that fully meets the test requirements. During the testing process, all system software functions are executed in the device simulation software according to the system test case requirements, such as command line testing, instant user authentication, alternate user address verification, and cardiac user monitoring. Before testing the user level and service heart rate, and please written code and create an executable file on the switching device, restart the device, and then perform all related tests by connecting the gateway server to the computer terminal. Users and servers create a real network. Before testing, the message debugging switch must be activated so that detailed information about all messages flowing to the switching device can be observed during the user authentication phase and by verifying the operation of the system. We analyze and confirm the text. Similar test modes are also used for offline function testing and cardiac function. In addition to tracking messages, more advanced tests are required for offline and offline functions, that is, using two different authentication methods to repeatedly perform online and offline functions.

3.3. Test Content and Results

3.3.1. Function and Performance Test. The operation test of the network access control system is mainly divided into the following aspects: (1) whether the gateway authentication in direct operation is normal; (2) whether the auxiliary address function is normal gateway authentication; (3) user authentication: the user can go to the page recognized after successful authentication; (4) whether the user is offline; and (5) whether the user can be authenticated offline by the command line.

We enter the user name and password in the PC browser-based identity verification interface to perform the identity verification and billing process and ensure that the identity verification is successful. Success or failure, and then go to the specified page to check whether the user's Internet status is normal, and check the user's status through each step of the command line, and the end user can access the network. Then, when the user closes the authentication interface, please check whether the user is offline normally. And through the command line, users can enforce the following operations to deny access to Internet resources. Then, we disconnect the server to check whether the user has been authenticated, whether the authentication is successful, and whether the user can access the network.

3.3.2. Abnormal Test. The abnormal test is mainly divided into the following aspects: (1) The link is repeatedly UP/DOWN, (2) malicious protocol message attack, and (3) interface plugging and unplugging.

The abnormal test is a test of the certification stability and certification reliability of the project. During the authentication process, various abnormal conditions will be

Table 1: Performance test results.

Test item	Test content	Test results
Performance testing	Whether a large number of users can be successfully authenticated at the same time	Success
	Whether the network access control system is running stably, check the memory usage condition	Memory usage finally stabilized
	Whether the data on the main board and the standby board are consistent	Consistent data

Table 2: Abnormal test results.

Test item	Test content	Test results
Performance testing	The link repeatedly up/down, whether the packet is retransmitted	There is debugging information for retransmission of packets
	Construct the correct protocol packet attack and observe the debugging information	Message is discarded
	Construct wrong protocol packet attack, observe debugging information	Message is discarded
	Plug and unplug the interface and observe whether the main/standby switchover is successful	Active/standby switchover succeeded

checked to ensure that the high security and reliability requirements of the gateway authentication are met.

4. Application Research Analysis of Access Control System Based on Big Data in Education Information Security Guarantee

According to the demand analysis and test content of the network access control system, black box testing is used to construct test cases to test whether the system meets the expected goals. When testing the user permissions of the traditional and the network access control system constructed in this article, the test times are 1000 times each, a total of 2000 times; the test results are shown in Figure 2.

When testing the functions of the traditional and the network access control system constructed in this article, the test times are 1000 times each, totaling 2000 times, and the test results are shown in Figure 3.

When testing the performance of the network access control system, the test results are shown in Table 1.

When the performance of the network access control system is abnormally tested, the test results are shown in Table 2.

It can be found from the test that the network access control system basically achieves the expected functional requirements and performance requirements. Because the networking environment is relatively simple and combined with the combination of testing in a simulated environment, there is still a certain gap between the actual situation and the actual situation.

5. Conclusions

With the rapid development of information technology, the problem of information security threats is also increasing day by day, and the requirements for information security are also increasing. This makes the information security system must continue to develop rapidly to face and meet the emergence and upcoming emergence security threats. This topic discusses the application research of access control system based on big data in education information security and takes the application of access control system in education information security as the research goal and fully studies the basic theories, core methods, and basic principles of access control systems, using the existing model of information system security, from the physical. Starting from the perspective of, while emphasizing technology, network, organization, and management, we build a security model of the education system with security strategy as the main content. It also analyzes the security issues and security technologies (data encryption, intrusion detection, identity authentication, etc.). It focuses on the analysis of the security access control technology in the education information system. The access control used in this article adds a third-level element between the subject and the object to link the authority and authorization of the subject and the object, which makes it easier to connect computer expression with reality. There are some shortcomings in the access control model proposed in this paper. And in the research of this article, the experiment is mainly based on an access control model, and the object of the experiment has greater limitations. In future research, modern artificial intelligence technology, neural network, and other related content will be combined to design an access control model. At the same time, we should also consider strengthening resource management and access control strategies to improve resource flexibility and scalability.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there is no conflict of interest with any financial organizations regarding the material reported in this manuscript.

Authors' Contributions

Zhong Peng and Feng Liang contributed equally to this work as co-first author.

Acknowledgments

This paper is one of the following projects "supported by 1000 Middle-aged and Young Backbone Teachers Cultivation Plan of Guangxi Colleges and Universities" Program Research funding: The Theory and Empirical Study of Community Sports Public Facilities Management Service Outsourcing in Guangxi.

References

[1] N. Kumar Thanigaivelan, E. Nigussie, A. Hakkala, S. Virtanen, and J. Isoaho, "CoDRA: context-based dynamically reconfigurable access control system for android," *Journal of Network and Computer Applications*, vol. 101, no. jan., pp. 1–17, 2018.

[2] A. S. Konoplev and M. O. Kalinin, "Access control system for distributed computing networks," *Automatic Control & Computer Sciences*, vol. 50, no. 8, pp. 664–668, 2016.

[3] D. Gruntz, C. Arnosti, and M. Hauri, "MOONACS: a mobile on-/offline NFC-based physical access control system," *International Journal of Pervasive Computing & Communications*, vol. 12, no. 1, pp. 2–22, 2016.

[4] R. S. Hsiao, T. X. Chen, C. H. Kao, H. P. Lin, and D. B. Lin, "An intelligent access control system based on passive radio-frequency identification.," *Sensors and materials: An International Journal on Sensor Technology*, vol. 29, no. 4, pp. 355–362, 2017.

[5] S. Doi, H. Ide, K. Takeuchi, and S. Fujita, "Development of opt-in agreement and access control system for patients in a personal health record," *Transactions of Japanese society for Medical and Biological Engineering*, vol. 55, no. 1, pp. 45–49, 2017.

[6] S. Namasudra and P. Roy, "PpBAC," *Journal of Organizational and End User Computing*, vol. 30, no. 4, pp. 14–31, 2018.

[7] H. Kaffel-Ben Ayed and B. Zaghdoudi, "A generic Kerberos-based access control system for the cloud," *Annals of Telecommunications*, vol. 71, no. 9-10, pp. 555–567, 2016.

[8] R. Thirukkumaran and P. Muthukannan, "TAACS-FL: trust aware access control system using fuzzy logic for internet of things," *International Journal of Internet Technology & Secured Transactions*, vol. 9, no. 1/2, pp. 201–220, 2019.

[9] F. P. Diez, D. S. Touceda, J. S. Camara, and S. Zeadally, "Lightweight access control system for wearable devices," *IT professional*, vol. 21, no. 1, pp. 50–58, 2019.

[10] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, pp. 42–52, 2018.

[11] C. Anglès–Tafalla, J. Castellà-Roca, M. Mut–Puigserver, M. M. Payeras–Capellà, and A. Viejo, "Secure and privacy-preserving lightweight access control system for low emission zones," *Computer Networks*, vol. 145, pp. 13–26, 2018.

[12] Q. Wang, Z. Mu, and L. Jin, "Control method of robot detour obstacle based on EEG," *Neural Computing and Applications*, pp. 1–8, 2021.

[13] O. S. Amosov, S. G. Amosova, Y. S. Ivanov, and S. V. Zhiganov, "Using the deep neural networks for normal and abnormal situation recognition in the automatic access monitoring and control system of vehicles," *Neural Computing and Applications*, vol. 33, no. 8, pp. 3069–3083, 2021.

[14] P. Andriotis, G. Stringhini, and M. A. Sasse, "Studying users' adaptation to Android's run-time fine-grained access control system," *Information Security Technical Report*, vol. 40, pp. 31–43, 2018.

[15] M. Kuzlu, C. Fair, and O. Guler, "Role of artificial intelligence in the internet of things (IoT) cybersecurity," *Discover Internet of Things*, vol. 1, no. 1, 2021.

[16] M. S. Heer, H. Chavhan, V. Chumber, and V. Sharma, "A study of internet of medical things (IoMT) used in pandemic Covid-19 for healthcare monitoring services," *Journal of Cybersecurity and Information Management*, vol. 5, 2020.

[17] W. Susilo, P. Jiang, F. Guo, G. Yang, Y. Yu, and Y. Mu, "EACSIP: extendable access control system with integrity protection for enhancing collaboration in the cloud," *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 12, pp. 3110–3122, 2017.

[18] P. C. Huang, C. C. Chang, Y. H. Li, and Y. Liu, "Efficient access control system based on aesthetic QR code," *Personal and Ubiquitous Computing*, vol. 22, no. 9, pp. 1–11, 2018.

[19] Z. Yushu, H. Qi, C. Guo, Z. Xinpeng, and X. Yong, "A low-overhead, confidentiality-assured, and authenticated data acquisition framework for IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7566–7578, 2019.

[20] R. Wang, Y. Wei, H. Song et al., "From offline towards real-time verification for robot systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1712–1721, 2018.

[21] J. Ghanta, B. Tarakeswara, and B. Sathyanarayana, "Optimized privacy-preserving access control system for relational incremental data," *International Journal of Computer Applications*, vol. 136, no. 7, pp. 16–19, 2016.

[22] T. Sathishkumar, G. P. Rao, and P. Arumugam, "Database design for physical access control system for nuclear facilities," *Nuclear Engineering and Design*, vol. 305, pp. 68–72, 2016.