Hindawi
Scientific Programming
Volume 2020, Article ID 8875069, 10 pages
https://doi.org/10.1155/2020/8875069

Research Article

A New Scalable and Expandable Access Control Model for Distributed Database Systems in Data Security

Mehmet Guclu, Cigdem Bakir, and Veli Hakkoymaz

Department of Computer Engineering, Yildiz Technical University, Istanbul 34220, Turkey

Correspondence should be addressed to Mehmet Guclu; mehmetguclu007@gmail.com

Received 5 August 2020; Revised 21 August 2020; Accepted 29 August 2020; Published 10 September 2020

Academic Editor: Habib Ullah Khan

Access control models are an important tool developed for securing today's data systems. Institutions use the access control models specifically to define who their employees are, what they can do, which resources they can reach, and which processes they can perform and use them to manage the whole process. This is a very hard and costly process for institutions with distributed database systems. However, access control models cannot be implemented in a qualified way due to the fact that the conditions for defining users' demands to reach resources distributed on different servers, one of which is consequentially bound to the other, the verification and authorization of those user demands, and being able to monitor the actions of the users cannot be configured in an efficient way all the time. With our model suggested in this study, the aim is to automatically calculate the permissions and access levels of all users defined in the distributed database systems for the objects, and, in this way, we will reach a more efficient decision as to which objects the users can access while preventing their access to the information they do not need. Our proposed model in this study has been applied to real life data clusters from organizations providing health and education services and a public service. With the proposed model, all models have been run on servers sharing resources in a private network. The performance of the proposed model has been compared to that of traditional access models. It was confirmed that the proposed model presented an access control model providing more accurate access level results as well as being scalable to many distributed database systems.

1. Introduction

Today, there are new threats damaging the information systems and resources: armored viruses, ransomware, and cryptoLocker malware [1]. Despite the most enterprising steps taken to protect the systems from these harmful threats, the attackers can sometimes be successful. Every phenomenon causing a violation of any one of the principles of confidentiality, integrity, and accessibility—the three main elements of information security—is a violation of security [2]. While some violations deliberately make the systems inaccessible and interrupt services, some of them occur due to accidental software or hardware failures. Either by accident or malice, security violations seriously affect the activity and reliability of an institution.

Denial of service attacks, distributed denial of service attacks, inappropriate surfing behaviors on the Web, wiretapping, access to resources using a backdoor means of access, and accidental or deliberate data interchanges are leading factors causing security violations [3]. Deliberately or accidentally interchanged data affects the integrity principle of security in computing systems and in particular plays a significant role in the occurrence of deliberate or accidental data interchange phenomena [4]. There is a need for a good access model designed according to the scale of the organization and to the confidential access rights necessary for the users to cope with these kinds of problems. In this study, the aim was to automatically calculate the permission and access levels of all users defined in the distributed database systems based on the objects. In this way, a more efficient decision can be reached as to which objects users can access and to prevent their access to information they do not need, in real time.

Access control-based models are one of the most important principal measures used to prevent unauthorized access and minimize the impact of security violation [5]. Today, there are access control models specifically designed. However, it is seen that these models cannot completely

meet the needs of the rapidly increasing number of systems that are becoming more complex day by day, place a serious financial burden on the system, cannot completely ensure data flow control, and, to a great degree, cause a loss of flexibility in the application [6–9]. For this reason, it is also seen that it is not only sufficient for the access control models to be configured to protect the information systems from unauthorized accesses, malicious users, and erroneous use; it is also important that they be easily manageable and scalable in accordance with the organizational structure and that the access control functionality be designed consistently.

There are many real-world applications where static access control models such as judicial network information systems, defense systems, and hospital management systems are not effective. The main reasons for this are as follows: we can list the confidentiality, security restrictions, and level of access difference according to the organizational structure, the initially decided security policies cannot be dynamically changed in accordance with the changing corporate or commercial conditions and business requirements, and the access controls are not easily managed. In our study, referring to such problems that we experience in real system applications allows dynamically changing the permission and access level of the user on the object, based on the current status of the user and object within the organizational structure and/or their status/level of change/updated over time (authority level, some privileges, exceptions, degree of privacy, etc.) that can be adapted to different systems. An access control technique is presented.

The access control model developed in this study addressed the problems frequently faced in applications and provided a model that is more functional, more easily manageable, and more scalable and can deliver more consistent results. The main contribution and aim of this study was to automatically calculate the permission and access levels of all users having an active role in distributed database systems, avoid overauthorization, and deliver more efficient decisions on which objects users can access and prevent their access to information they do not need.

The remaining parts of this study have been organized as follows: there is an introduction in the first section, section two looks at related studies, and materials and methods are covered in section three, while the experimental study is detailed in section four, and section five covers the conclusions.

2. Related Works

Cloud computing is one of the advanced areas in the Information Technology (IT) sector today. Because there are many computer pirates and malicious users on the Internet, it is very important to ensure the confidentiality of the data in the medium of the cloud. For this purpose, it is seen that the number of cloud computing-based advanced access control models has been recently and rapidly increasing [10,11]. Behera and Khilar [12] developed a new access control method. The suggested method authorizes the user according to the user's value before entering the cloud environment. For this, the value of both the user and the cloud resources is calculated. If the value of both the users and the cloud resources is higher than the threshold values, it is deemed as reliable. In another study explaining the validity of current access control models for cloud computing and their services, an access control model increasing the security and preventing unauthorized users from accessing the cloud resources was presented [13].

In the current Distribution Version Control System (DVCS) where the access control principles are distributed across many heterogeneous systems, it is hard to respect the principle of least privilege. In some studies, the main hardships experienced in advance towards a more thorough and manageable access control model in distributed systems have been mentioned [7,9,14]. In one study, an access control architecture that can be adapted by the Industrial Control System (ICS) community has been presented for controlling any access via policies in accordance with the least privilege principle [14]. The aim was to protect central policy management and every bound field device in the suggested architecture. Bertolissi and Fernandez [15] defined a model for their access control design by considering the confidentiality requirements of the distributed media. In this study, a framework was suggested for the implementation of access control policies by taking into consideration the local policies determined by every member on a distributed system consisting of various sites so that each one of them will protect their own resources.

Due to their widespread use, IoT devices are highly likely to contain various security vulnerabilities and threats. Therefore, dealing with IoT-related attacks, vulnerabilities, security, and privacy challenges requires a strong security mechanism. Liao et al. demonstrated that a strong security mechanism can be achieved better with mobile computing, which provides both hardware- and software-based security solutions [16].

There are also some of methodologies put forward to evaluate the security of software components. Fuzzy Logic (FL) approach is modeled to evaluate the safety of components in [17]. The research has shown that the proposed methodology based on ISO/IEC 18028-2 security attributes is useful in situations of uncertainty, thus helping to select the most secure software component. In another study, a method that evaluated the security of software components to enable the software development process is presented [18]. The security of the software component was evaluated using the ANP model based on specific security attributes provided of ISO/IEC 27002. Another study, which presented a system-based differential mathematical model for software birthmark-based comparisons and evaluation of security in end-to-end communication systems, evaluated the smoothing of software piracy and theft detection process and the security of end-to-end communication systems [19]. In another study, it has been shown how data security is ensured with machine learning algorithms [20].

According to the research findings of Rehman et al., it was stated that some people provide fake information to the websites of social media and nonprofit organizations because they think that users collected too much information for the sake of security and individuals feel insecure about

the personal information provided to them [21]. In the study, it was emphasized that it is important to read the minds of the users and get feedback from them in order to minimize this gap between users and service providers.

Data access can be statically inspected using role-based or policy-based access models. However, it was seen that there was still a large gap in the issue of ensuring data access security in the great data age where many studies are conducted on storing today's huge amounts of unconfigured data [22, 23]. There are many real-world applications where static access control systems are not efficient, such as airport search/observation, defense, and hospital management systems [24]. There is a need for a system that learns and adapts according to the user reality. The current role-based access control system easily attracts uninvited guests. Again, in policy-based access control, a deficiency in adaptation occurs because a policy decided at the beginning cannot be dynamically changed. Risk-adaptive access control—suggested by Srivastav and Shekokar —presents a framework that understands the user reality, calculating the risk and acting on this basis afterwards [24]. This framework considers many real-world qualifiers, such as access period, access place, previous history of the request (how many times the same request has been repeated), and the precision of the requested data. Though that study shows similarity to this study in terms of purpose and scope, the previous actions and access requests of the user are not considered in this current study. The model suggested in this study assigns a value to every user in different dimensions appropriate to the organizational structure and relates the access permission to the object with the dimension values and access levels of the user. In other words, it calculates the access permission and level of a user related to an object according to the abilities or values owned by that user.

3. Traditional Access Control Models

In the Mandatory access control model, access of users to the resources is controlled in accordance with certain rules predetermined by a central authority. This type of access control is widely observed in military confidentiality classification. In the Discretionary access control model, users can give access authorizations to other users within the limits assigned to them or they can determine the limitations. This type of access control is commonly seen in folder and file authorizations of operating systems. RBAC provides access rights based on the roles and privileges of the users. RBAC requires users to be assigned to different roles to get the associated permissions. However, the problems of role explosion limit its use to enterprise systems only. Here, a user may have multiple roles or capacities within a given organization. Thus, when the subject is seeking access to an object, the user must first indicate the role within which the request is being made [25].

4. The Proposed Model

The flow diagram of our proposed model is shown in Figure 1.

Data are expressed as objects in our proposed model. Users are classified according to the security dimensions. A security dimension explains the characteristics of a user, and every dimension contains some values that can be assigned to the users. For instance, some example values that can be owned by users in different security dimensions are called Unit, Security Classification, Business Title, and Operation, as shown in Table 1. Unit dimensions within the security dimensions that can be assigned to the user include Unit A, Unit B, Unit C, Unit D, and Unit E values. The Security Classification dimension consists of Top Secret, Secret, and Unclassified values; the Business Title dimension can be Head Doctor, Doctor, IT Personnel, Nurse, and Purchasing Personnel values; and the Operation dimension can consist of Process A, Process B, Process C, Process D, Process E, and Process F values.

A security dimension may have the following characteristics.

4.1. Ordered Dimension. If a dimension is ordered, the dimension values are ordered and the order is compositional; it also covers the values below the value assigned to a user. For example, the values of Top Secret, Secret, and Unclassified values occur in the dimension called Security Classification. A user assigned with the Secret value is also automatically conferred with the Confidential and Unclassified values.

4.2. Unordered Dimension. If a dimension is unordered, the dimension values are not ordered and more than one value can be assigned to a user. For instance, the values of Process A, Process B, Process C, Process D, Process E, and Process F are within the dimension called Operation. A user can take part in both Process C and Process E operations.

A user whose Business Title is Head Doctor assigns the dimension values to other users. At least one value should be assigned to every user from every dimension. However, other values can be assigned in other dimensions. For example, each one of the five users in 2 takes part in different units. While User 1, who is in Unit E and can perform processes C and D, is a nurse in the Confidential Security class, User 4, who is in Unit A and can perform processes A, B, and F, is a doctor from the Confidential Security class.

Each user uses dimension values for the access model. Each user can or cannot access an object according to these dimension values. Namely, a user may have read and write access to an object according to the values taken from all the security dimensions.

Access permission lists should contain a value from each access dimension. In addition, it can also contain some values from the same dimension (such as Process A, Process B, and Process F). The access level of users to objects is determined according to the dimension values taken from each security dimension. For instance, read and write access level can be used for the Purchasing Personnel taking place in the Business Title security dimension and the read only access level can be allocated to the Nurse.

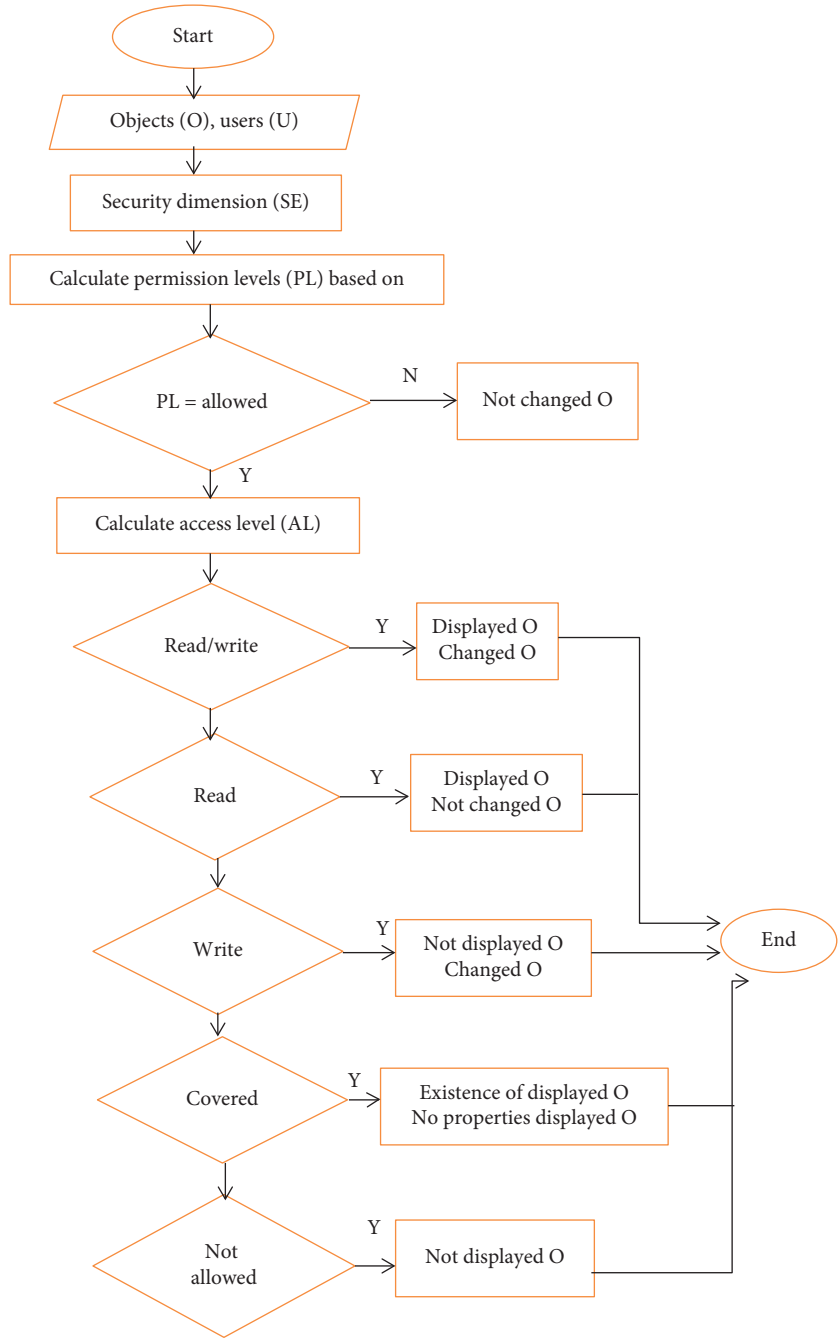

Figure 1: The flow diagram of the proposed model.

Table 1: Security dimensions.

	Security dimension		
Unit	Security Classification	Business Title	Process
Unit A	Top Secret	Head Doctor	Process A
Unit B	Secret	Doctor	Process B
Unit C	Confidential	IT Personnel	Process C
Unit D	Unclassified	Nurse	Process D
Unit E		Purchasing Personnel	Process E
			Process F

Table 2: The dimension values of five different users.

Security dimension	User 1	User 2	User 3	User 4	User 5
Unit	Unit E	Unit B	Unit D	Unit A	Unit C
Security Classification	Confidential	Secret	Confidential	Secret	Top Secret
Business Title	Nurse	IT Personnel	Nurse	Doctor	IT Personnel
Operation	Processes C and D	Processes B, E, and F	Processes C, D, and E	Processes A, B, and F	Processes A, B, C, D, E, and F

4.3. Permission Levels. Permission levels are the different ability levels that allow for changes to the security settings of an object. The permission level for an object is collectively determined from within the permissions assigned to that object:

If the permission level is *Allowed*, the security settings of the object can be changed.

If the permission level is *Not Allowed*, the security settings of the object cannot be changed.

So, if the permission level of an object is *Allowed*, the object can be queried and its security settings can be changed, but if the access level is *Not Allowed*, the object cannot be displayed.

4.4. Access Levels. Access levels are the different ability levels to see or change objects. The access level to an object is collectively determined within the access permissions of the object:

(i) If the access level of a user is *Read/Write*, the object can be displayed and changed

(ii) If the access level of a user is *Read Only*, the object can be displayed but cannot be changed

(iii) If the access level of a user is *Write Only*, the object cannot be displayed but can be changed

(iv) If the access level of a user is *Covered*, the existence of the object can be displayed, but its properties cannot be displayed

(v) If the access level of a user is *Not Allowed*, the object cannot be displayed, and the object does not show up in the query results

4.5. Access and Permission Levels. Access permission to an object is related to the dimension values (the value taken from each dimension by a user, such as the values defined for the 5 different users in Table 2) and access level (Read/Write, Read Only, Covered, or Not Allowed). In other words, the access permission and level are revealed for an object by a user according to the abilities or dimension values owned by that user. If the access level of the user is covered or above (Covered, Read Only, Write Only, and Read/Write), the access of that user to the object is allowed.

4.6. Access Level or Permission Level in One Dimension. Access permission to an object can be related to the values in a dimension for many access levels (e.g.,, while a user could only get the Read Only access level for Process B in the Operation dimension, they could get the access levels of Read and Write for Process C). Permission levels could also be valid for a similar situation. In these situations, the least restrictive access and permission levels are used.

If expressed in an example, the following dimension values could be assigned to a user (Table 3).

The user could display the object with access permissions given in Table 4.

The object could have the permissions given in Table 5.

Object access permissions specify that Process D user membership in the Operation dimension has been set up with *Read/Write* access. Because there is no access permission defined for Process A in the Operation dimension, the user membership for Process A in the Operation dimension is set up with the *Not Allowed* access level. The least restrictive of these access levels is the Read and Write level; for this reason, this access level is used for the Operation dimension.

Object access permissions specify that the Confidential Security Classification of the user has been set up with *Read Only* access—being the least restrictive in this case. Because the object does not have any permission to relate the Nurse Title to a permission level, the resulting permission is the *Not Allowed* level.

4.7. General Access or Permission Level of the Object. The calculation of the least restrictive access or permission level in each dimension may have different results for each dimension. In this situation, the least restrictive access or permission level is used each time.

The general calculation is shown in Figure 2. According to Figure 1, the *Read Only* level is used for the Unit dimension, the *Read/Write* access level is used for the Operation dimension, and the *Read Only* access level is used for the Security Classification dimension. Because the most restrictive one of these levels is *Read Only*, the general access level taken by the user for the object becomes *Read Only*.

5. Experimental Study

Three different real datasets taken from the institutions delivering health, education, and public services have been used in the study, and the success of the suggested access control model and other methods has been assessed according to the results attained from each dataset.

5.1. Datasets. The three datasets used in the study taken from different sectors underwent a preliminary process so

Table 3: Dimension values defined for User 1.

Security dimension	User 1
Unit	Unit E
Security Classification	Confidential
Business Title	Nurse
Operation	Processes C and D

Table 4: Access levels for an object.

Security dimension	Dimension value	Access level
Unit	Unit E	Read Only
	Secret	Write Only
Security Classification	Confidential	Read Only
	Confidential	Covered
Operation	Process A	Read
Operation	Process D	Read/Write

Table 5: Access permissions for the object.

Security dimension	Dimension value	Permission level
Business Title	Doctor	Allowed

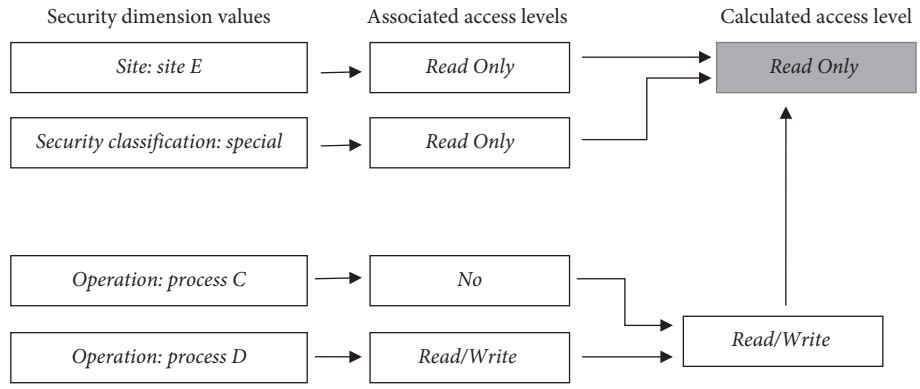

Figure 2: The access level.

that each user and object mentioned in the dataset was classified according to the security dimensions. Real classification scales for these institutions have been taken as the basis for the classification process. The dataset taken from the health sector consisted of 107 users, 36,251 objects, and 8 security dimensions; the dataset taken from the education sector consisted of 292 users, 72,988 objects, and 6 security dimensions, and the dataset taken from the public sector consisted of 1355 users, 752,220 objects, and 11 security dimensions. Datasets have been labeled as the health dataset, education dataset, and public dataset.

5.2. Experimental Analysis. Together with our suggested model, other access control models have been used on a platform operating a real distributed system, and all models have been separately applied to the three datasets. The permission and access level results attained for all models applied to each dataset were compared to the permission and access level results in use by the application belonging to the sector from which the dataset was taken, and the performance values of the methods were compared.

Table 6 shows the calculated access permission and level results for an object with ID number "1" in the health dataset. Table 7 shows the valid access permission and level results for an object with ID number "1" in the health dataset. When both tables were compared, the calculated access permissions appear to be 100% similar to the valid access permissions. While the valid access level for User 4 is Read/Write, the calculated access level is found as Only Write. In this case, while the accuracy rate of the calculated access permission for the object with ID number "1" is 100%, the accuracy rate of the calculated access level will be 75%.

The percentages of correct permission and access level detection for each method were taken as the basis for the performance assessment of the methods applied to the datasets.

Table 6: Calculated access permission and level results.

Dataset: health	Object ID: 1	Users	Permission level	Access level
		User 1	Allowed	Only Read
		User 2	Allowed	Read/ Write
		User 3	Not Allowed	Not Allowed
		User 4	Allowed	Only Write

Table 7: Access permission and level results in industry.

Dataset: health	Object ID: 1	Users	Permission level	Access level
		User 1	Allowed	Only Read
		User 2	Allowed	Read/ Write
		User 3	Not Allowed	Not Allowed
		User 4	Allowed	**Read/ Write**

5.3. Performance Results of the Proposed Model. Test results for the suggested model applied to the health, education, and public datasets are shown in Table 8. The testing showed that the suggested model achieved a correct permission level of 98.20% for the health dataset and access levels were correctly detected in 94.70% of cases where the object permission level had been correctly detected. For the education dataset, permission levels were correctly detected in 95.03% of cases, and access levels were correctly detected in 90.95% of cases where the object permission level had been correctly detected. For the public dataset permission levels were correctly detected in 97.91% of cases; access levels were correctly detected in 95.12% where the object permission level had been correctly detected.

When the results produced by the suggested model were assessed, it could be said that the suggested model achieved correct access permission and access level at 90% and above in the datasets belonging to the three different sectors. In addition, it was observed that as the security dimension (number of properties) increased, the success ratio for detection at the access level also increased (Figure 3). In addition, when the security dimension number was higher than other datasets, the success ratio was higher, as in the public dataset where the number of users and objects is higher compared to the others.

5.4. Performance Results for the RBAC. Test results for the role-based access control model on the health, education, and public datasets are shown in Table 9. The testing showed that this model achieved a correct permission level of 92.17% for the health dataset and access levels were correctly detected in 90.63% of cases where the object permission level had been correctly detected. For the education dataset, permission levels were correctly detected in 89.09% of cases, and access levels were correctly detected in 85.98% of cases

Table 8: Permission and access level performance of the proposed model.

	Access permission	Access level
Health dataset	98.20%	94.70%
Education dataset	95.03%	90.95%
Public dataset	97.91%	95.12%

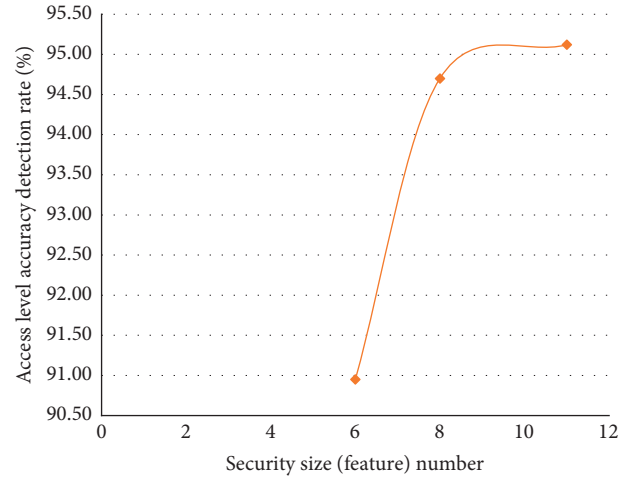

Figure 3: Access level success rate according to the number of security dimensions.

Table 9: Permission and access level performance for RBAC.

	Access permission	Access level
Health dataset	92.17%	90.63%
Education dataset	89.09%	85.98%
Public dataset	89.42%	82.77%

where the object permission level had been correctly detected. For the public dataset, permission levels were correctly detected in 89.42% of cases; access levels were correctly detected in 82.77% where the object permission level had been correctly detected.

When the results rendered by the RBAC model were assessed, it was shown that the model detected correct access permission and access levels at 90% and above in the health dataset consisting of less users and objects, but a decrease was observed in the accuracy percentage of the access level, especially as the number of users and objects increased.

5.5. Performance Results for the MAC/DAC. Test results for the MAC/DAC on health, education, and public datasets are shown in 10. In the test results for this model, the performance percentage of the model for MAC and DAC with the higher access permission and access level accuracy has been taken as the basis for the assessment. The testing showed that this model achieved a correct permission level of 87.60% for the health dataset and access levels were correctly detected in 86.02% of cases where the object permission level had been correctly detected. For the education dataset, permission

Table 10: Permission and access level performance of MAC/DAC.

	Access permission (%)	Access level (%)
Health dataset	87.60	86.02
Education dataset	84.79	81.39
Public dataset	84.21	79.54

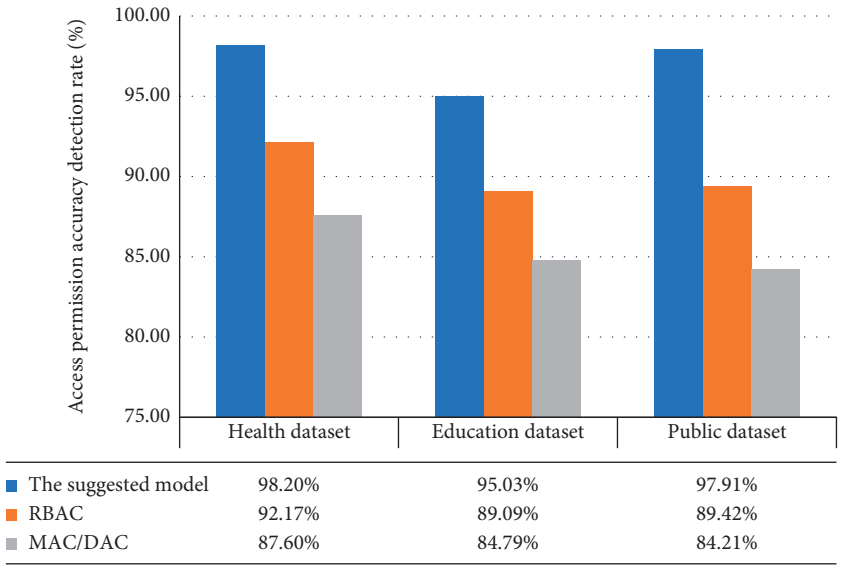

Figure 4: Correct detection rate for access permission in the three models.

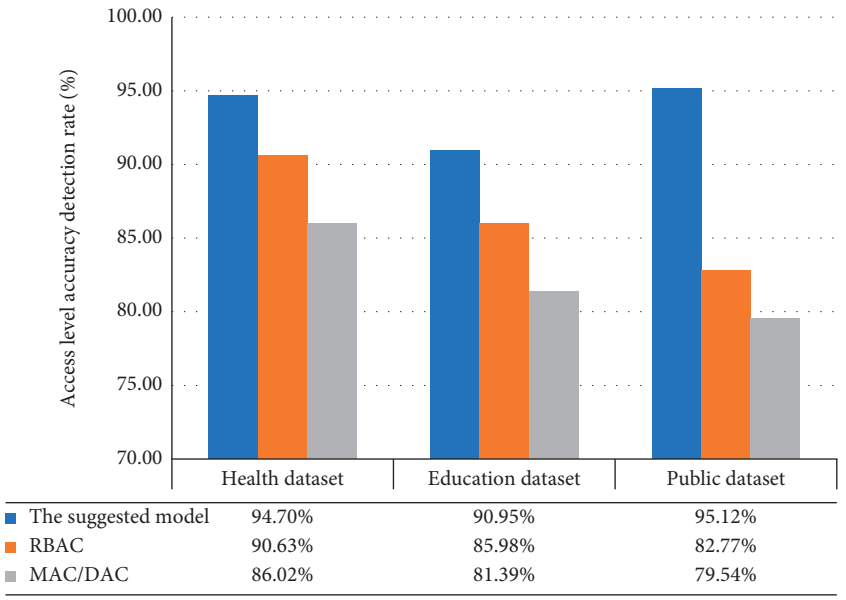

Figure 5: Correct detection rate for access level in the three models.

levels were correctly detected in 84.79% of cases, and access levels were correctly detected in 81.39% of cases where the object permission level had been correctly detected. For the public dataset, permission levels were correctly detected in 84.21% of cases; access levels were correctly detected in 79.54% where the object permission level had been correctly detected.

When the results produced by the MAC/DAC models were assessed, as in the RBAC model, it was shown that this model also delivered higher percentages of correct access permissions and access level in the health dataset, but a decrease was observed in the accuracy of access permissions and access levels, especially as the number of users and objects increased.

5.6. Performance Evaluation. Given that the suggested model delivered more successful results for the access permission and access level detection rate when compared to other techniques—as seen in Figures 4 and 5—it can be said that it achieved correct detection rate of 90% and above in all three datasets. The other techniques were less successful in datasets with high numbers of users and objects. So, this result showed a more expandable technique for different sector applications compared to other techniques and a more scalable technique for the same sector applications.

6. Conclusions

The proposed new access control model investigated in this study was applied to a real distributed system, and, in this way, calculations were made as to which users could access the data stored in different physical media with access permission and level.

With the access control that we proposed in the study, access permissions of users to an object in a distributed environment are associated with the dimension values and object access levels owned by the user. Compared to other access control methods based on performance evaluation, the proposed model dynamically calculates the user's access and level on an object based on the specific permissions and powers that a user has, the size values assigned to him, and the access permissions and levels of the object.

When the experimental results delivered by the suggested model were assessed, the suggested model was applied to the datasets belonging to three different sectors taken from real life and the performance of the suggested model was compared to the Traditional Access Control frequently encountered in real system applications. It has been shown that the suggested model delivered correct access permission and access level 90% and above cases in all three datasets and also delivered successful results in a way that was scalable for all three sectors when compared to other models. As a result, the particular problems frequently faced in distributed system applications were dealt with and the suggested model is expandable and scalable for distributed systems while delivering more consistent authorization results.

As a continuation of this study, the suggested model will be developed and a new framework, taking the access period, access place, and user behaviors as the basis for the design, will be presented.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. E. Whitman and H. J. Mattord, *Principles of Information Security, Course Technology*, Cengage Learning, Boston, MA, USA, 2012.

[2] M. G. Solomon and D. Kim, *Fundamentals of Information Systems Security*, Jones & Bartlett Learning, Burlington, MA, USA, 3rd edition, 2016.

[3] M. Guclu, C. Bakir, V. Hakkoymaz, and B. Diri, "Comparisons on intrusion detection and prevention systems in distributed databases," *Balkan Journal of Electrical and Computer Engineering*, vol. 7, pp. 446–455, 2019.

[4] J. Andress, *The Basics of Information Security Understanding the Fundamentals of InfoSec in Theory and Practice*, pp. 17–49, Elsevier, Amsterdam, Netherlands, 2011.

[5] A. S. M. Kayes, W. Rahayu, P. Watters, M. Alazab, T. Dillon, and E. Chang, *Achieving security scalability and flexibility using Fog-Based Context-Aware Access Control*, vol. 107, pp. 307–323, Elsevier, Amsterdam, Netherlands, 2020.

[6] M. Kotari and N. N. Chiplunkar, *Investigation of Security Issues in Distributed System Monitoring, Information Sciences*, pp. 609–634, Springer, Berlin, Germany, 2020.

[7] M. Kotari and D. N. N. Chiplunkar, "Framework of security mechanisms for monitoring adaptive distributed systems," *IOSR Journal of Computer Engineering*, vol. 18, no. 04, pp. 25–36, 2016.

[8] M. S. Shin, H. S. Jeon, Y. W. Ju, B. J. Lee, and S. P. Jeong, "Constructing RBAC based security model in u-healthcare service platform," *The Scientific World Journal*, vol. 2015, Article ID 937914, 13 pages, 2015.

[9] J. Reid, I. Cheong, M. Henrickson, and J. Smith, "A novel use of RBAC to protect privacy in distributed health care information systems," in *proceedings of the 8th Australasian Conference on Information Security and Privacy (ACISP 2003)*, Wollongong, Australia, July 2003.

[10] J. Li, Z. Liao, C. Zhang, and Y. Shi, "A 4D-role based access control model for multitenancy cloud platform," *Mathematical Problems in Engineering*, vol. 2016, Article ID 2935638, 16 pages, 2016.

[11] R. Lu, Y. Rahulamathavan, H. Zhu, C. Xu, and M. Wang, "Security and privacy challenges in vehicular cloud computing," *Mobile Information Systems*, vol. 2016, Article ID 6812816, 2 pages, 2016.

[12] P. K. Behera and P. M. Khilar, "A novel trust based access control model for cloud environment," in *Proceedings of the International Conference on Signal, Networks, Computing, and Systems*, Springer, Rourkela, India, pp. 285–295, 2016.

[13] S. Pandey, A. Dwivedi, J. Pant, and M. Lohani, "Security enforcement using TRBAC in cloud computing," in *Proceedings of the International Conference on Computing, Communication and Automation (ICCCA)*, pp. 1232–1238, IEEE, Noida, India, 2016.

[14] J. H. Huh, R. B. Bobba, T. Markham et al., "Next-generation access control for distributed control systems"" *IEEE Internet Computing*, vol. 20, no. 5, pp. 28–37, 2016.

[15] C. Bertolissi and M. Fernández, "A metamodel of access control for distributed environments: applications and properties," *Information and Computation*, vol. 238, pp. 187–207, 2014.

[16] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[17] S. Nazir, S. Shahzad, S. Mahfooz, and M. . Nazir, "Fuzzy logic based decision support system for component security evaluation," *The International Arab Journal of Information Technology*, vol. 15, pp. 1–9, 2015.

[18] S. Nazir, S. Shahzad, M. Nazir, and H. U. Rehman, "Evaluating security of software components using analytic network

process," in *Proceedings of the 11th International Conference on Frontiers of Information Technology (FIT)*, pp. 183–188, IEEE, Islamabad, Pakistan, 2013.

[19] M. Li, S. Nazir, H. U. Khan, S. Shahzad, and R. Amin, "Modelling features-based birthmarks for security of end-to-end communication system," *Security and Communication Networks*, vol. 2020, Article ID 8852124, 9 pages, 2020.

[20] J. Zhang, S. Nazir, A. Huang, and A. Alharbi, "Multicriteria decision and machine learning algorithms for component security evaluation: library-based overview," *Future of Information and Communication Conference*, vol. 2, pp. 964–974, 2019.

[21] H. U. Rehman, A. U. Rehman, S. Nazir, I. U. Rehman, and N. Uddin, "Privacy and security—limits of personal information to minimize loss of privacy," *Future of Information and Communication Conference*, vol. 2, pp. 964–974, 2019.

[22] K. Szczypiorski, L. Wang, X. Luo, and D. Ye, "Big data analytics for information security," *Security and Communication Networks*, vol. 2018, Article ID 7657891, 2 pages, 2018.

[23] P. Angin, B. Bhargava, and R. Ranchal, "Big data analytics for cyber security," *Security and Communication Networks*, vol. 2019, Article ID 4109836, 2 pages, 2019.

[24] K. Srivastava and N. Shekokar, *Machine Learning Based Risk-Adaptive Access Control System to Identify Genuineness of the Requester*, pp. 129–143, Springer, Berlin, Germany, 2020.

[25] D. Kim and M. G. ve Solomon, *Fundamentals of Information Systems Security*, Jones and Bartlett Publishers Inc., Burlington, MA, USA, 2016.