IRSTI 20.01.07
UDC 20.01 **DOI 10.70239/arsu.2025.t80.n2.06**

AUTHORIZATION IN ELECTRONIC HEALTHCARE SYSTEMS

PENELOVA M.*, DIMITROV V.

Penelova Maria – Doctoral student, St. Kliment Ohridski Sofia University, Sofia, Bulgaria
E-mail: i_n_f@abv.bg, https://orcid.org/0000-0002-5005-6446
Dimitrov Vladimir – Professor, St. Kliment Ohridski Sofia University, Sofia, Bulgaria
E-mail: cht@fmi.uni-sofia.bg, https://orcid.org/0000-0002-7441-253X

Abstract. Blockchain electronic record is an innovative approach for storing health information. There is still an issue with protection of blockchain from unauthorized access. Healthcare industry clearly distinguishes several types of users, which can access medical data. Authors recommend to use of roles as authorization policies in healthcare systems. On the other hand, using only roles does not provide detailed checks and is not sufficient for achieving privacy. The paper is concerned with the application of Hybrid Role and Attribute Based Access Control (HRABAC) in blockchain systems. This model uses roles and policy functions with attributes for authorization. Use cases are presented for three roles: Admin, Doctor and Patient. A concrete project with blockchain smart contracts is developed in the programming language Solidity. Data protection with detailed checks is applied from the model HRABAC. The access control decisions are tested with test suite Truffle. The test results meet the requirements for privacy. This paper shows that HRABAC is easy to apply and secure model for blockchain applications in healthcare.

Key words. access control, authorization, blockchain, electronic health records, hybrid role and attribute based access control, smart contracts.

Introduction

Authorization or access control [7] is a part of the security of software applications. It regulates the subject's access requests to an object (resource) according to assigned permissions. For example, the subject can insert or read data, if the corresponding user has been previously authorized to perform such actions in the system.

Authorization is a main task in blockchain and especially in Electronic Health Records (EHRs) [14], because they contain sensitive personal information. Authors recommend roles to be used in EHRs as access control approach [13]. Roles are used as policies in Role-Based Access Control (RBAC) [9], that is published in 1996 [10]. It is the most popular model in enterprise software. RBAC does not check permissions in detail. Attribute-Based Access Control (ABAC) [12] is another popular model for authorization. It provides detailed checks applying fine-grained policies with attributes, that protect personal data. ABAC has a disadvantage – it is complex to be applied. It is a good approach to use benefits of both access control models – RBAC and ABAC [11] and to avoid their limitations.

Role-Based Access Control Using Smart Contract (RBAC-SC) [1] is presented in 2018 and it is designed for blockchain. RBAC-SC consists of a smart contract, that includes functions for creating user-role assignments, and a challenge-response protocol, which verifies the role of the user. RBAC-SC is appropriate for users, that belong to different organizations. It does not provide fine-grained access control.

In 2020 a scalable RBAC system [2] is proposed. It is deployed on network that use a specific blockchain protocol. The nodes share capabilities with gasless transactions. The system lacks detailed authorization checks before accessing an object.

A solution for data management [3] is introduced in 2020. It applies roles and rules in smart contracts for access control purpose. There is peer-to-peer network, where the nodes can participate in different institutions. The access control is distributed between blocks in the application. It does not provide fine-grained access control.

An access control approach using blockchain approach is introduced in 2020 [4]. It is RBAC model designed for blockchain smart contracts and knowledge management system. Algorithms for smart contracts are proposed. This approach does not provide detailed checks before accessing an object.

Dynamic and Fine-grained Role-Based Access Control Scheme [5] is published in 2021. The model is designed for smart contracts. The roles are assigned to user with encryption of attributes. Anyway, there are not detailed checks, when accessing different objects within one role – for example own record and not own record (of another user). Therefore, there is a lack of fine-grained access control.

New architecture with smart contracts, that is designed to IoT, is proposed in 2024 [6]. It uses only attributes and provides fine-grained authorization. The proposed scheme consists of five entities: IoT device, gateway, cloud server, data user and blockchain. IoT device collects data and stores it to cloud servers via using a gateway. The gateway is an agent for a group of devices. It applies access control policies to protect the blockchain nodes. Cloud server stores encrypted data from IoT gateway. Data users obtain ciphertexts from cloud servers and decrypt them. Blockchain stores access control policies in smart contracts. Anyway, authors have concluded, that using only attributes for authorization is complex [11]. Furthermore, in the healthcare industry, roles as job titles: doctor, admin and etc., guarantee that within each role the users have the same access rights. Role as access control policy is more auditable. There is no author who suggests not using roles for healthcare industry [13].

The access control model HRABAC, that is proposed in 2021 [8], extends RBAC with adding policy functions, that compare the values of certain attributes of subject with the values of the relevant attributes of the object. This provides fine-grained access control in the systems, which implement it. In this paper, we will show how to use HRABAC in a blockchain application for the healthcare industry. Different use cases are shown. Smart contracts that implement the model HRABAC in blockchain have been developed and presented.

Materials and methods of research

Let there is a healthcare blockchain application. There are three types of users: admin, doctor and patient. In the context of HRABAC, we can determine three roles: Admin, Doctor and Patient, that are relevant to these three user types.

The role Admin can view all EHRs in the system. The role Admin has no requirement for more detailed authorization checks to be performed.

The users who have the role Doctor can create new EHR and can see only these EHRs, which they have previously created for their own patients.

The users with the role Patient should see only his/her own EHRs.

These use cases for the above-mentioned roles are shown in Figure 1 below.

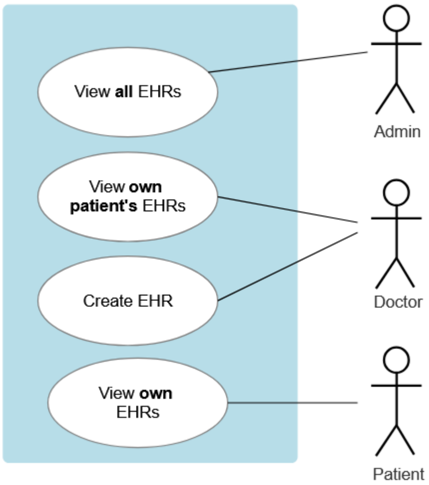
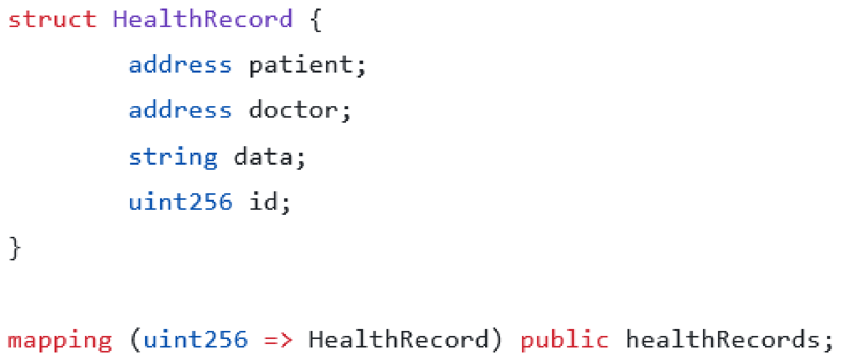


Figure 1. Use-case diagram of electronic healthcare system

A health record in blockchain can be represented as struct in programming language Solidity [15], as it is shown on Listing 1.

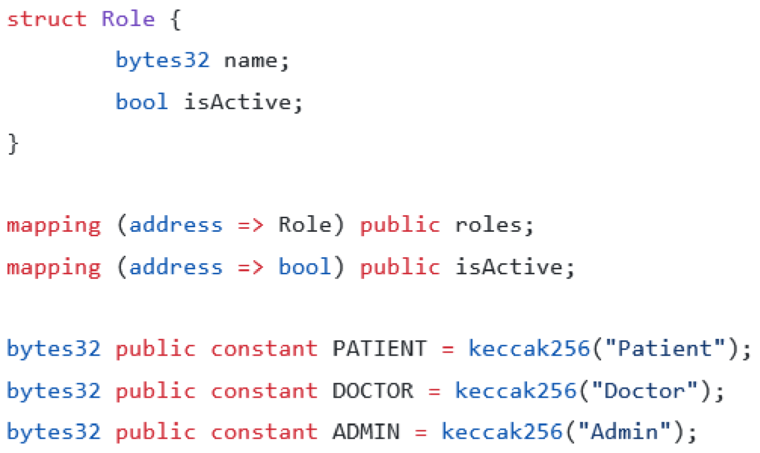


```
struct HealthRecord {
        address patient;
        address doctor;
        string data;
        uint256 id;
}

mapping (uint256 => HealthRecord) public healthRecords;
```

Listing 1. A health record in blockchain

A role can be represented as struct in Solidity. The attribute *isActive* is included for additional security. The names of roles are constants, as it is shown on Listing 2.



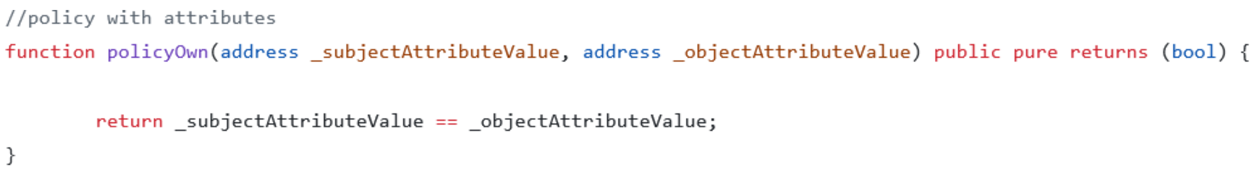
```
struct Role {
        bytes32 name;
        bool isActive;
}

mapping (address => Role) public roles;
mapping (address => bool) public isActive;

bytes32 public constant PATIENT = keccak256("Patient");
bytes32 public constant DOCTOR = keccak256("Doctor");
bytes32 public constant ADMIN = keccak256("Admin");
```

Listing 2. Roles of HRABAC in Solidity

Attribute policies of HRABAC can be implemented as functions in blockchain smart contracts, that compare subject attributes with object attributes, as it is shown on Listing 3.

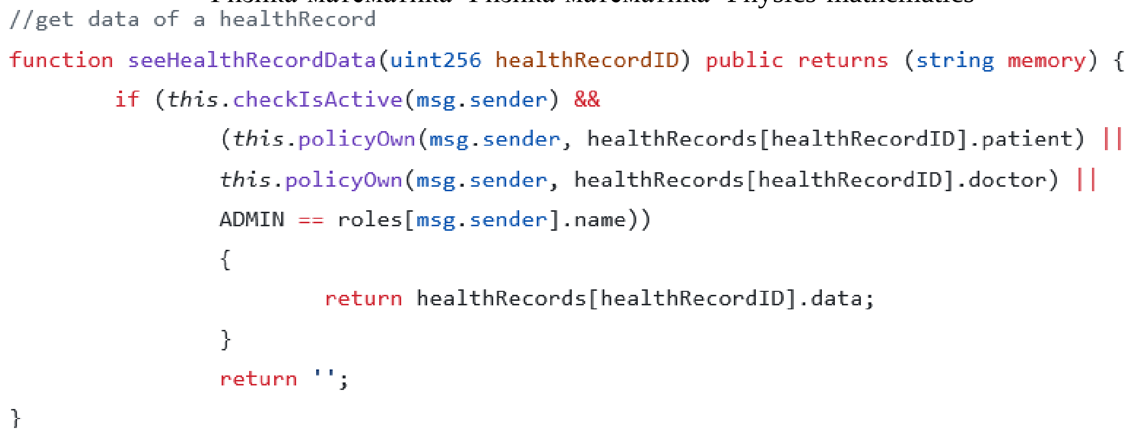


```
//policy with attributes
function policyOwn(address _subjectAttributeValue, address _objectAttributeValue) public pure returns (bool) {

        return _subjectAttributeValue == _objectAttributeValue;
}
```

Listing 3. Attribute policy in smart contract

The access control checks of HRABAC in a function of Solidity smart contract are shown on Listing 4.



```
//get data of a healthRecord
function seeHealthRecordData(uint256 healthRecordID) public returns (string memory) {
        if (this.checkIsActive(msg.sender) &&
                (this.policyOwn(msg.sender, healthRecords[healthRecordID].patient) ||
                this.policyOwn(msg.sender, healthRecords[healthRecordID].doctor) ||
                ADMIN == roles[msg.sender].name))
                {
                        return healthRecords[healthRecordID].data;
                }
                return '';
 }
```

Listing 4. A function of smart contact that permits/denies access to personal data

There are two types of authorization checks in HRABAC:

- a check for a suitable role;
- applying a policy that compares the values of subject attributes with the values of object attributes.

Results and its discussion

The access control decisions [17] of the proposed implementation of HRABAC are tested with test suite Truffle [16].

In the testing, there are considered the following scenarios:

1. A user, that is assigned to role Doctor, makes an access request to previously created from him/her record with medical information. The user is active and the role is active. The test checks whether the access is permitted. The expected result is, that Doctor can see previously created from him/her EHR;

2. A user with the role Doctor makes an access request for an EHR, which is created from another doctor. The user is active and the role is active. The test checks whether the access request is rejected. The expected result is, that Doctor cannot see an EHR, which is created form another doctor;

3. A user who is assigned to the role Patient tries to access an own EHR. The user and the role are active. The test checks whether the access is granted. The expected result is, that Patient can see his/her own EHR.

4. A user with the role Patient makes an access request for an EHR, that is not owned by him/her. The user and the role are active. The test checks whether the access is denied. The expected result is, that HRABAC prevents Patient to see an EHR of another Patient;

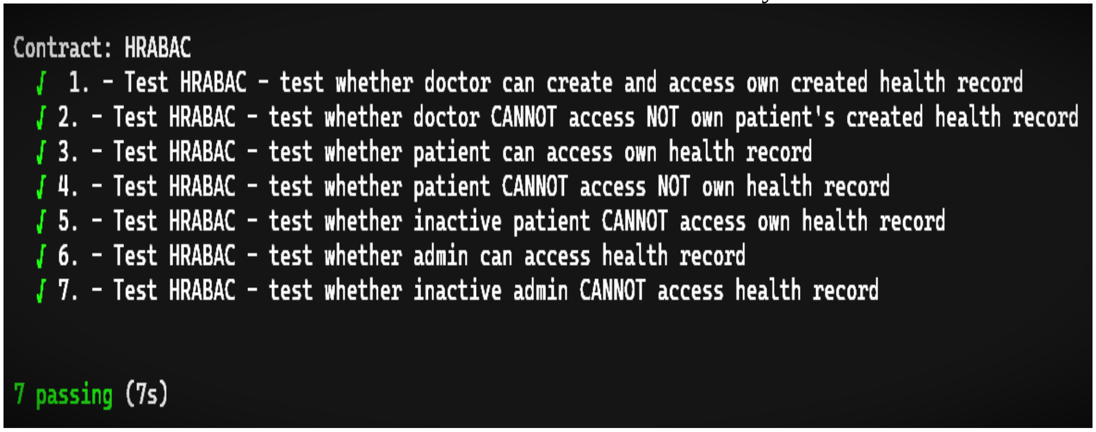
5. A user with inactive account (address), that is assigned to the role Patient, makes an access request to own EHR. The test checks whether the access decision is False (access denied). The expected result is False.

6. A user with the role Admin tries to access an EHR. The user is active and the role is active. The test checks whether this user is able to see the medical information. The expected result is, that Admin can see the EHR.

7. An inactive user with the role Admin makes an access request to an EHR. The test checks whether there is refusal of revealing the medical information (access denied). The expected result is, that inactive Admin cannot see the EHR.

Now, let unit tests be run with Truffle [16]. For each of the mentioned test scenarios, there is a check that compares the actual result with the expected result. If the test passes, this means there is no divergence between the result and expectation.

The results from testing of HRABAC are shown on Figure 2.



```
Contract: HRABAC
  ✓  1. - Test HRABAC - test whether doctor can create and access own created health record
  ✓ 2. - Test HRABAC - test whether doctor CANNOT access NOT own patient's created health record
  ✓ 3. - Test HRABAC - test whether patient can access own health record
  ✓ 4. - Test HRABAC - test whether patient CANNOT access NOT own health record
  ✓ 5. - Test HRABAC - test whether inactive patient CANNOT access own health record
  ✓ 6. - Test HRABAC - test whether admin can access health record
  ✓ 7. - Test HRABAC - test whether inactive admin CANNOT access health record


7 passing (7s)
```

Figure 2. The results from testing HRABAC in healthcare blockchain system

All the tests passed and real results meet the expectations. Therefore, the access control model HRABAC works and it can be implemented in smart contracts, in order to protect data in blockchain healthcare systems.

Conclusion

This paper proposes an example implementation in Solidity of the model HRABAC in blockchain smart contracts designed to healthcare industry. There are three types of roles, that require different level of granularity for each. High granularity is achieved by using policy functions that compare the values of corresponding subject’s attribute and object’s attribute.

The work of the model HRABC is tested against several test scenarios. The unit tests passed without divergence with the actual and the expected result. Therefore, the access decisions are made correctly.

The model HRABAC is proven to be secure. It can be implemented in blockchain smart contracts, in order to keep sensitive data (like medical information) private. In the future, HRABAC can be applied and tested in other new technologies.

References

1. Cruz J., Kaji Y., Yanai N., RBAC-SC: Role-Based Access Control Using Smart Contract. IEEE Access: *12240-122* 2016, Volume 4, pp. 1-12.

2. Rahman M., Scalable Role-Based Access Control Using The EOS Blockchain. arXiv preprint arXiv:2007.02163 2020, https://doi.org/10.48550/arXiv.2007.02163 (accessed on 26.03.2025)

3. Samaniego M., Kassani S., Espana C., Deters R., Access Control Management for Computer-Aided Diagnosis Systems Using Blockchain. arXiv preprint arXiv:2006.11522. 2020, https://arxiv.org/pdf/2006.11522 (accessed on 26.03.2025)

4. Nyame G., Qin Z., Agyekum K., Sifah E., An ECDSA Approach to Access Control in Knowledge Management Systems Using Blockchain. Information 2020, Volume 11, Issue 2, 111. https://doi.org/10.3390/info11020111

5. Liu D., Dong A., Yan B., Yu J., DF-RBAC: Dynamic and Fine-grained Role-Based Access Control Scheme with Smart Contract. Procedia Computer Science 2021, Volume 187, pp. 359-364, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.04.074.

6. Yang Z., Chen X., He Y., Liu L., Che Y., Wang X, Xiao K., Xu G., An attribute-based access control scheme using blockchain technology for IoT data protection, High-Confidence Computing 2024, Volume 4, Issue 3, pp. 1-10

7. Penelova M., Access Control Models. Cybernetics and Information Technologies 2021, Volume 21, Issue 4, Sofia 2021, Print ISSN: 1311-9702; Online ISSN: 1314-40811, DOI: 10.2478/cait-2021-

00444, pp. 77-104.

8. Penelova M., Hybrid Role and Attribute Based Access Control Applied in Information Systems. Cybernetics and Information Technologies 2021, Volume 21, Issue 3, Sofia 2021 Print ISSN: 1311-9702; Online ISSN: 1314-4081, DOI: 10.2478/cait-2021-0031, pp. 85-96.

9. Ferraiolo D., Kuhn D., Chandramouli R. Role-Based Access Control. Second Edition. Publisher: Artech House, 2007, pp. 418

10. Sandhu R., Coyne E., Feinstein H., Youman C. Role-Based Access Control Models. IEEE Computer 1996, Volume 29, No 2, pp. 38-47.

11. Kuhn D., Coyne E., Weil, T. Adding Attributes to Role-Based Access Control. IEEE Computer 2010, Volume 43, No 6, pp. 79-81.

12. Hu V., Ferraiolo D., Kuhn R., Schnitzer A., Sandlin K., Miller R., Karen S. Guide to Attribute Based Access Control (ABAC) Definitions and Considerations. In: NIST Special Publication 2014, 800-162, SIN'13.

13. de Carvalho Junior M., Bandiera-Paiva P. Health Information System Role-Based Access Control Current Security Trends and Challenges. J Healthc Eng. 2018 doi: 10.1155/2018/6510249. PMID: 29670743; PMCID: PMC5836325.

14. Raju N., Quazi F. Blockchain Applications in Electronic Health Records (EHRs). International Journal of Global Innovations and Solutions (IJGIS) 2024, pp. 2 – 15, http://dx.doi.org/10.21428/e90189c8.5043b7de

15. Solidity documentation. Available online: https://docs.soliditylang.org/en/latest/ (accessed on 26.03.2025)

16. Truffle documentation. Available online: https://archive.trufflesuite.com/docs/ (accessed on 26.03.2025)

17. The source code of this paper: Authorization in Electronic Healthcare Systems. Available online: https://github.com/MGP-Ucict/smart-contracts-hrabac (accessed on 26.03.2025)

Әдебиеттер тізімі

1. Cruz J., Kaji Y., Yanai N., RBAC-SC: Role-Based Access Control Using Smart Contract. IEEE Access: 12240-122 2016, Volume 4, pp. 1-12.

2. Rahman M., Scalable Role-Based Access Control Using The EOS Blockchain. arXiv preprint arXiv:2007.02163 2020, https://doi.org/10.48550/arXiv.2007.02163 (accessed on 26.03.2025)

3. Samaniego M., Kassani S., Espana C., Deters R., Access Control Management for Computer-Aided Diagnosis Systems Using Blockchain. arXiv preprint arXiv:2006.11522. 2020, https://arxiv.org/pdf/2006.11522 (accessed on 26.03.2025)

4. Nyame G., Qin Z., Agyekum K., Sifah E., An ECDSA Approach to Access Control in Knowledge Management Systems Using Blockchain. Information 2020, Volume 11, Issue 2, 111. https://doi.org/10.3390/info11020111

5. Liu D., Dong A., Yan B., Yu J., DF-RBAC: Dynamic and Fine-grained Role-Based Access Control Scheme with Smart Contract. Procedia Computer Science 2021, Volume 187, pp. 359-364, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.04.074.

6. Yang Z., Chen X., He Y., Liu L., Che Y., Wang X, Xiao K., Xu G., An attribute-based access control scheme using blockchain technology for IoT data protection, High-Confidence Computing 2024, Volume 4, Issue 3, pp. 1-10

7. Penelova M., Access Control Models. Cybernetics and Information Technologies 2021, Volume 21, Issue 4, Sofia 2021, Print ISSN: 1311-9702; Online ISSN: 1314-40811, DOI: 10.2478/cait-2021-00444, pp. 77-104.

8. Penelova M., Hybrid Role and Attribute Based Access Control Applied in Information Systems. Cybernetics and Information Technologies 2021, Volume 21, Issue 3, Sofia 2021 Print ISSN: 1311-9702;

Online ISSN: 1314-4081, DOI: 10.2478/cait-2021-0031, pp. 85-96.

9. Ferraiolo D., Kuhn D., Chandramouli R. Role-Based Access Control. Second Edition. Publisher: Artech House, 2007, pp. 418

10. Sandhu R., Coyne E., Feinstein H., Youman C. Role-Based Access Control Models. IEEE Computer 1996, Volume 29, No 2, pp. 38-47.

11. Kuhn D., Coyne E., Weil, T. Adding Attributes to Role-Based Access Control. IEEE Computer 2010, Volume 43, No 6, pp. 79-81.

12. Hu V., Ferraiolo D., Kuhn R., Schnitzer A., Sandlin K., Miller R., Karen S. Guide to Attribute Based Access Control (ABAC) Definitions and Considerations. In: NIST Special Publication 2014, 800-162, SIN'13.

13. de Carvalho Junior M., Bandiera-Paiva P. Health Information System Role-Based Access Control Current Security Trends and Challenges. J Healthc Eng. 2018 doi: 10.1155/2018/6510249. PMID: 29670743; PMCID: PMC5836325.

14. Raju N., Quazi F. Blockchain Applications in Electronic Health Records (EHRs). International Journal of Global Innovations and Solutions (IJGIS) 2024, pp. 2 – 15, http://dx.doi.org/10.21428/e90189c8.5043b7de

15. Solidity documentation. Available online: https://docs.soliditylang.org/en/latest/ (accessed on 26.03.2025)

16._Truffle documentation. Available online: https://archive.trufflesuite.com/docs/ (accessed on 26.03.2025)

17. The source code of this paper: Authorization in Electronic Healthcare Systems. Available online: https://github.com/MGP-Ucict/smart-contracts-hrabac (accessed on 26.03.2025)

ЭЛЕКТРОНДЫҚ ДЕНСАУЛЫҚ САҚТАУ ЖҮЙЕСІНДЕ АВТОРИЗАЦИЯ

ПЕНЕЛОВА М.[*], ДИМИТРОВ В.

[*]**Пенелова Мария** – Докторант, «Әулие Клемент Охрид» София университеті, София қ., Болгария
E-mail: bankovagan@fmi.uni-sofia.bg, https://orcid.org/0000-0002-5005-6446
Димитров Владимир – Профессор, «Әулие Клемент Охрид» София университеті, София қ., Болгария
E-mail: cht@fmi.uni-sofia.bg, https://orcid.org/0000-0002-7441-253X

Аңдатпа. Блокчейн электрондық жазба денсаулық туралы ақпаратты сақтауға арналған инновациялық тәсіл болып табылады. Блокчейнді рұқсатсыз кіруден қорғау мәселесі әлі де бар. Денсаулық сақтау саласы медициналық деректерге қол жеткізе алатын пайдаланушылардың бірнеше түрін айқын ажыратады. Авторлар рөлдерді денсаулық сақтау жүйесіндегі рұқсат саясаты ретінде пайдалануды ұсынады. Екінші жағынан, тек рөлдерді пайдалану егжей-тегжейлі тексерулерді қамтамасыз етпейді және құпиялылыққа қол жеткізу үшін жеткіліксіз. Жұмыс блокчейн жүйелерінде Гибридті рөл мен атрибутқа негізделген қол жеткізуді басқаруды (HRABAC) қолдануға қатысты. Бұл үлгі авторизация үшін атрибуттары бар рөлдер мен саясат функцияларын пайдаланады. Қолдану жағдайлары үш рөлге арналған: Әкімші, Дәрігер және Пациент. Solidity бағдарламалау тілінде блокчейн смарт келісімшарттары бар нақты жоба әзірленген. Егжей-тегжейлі тексерулермен деректерді қорғау HRABAC үлгісінен қолданылады. Қол жеткізуді басқару шешімдері Truffle сынақ жиынтығымен тексеріледі. Сынақ нәтижелері құпиялылық талаптарына сәйкес келеді. Бұл құжат HRABAC қолдану оңай және денсаулық сақтау саласындағы блокчейн қосымшалары үшін қауіпсіз модель екенін көрсетеді.

Түйін сөздер: қол жеткізуді басқару, авторизациялау, блокчейн, электрондық медициналық карталар, рөлдер мен атрибуттарға негізделген гибридті қол жетімділікті басқару, ақылды келісімшарттар.

АВТОРИЗАЦИЯ В ЭЛЕКТРОННЫХ СИСТЕМАХ ЗДРАВООХРАНЕНИЯ

ПЕНЕЛОВА М.*, ДИМИТРОВ В.

***Пенелова Мария** – Докторант, Софийский университет «Св. Климент Охридский», г. София, Болгария
E-mail: bankovagan@fmi.uni-sofia.bg, https://orcid.org/0000-0002-5005-6446
Димитров Владимир – Профессор, Софийский университет «Св. Климент Охридский», г. София, Болгария
E-mail: cht@fmi.uni-sofia.bg, https://orcid.org/0000-0002-7441-253X

Аннотация. Электронные записи на основе блокчейна представляют собой инновационный подход к хранению медицинской информации. По-прежнему существует проблема защиты блокчейна от несанкционированного доступа. В сфере здравоохранения четко различают несколько типов пользователей, которые могут получить доступ к медицинским данным. Авторы рекомендуют использовать роли в качестве политик авторизации в системах здравоохранения. С другой стороны, использование только ролей не обеспечивает детальной проверки и недостаточно для достижения конфиденциальности. В статье рассматривается применение Гибридного контроля доступа на основе ролей и атрибутов (HRABAC) в блокчейн-системах. В этой модели используются роли и функции политики с атрибутами для авторизации. Представлены варианты использования для трех ролей: Администратор, Врач и Пациент. Конкретный проект с использованием смарт-контрактов на блокчейне разработан на языке программирования Solidity. Применяется защита данных с подробными проверками по модели HRABAC. Решения по контролю доступа проверяются с помощью тестового набора Truffle. Результаты теста соответствуют требованиям конфиденциальности. В данной статье показано, что HRABAC — это простая в применении и безопасная модель для приложений блокчейна в здравоохранении.

Ключевые слова: контроль доступа, авторизация, блокчейн, электронные медицинские карты, гибридное управление доступом на основе ролей и атрибутов, смарт контракты.