ПРИМЕНА БЛОКЧЕЈН ТЕХНОЛОГИЈЕ У ЦИЉУ ОБЕЗБЕЂИВАЊА СИГУРНОСТИ ПОДАТАКА У СЕРВИСИМА ПАМЕТНОГ ЗДРАВСТВА

Алдина Авдић[1] Улфета Маровац [2] Драган Јанковић [3]

Резиме: Коришћење савремених технологија у свим сферама живота нуди могућност прикупљања и обраде података грађана у циљу побољшања квалитета њиховог живота. Прикупљене податке треба сачувати од злоупотребе. Овај рад описује концепте електронске здравствене заштите у паметним градовима, као и проблеме који се јављају у заштити приватности пацијената који користе електронске здравствене услуге. Као једно решење проблема сигурности података у паметним здравственим сервисима предложено је коришћење блокчејн технологије и дати су начини за њену примену.

Кључне речи: здравствени сервиси, паметно здравство, сигурност података, блокчејн, паметни град

APPLICATION OF BLOCKCHAIN TECHNOLOGY IN DATA SECURITY IN SMART HEALTH SERVICES

Abstract: The use of modern technologies in all spheres of life offers the possibility of collecting and processing data of citizens in order to improve the quality of their lives. The collected data should be protected from misuse. This paper describes the concepts of e-health services in smart cities, as well as the problems that arise in protecting the privacy of patients who use e-health. As a solution to the problem of data security in smart health services, the use of blockchain technology has been proposed and ways for its application have been given.

Key words: health services, smart health, data security, blockchain, smart city

1. УВОД

Паметни град је место где традиционалне услуге постају флексибилније и ефикасније јер се користе информационе, дигиталне и телекомуникационе технологије [1]. Коришћење дигиталних технологија пружа боље јавне услуге становницима и ефикасније искоришћавање ресурса. Најважније компоненте паметних градова су паметни транспорт, паметна здравствена заштита, енергетска ефикасност, паметна технологија и инфраструктура, паметно образовање и паметно управљање. Паметна здравствена заштита укључује е-здравство и његове аспекте за побољшање јавних здравствених услуга у паметним градовима [4].

Инфраструктура паметног града укључује физичку инфраструктуру, информационо-комуникационе технологије (ИКТ) и сервисе. Физичка инфраструктура је стварни физички или структурни део паметног града, који укључује објекте, путеве, железнице, систем водоснабдевања итд. ИКТ инфраструктура је компонента паметног града која захваљујући рачунарским системима држи на окупу све остале компоненте. Сервисна инфраструктура заснива се на физичкој инфраструктури и може имати неке ИКТ компоненте [1]. ИКТ инфраструктура паметних градова заснива се на две блиско повезане и нове технологије, Интернету ствари (енгл. Internet of Things, IoT) и Биг Дејта [2], [3]. IoT се састоји од ствари (сензор, уређај повезан на мрежу с могућношћу

[1]PhD student, State University of Novi Pazar, Vuka Karadžića bb, 36300 Novi Pazar, apljaskovic@np.ac.rs
[2]PhD, State University of Novi Pazar, Vuka Karadžića bb, 36300 Novi Pazar, umarovac@np.ac.rs:
[3]PhD, Faculty of Electronic Engineering, University of Nis, Aleksandra Medvedeva 14, 18106 Niš, dragan.jankovic@elfak.ni.ac.rs

интеракције са корисником или управљања другим уређајем), локалне мреже, Интернета и облака. Биг Дејта чине велике количине података прикупљених од сензора, краудсорсинга итд. Складиштење и обрада ових података захтева сложенију обраду.

Да би се ове информације користиле у корист грађана и заштитиле од злоупотребе од стране трећих лица, неопходно је размишљати о њиховој заштити на специфичан начин. Наиме, шифровање ових података спречило би њихову обраду ради прикупљања услуга е-здравства. Супротно томе, ако би подаци остали у изворном облику, било би их лако злоупотребити. Решавање проблема приватности и сигурности података о пацијенту било је мотивација за писање овог рада.

Подаци о пацијенту могу се поделити у две групе: његови лични подаци (име, занимање, место становања) и здравствене информације (историја болести, дијагноза итд.). Електронски медицински извештаји које се не могу користити за откривање идентитета пацијента могу се користити за реализацију различитих здравствених услуга у паметном граду. Стога би требали бити у сировом облику, погодни за даљу прераду, али заштићени од злоупотребе. Погодан метод за заштиту ових података треба да обезбеди:

- заштиту од напада и промена треће стране,
- на основу доступних података не може се закључити идентитет пацијента, и
- да подаци који се могу користити за истраживање нису шифровани.

Због тога смо као решење овог проблема узели у обзир употребу блокчејн технологије [6], која је надалеко позната по крипто валутама. Ова технологија омогућава децентрализацију података, али и шифрирање дела података или чување под псеудонимом, који се може користити за заштиту приватних података. Циљ овог рада је да се искористи блокчејн технологија за обезбеђивање трајности и поузданости података пацијента потребних за примену услуга е-здравства у паметним градовима.

Рад је организован на следећи начин. Друго поглавље описује преглед сличних истраживања. Треће поглавље даје опис тренутно коришћених метода за заштиту података становника паметног града. Затим се даје опис блокчејн технологије. Следи опис интеграције блокчејн технологије и здравствених сервиса кроз чување електронских медицинских извештаја. На крају су дати закључци и правци даљег истраживања.

2. ПОВЕЗАНА ИСТРАЖИВАЊА

Могућност коришћења блокчејн технологије за сигурност трансакција у криптовалутама навела је многе истраживаче да размотре њену употребу у безбедности и приватности података у другим областима.

У раду [6] аутори су описали алгоритме за коришћење блокчејн технологије за чување приватних података. У радовима [5], [7], [8], [9] постоје начини за примену блокчејн технологије у здравственом систему, са нагласком на електронске здравствене услуге.

У раду [10] је описан преглед могућности коришћења блокчејн технологије за децентрализацију и заштиту података у услугама паметног града.

У раду [7] описан је прототип система MedRec за чување здравствених података и података намењених истраживању заснован на блокчејну.

У раду [11] приказани су случајеви употребе блокчејна у здравству и то кроз следеће услуге:

- праћење ланца снадбевања лековима како би се сузбила злоупотреба преписивања опиоида и спречила зависност пацијената од ових лекова,
- чување података за услуге телемедицине,
- контролисано дељење осетљивих података пацијента (праћење канцера, терапије, упути и сл.),
- дигитални идентитет пацијента и лични здравствени картон,
- информације о захтевима за покривање трошкова од стране здравственог осигурања.

Наш се рад, за разлику од горе поменутих, односи на паметне здравствене услуге и разматра начине за интеграцију блокчејн технологије како би се побољшала сигурност пацијената који користе ове услуге, као и за побољшање функционалности самих сервиса паметног здравства.

3. ПОСТОЈЕЋЕ МЕТОДЕ ЗА ЗАШТИТУ ПОДАТАКА У ПАМЕТНОМ ГРАДУ

На основу горе поменутих сервиса паметног здравства, видели смо да прикупљање велике количине информација може бити од велике помоћи пацијенту. Насупрот томе, ови подаци се могу злоупотребити. Што се тиче личних података, могуће је добити информације као што су навике пацијента, социјални статус и, наравно, његово здравствено стање. На пример, у картици здравственог осигурања постоје подаци о занимању и запослењу. У малим местима је чак и на основу ових података могуће открити ко је пацијент.

Ако су кориснички подаци шифровани, из њих се не могу извући нови закључци. Ако остану непромењени, они могу послужити за стицање нових знања, али приватност података је неизвесна. Постоји неколико метода за решавање овог проблема, од којих су најважније:

- Статистичка контрола објављивања. Табеларни подаци прикупљени од пацијената називају се и микроподаци. Овом методом се врши промена микроподатака како би се осигурао минималан губитак информација, истовремено смањујући могућност поновног идентификовања корисника на основу података [12].
- Модел приватности B3 омогућава заштиту приватности када се користе услуге засноване на локацији. Будући да такве услуге примају информације да неко са одређене локације нешто пита, неопходно је онемогућити праћење ових личних података, али само да одговоре на питање [13]. Овај модел се такође може применити на сервисе базиране на локацији у оквиру паметног здравства.
- Модел 5Д приватности [13] заснован је на следећих пет димензија: приватност идентитета, приватност упита, приватност локације, приватност отиска и приватност власника. Овај модел представља проширење претходног модела за последње две димензије. Приватност отиска односи се на заштиту приватности када се користи одговарајућа технологија за прикупљање података сензора, тако да се они не дају трећој особи и не злоупотребљавају. Приватност власника односи се на приватност корисничких података које различите градске службе имају о кориснику.

Недостатак ових метода је што су развијене као начин заштите приватних података свих сервиса паметног града, а да се посебно не решавају проблеми приватности и сигурности података о пацијенту. Такође, ове методе омогућавају сакривање идентитета пацијента, али не пружају заштиту од злоупотребе треће стране. Подаци о здрављу једна су од најосетљивијих категорија података у ИКТ инфраструктури и њихово злоупотреба може довести до најтежих последица, па се мора посебно водити рачуна о њиховој заштити.

4. БЛОКЧЕЈН ТЕХНОЛОГИЈА

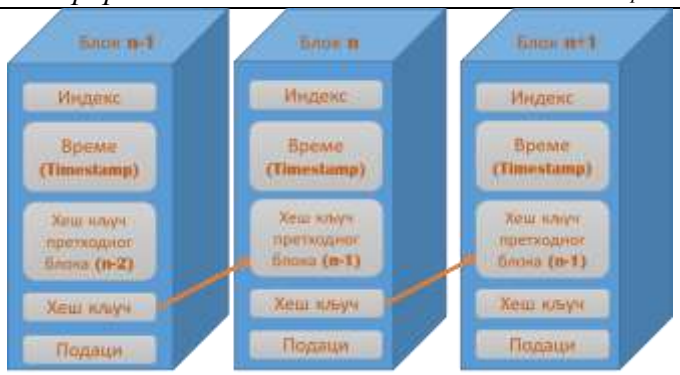
Термин блокчејн везује се за појаву крипто валута. Најпопуларнија међу њима је биткоин, који је први пут описао научник или група њих под псеудонимом Сатоши Накамото 2008. године [14]. У исто време, као начин заштите власништва над крипто валутама, блокчејн је предложен као начин за евидентирање биткоин трансакција.

Функционисање блокчејна може се описати на принципу биткоин трансакције. Слика 1. Блокчејн, у овом случају, представља колекцију дигиталних новчаника. На пример, ако желимо да извршимо пренос биткоина из новчаника А у новчаник Б, сви чланови биткоин блок ланца морају то знати. Креира се нови блок који садржи информације о времену трансакције и информације о њему. Да бисте додали креирани блок у блокчејн, морају га верификовати други у ланцу. На тај начин трансакција је видљива свима.

То значи да су сви подаци о трансакцијама у бази података која се јавно дистрибуира свим власницима, тј. ти подаци су јавно доступни. А податке шаљу корисници који имају псеудоним, па су информације унутар блока анонимне [14], [5].

Слика 2 приказује структуру блокчејна и блока у ланцу. Поред ИД броја блока и времена креирања блока (временска ознака), сваки блок садржи свој хеш кључ у заглављу, као и хеш кључ претходног блока и наравно податке. Подаци у случају криптовалуте су количина новца и трансакције, док ће у нашем моделу садржати информације о пацијенту.

Слика 1 – Снимање трансакције у биткоин блокчејну



Слика 2 – Структура блокчејна

5. ПРИМЕНА БЛОКЧЕЈН ТЕХНОЛОГИЈЕ У СЕРВИСИМА ПАМЕТНОГ ЗДРАВСТВА

Као што је поменуто у претходном поглављу, за сигурност трансакција у криптовалутама, блокчејн се користи као колекција дигиталних новчаника. Све промене се чувају на дистрибуиран и децентрализован начин и немогуће је вршити нерегуларне промене. За здравствени систем са дигиталним услугама које укључују различите врсте клијентских апликација, важно би било прочитати податке, а ако се промене, то би била ваљана промена коју су одобрили учесници у ланцу.

Колекција дигиталних новчаника, у овом случају, била би збирка медицинских картона пацијената једног од паметних градова или држава. Овај начин чувања података гарантује сигурност осетљивих података који се чувају у EMP (електронски здравствени картон). На слици 3 дат је пример чувања EMP-а из МЕДИС.НЕТ [15] информационог система. У пољу за трансакцију чувају се подаци о пацијенту из електронског извештаја за одговарајући преглед. Ови извештаји чине ланац блокова, унутар ког се подаци не могу мењати.

Слика 3 – Структура блокчејна с подацима из EMP-а

Симулација креирања блокчејна у коме су блокови по један медицински извештај одрађена је у програмском језику Пајтон, уз модификацију решења које је дато на линку [16]. Притом је извршено мерење потребно за креирање ланца, блока, и трансакције и добијено просечно време дато је у табели 1. Евидентно је да време за унос података у блокчејн није веће од времена за унос података у било коју базу података, а и једноставна имплементација је додатни аргумент за интеграцију у

здравственим сервисима. У трансакцији се чувају подаци о пацијенту, али само они подаци на основу којих се не може закључити о индентитету пацијента. Број здравственог осигурања представља назив блока у ланцу.

Табела 1 – Време извршења функција за упис EMP-а у блокчејн

Назив функције	**Просечно време извршења (с)**
Креирање блокчејн објекта	1.130000000000575e-05
Креирање блокчејн трансакције	8.30000000000275e-06
Додавање новог блока	0.0001152999999999999874

Поред чувања електронских медицинских извештаја у блокчејну, две врсте паметних здравствених услуга би могле бити омогућене на ефикаснији начин чувањем података у блокчејну:

- **Услуге у којима појединачног пацијента подржава интелигентна здравствена инфраструктура.** На пример, услуга у којој старији пацијенти могу да користе паметне наруквице или мобилну апликацију да притисну помоћно дугме, а преко сензора на IoT уређајима могу да пошаљу тренутне параметре телесне температуре, нивоа шећера у крви, брзине откуцаја срца, притиска и то би могло да се забележи у картону пацијента. Најновији, као и ранији подаци о пацијенту, могу се користити за, на пример, откривање предстојећих проблема и за предлагање начина спречавања различитих врста удара помоћу машинског учења. Овде би се приватни подаци пацијента који се шаљу здравственој инфраструктури паметног града чували у блокчејну.
- **Услуге које користе велике количине података како би извукле закључке о здрављу становништва паметног града.** На пример, подаци свих пацијената могли би се користити за визуелизацију података о зараженост током епидемије или вакцинацији на основу података из EMP. Такође, подаци о епидемијама, (нпр. као што су бројеви заражених, умрлих и на респиратору у току пандемије болести изазване корона вирусом) могли би се чувати у блокчејну, и на тај начин избећи измене и сумње у тачност приказаних бројки.

6. ЗАКЉУЧАК

У раду се описује начин који омогућава складиштење здравствених података помоћу блокчејна из два разлога. Први је дистрибуција података и немогућност њихове промене од стране треће стране, а други је чување података под псеудонимом тако да се подаци не могу злоупотребити, а могу се користити у сврху истраживања или пружања електронских здравствених услуга у паметном граду.

Како се исте одредбе о здравственом систему примењују на нивоу целе земље, будућа истраживања биће усмерена на овај аспект, и на усклађивање са општом регулативом о заштити података ГДПР (енгл. General Data Protection Regulation) [17].

Такође ћемо размотрити како неке од најосетљивијих података учинити заштићеним користећи блокчејн технологију на примеру једног од широко коришћених медицинских информационих система у Србији, МЕДИС.НЕТ.

7. ЗАХВАЛНИЦА

Овај рад је делемично подржан од стране Министарства просвете, науке и технолошког развоја Републике Србије по пројектима ИИИ44007 и ОН 174026.

8. ЛИТЕРАТУРА

[1] Mohanty S. P., Choppali U., & Kougianos E. (2016). *Everything you wanted to know about smart cities: The internet of things is the backbone*. IEEE Consumer Electronics Magazine, бр.5, стр. 60-70.

[2] Zanella A., Bui N., Castellani A., Vangelista L., & Zorzi M. (2014). *Internet of things for smart cities*. IEEE Internet of Things journal, бр.1, стр. 22-32.

[3] Batty M. (2013). *Big data, smart cities and city planning*, Dialogues in Human Geography, бр. 3, стр. 274-279.

[4] Solanas A., Patsakis C., Conti M., Vlachos I. S., Ramos V., Falcone F., & Martinez-Balleste A. (2014). *Smart health: a context-aware health paradigm within smart cities*. IEEE Communications Magazine, бр. 52, стр. 74-81.

[5] Mettler M. (2016). *Blockchain technology in healthcare: The revolution starts here*. e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on IEEE, стр. 1-3.

[6] Zyskind G., & Nathan O. (2015). *Decentralizing privacy: Using blockchain to protect personal data*. Security and Privacy Workshops (SPW), стр. 180-184.

[7] Ekblaw A., Azaria A., Halamka J.D. & Lippman A. (2016). *A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data.* In Proceedings of IEEE open & big data conference, бр. 13, стр. 13.

[8] Linn L.A., & Koo M. B. (2016). *Blockchain for health data and its potential use in health it and health care related research*. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST.

[9] Angraal S., Krumholz H. M. & Schulz W. L. (2017). *Blockchain technology: applications in health care*. Circulation: Cardiovascular Quality and Outcomes бр. 10.

[10] Biswas K. & Muthukkumarasamy V. (2016). *Securing smart cities using blockchain technology*. High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on. IEEE, стр. 1392-1393.

[11] Martinez-Balleste A., Pérez-Martínez P. A., & Solanas A. (2013). *The pursuit of citizens' privacy: a privacy-aware smart city is possible*, IEEE Communications Magazine, бр. 51, стр. 136-141.

[12] Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). *Blockchain technology use cases in healthcare*. In Advances in computers, бр. 111, стр. 1-41.

[13] Satoshi, N. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

[14] https://bitcoin.org/bitcoin.pdf

[15] Milenković A., Janković D., Stojković M., Veljanovski A., & Rajković P. (2014) *Kolaboracija mobilnih senzorskih aplikacija i medicinskog informacionog sistema*. INFOTEH-Jahorina, бр. 13, стр. 879-884.

[16] https://github.com/mchrupcala/blockchain-walkthrough

[17] https://gdpr-info.eu/