IoT მოწყობილობების იდენტობების (Machine Identity-ის) მართვის სისტემა

შარმიაშვილი გიორგი

სამაგისტრო ნაშრომი წარდგენილია ილიას სახელმწიფო უნივერსიტეტის ბიზნესის, ტექნოლოგიისა და განათლების ფაკულტეტის,

ტექნოლოგიის სკოლის, პროგრამული ინჟინერის მაგისტრის აკადემიური ხარისხის მინიჭების მოთხოვნების შესაბამისად

სამაგისტრო ნაშრომი

სამეცნიერო ხელმძღვანელი:

ერეკლე მაღრაძე

ილიას სახელმწიფო უნივერსიტეტი

თბილისი, 2023

განაცხადი

როგორც წარდგენილი სამაგისტრო ნაშრომის ავტორი, ვაცხადებ, რომ ნაშრომი წარმოადგენს ჩემს ორიგინალურ ნამუშევარს და არ შეიცავს სხვა ავტორებისადმი აქამდე გამოქვეყნებულ, გამოსაქვეყნებლად მიღებულ ან/და დასაცავად წარდგენილ მასალებს, რომლებიც ნაშრომში არ არის მოხსენიებული ან ციტირებული სათანადო წესების შესაბამისად.

გიორგი შარმიაშვილი

10 ივლისი2023

მადლობა

მინდა მადლობა გადავუხადო ჩემს ხელმძღვანელს, ბატონ ერეკლე მაღრაძეს, მისი ხელმძღვანელობისა და მხარდაჭერისთვის. მისმა ღირებულმა ცოდნამ და გამოცდილებამ მნიშვნელოვანი როლი ითამაშა ამ ნაშრომის ჩამოყალიბებაში.

შარმიაშვილი გიორგი

სარჩევი

აბსტრაქტი.....5

Abstract.....12

საკვლევი საკითხები.....15

კვლევის მიზანი.....16

ლიტერატურის მიმოხილვა.....17

იმპლემენტაცია.....25

იმპლემენტაციის გაუმჯობესება.....28

დასკვნა.....30

წყაროები.....31

ილუსტრაციების ჩამონათვალი

სურათი 1 - ბლოკჩეინის სტრუქტურა.....17

სურათი 2 - IAM სისტემის არქიტექტურა დაფუძნებული არაკლონირებად ფუნქციაზე.....19

სურათი 3 - წვდომის კონტროლი ჭკვიანი კონტრაკტების გამოყენებით.....21

სურათი 4 - აბსტრაქტული არქიტექტურა შემოთავაზებული სისტემის.....22

სურათი 5 - ყალბი მოწყობილობის იმპლემენტაცია.....25

სურათი 6 - მარტივი იდენტობის მართვის სისტემის იმპლემენტაცია.....26

სურათი 7 - OTA პროტოკოლის არქიტექტურა 29

აბრევიატურების ჩამონათვალი

IAM Systems - Identity and Access Management Systems (იდენტობისა და წვდომის სისტემები)

IoT - Internet Of Things (ნივთების ინტერნეტი)

API - Application Programming Interface (აპლიკაციის პროგრამირების ინტერფეისი)

OTA – Over the Air (საჰაერო განახლება)

აბსტრაქტი

თანამედროვე ციფრულ სამყაროში, სადაც ონლაინ ინტერაქციები და ტრანზაქციები ნორმად იქცა, ციფრული იდენტობის ცნებამ მნიშვნელოვანი ადგილი დაიკავა. ციფრული იდენტობა წარმოადგენს ინდივიდის, ორგანიზაციის ან რაიმე მოწყობილობის უნიკალურობას. ის მოიცავს ატრიბუტებს, ინფორმაციის კრებულს, რომელიც ადასტურებს ამ იდენტობის სინამდვილეს. ციფრულ იდენტობებს დიდი ადგილი უკავია უამრავ სფეროში, მაგალითად: ონლაინ მაღაზია, სოციალური მედია, ფინანსები და სხვა სერვისები. ინდივიდები ქმნიან ციფრულ იდენტობას, გადიან ავთენტიფიკაციას და ამის მეშვეობით ამტიკეცებენ ციფრულ უფლებებს ამა თუ იმ რესურსზე.

იდენტობის და წვდომის სისტემები [1](IAM Systems) დიდ როლს თამაშობს ინდეტობის მართვისათვის და წვდომის ნებართვის განსაზღვრისათვის ბევრ სფეროში. ერთ-ერთი დიდი გამოყენება კი ნივთების ინტერნეტია[2] (IoT). როცა საქმე ეხება ნივთების ინტერნეტის საკითს, იდენტობის და წვდომის სისტემა უნდა იყოს რაც შეიძლება დახვეწილი, დაცული, და უნდა იძლეოდეს ამ ნივთების აუტენტიფიკაციის, იდენტიფიკაციის და ავტორიზაციის მოქნილ შესაძლებლობას.

ინდეტობის და წვდომის სისტემას უნდა შეეძლოს ახალი მოწყობილობის დამატება, ანუ იდენტობის მინიჭება, უნდა იყოს უსაფრთხო, ყველა ნივთს/მოწყობილობას

---

[1] იდენტობისა და წვდომის სისტემები არის უსაფრთხოებისა და ბიზნესის დისციპლინა, რომელიც მოიცავს მრავალ ტექნოლოგიას და ბიზნეს პროცესს, რათა დაეხმაროს ადამიანებს ან მოწყობილობებს საჭირო დროს სწორ აქტივებზე წვდომა ჰქონდეთ.

[2] ნივთების ინტერნეტი არის ფიზიკური მოწყობილობების ქსელი, რომლებიც დაკავშირებულია სენსორებთან, პროგრამულ უზრუნველყოფასა თუ სხვადასხვა ტექნოლოგიებთან მონაცემის გაცვლის მიზნით.

მიანიჭოს კრიპტოგრაფიული გასაღები, რომელიც ამ მოწყობილობის სიცოცხლის განმავლობაში გამოიყენება. ასევე, ამ სისტემას უნდა შეეძლოს უსაფრთხო ავტორიზაცია და მოწყობილობების სიცოცხლის მართვა ანუ იდენტობის მინიჭება, იდენტობის დეაქტივაცია და წაშლა. ასევე მნიშვნელოვანი საკითხია აუდიტი და ჩანაწერები, ანუ რომელმა მოწყობილობამ რა მოქმედება შეასრულა, და რა რესურსთან ჰქონდა ურთიერთობა. ეს ყველაფერი უნდა ინახებოდეს და ამის მონიტორინგი უნდა იყოს მარტივი და მართვადი.

მნიშვნელოვანია ასევე რომ, ინდეტობის და წვდომის სისტემა ადვილად უნდა იყოს ინტეგრირებადი ნივთების ინტერნეტის პლათფორმასთან და კლიენტის ინფრასტრუქტურასთან, თუ კი ასეთი არსებობს. ესეთი შუამავლობა, ხელს შეუწყობს მოწყობილობებისა და კლიენტის მხარეს შორის კომუნიკაციას, უზრუნველყოფს უსაფრთხოებას და კონფიდენციალურობას. ამით შესაძლებელი იქნება უამრავ პლათფორმასთან სწრაფი და მარტივი ინტეგრაცია მცირე დროში, რაც ზოგი ბიზნესითვის ან ინსტიტუტისთვის ძალიან მნიშვნელოვანია.

ზემოთ ნახსენებია ძირითადი მნიშვნელოვანი თვისებები რაც უნდა ჰქონდეს ინდეტობის და წვდომის სისტემას, მაგრამ პრაქტიკაში ამის მიღწევა ხშირ შემხვევაში რთულია და ბევრ პრობლემასთან არის დაკავშირებული (*Access management of Iot devices using access control mechanism and decentralized authentication: A Review*). ტრადიციული იდენტობისა და წვდომის სისტემები დაფუძნებულია ცენტრალურ სტრუქტურაზე და ეს ქმნის საფრთხის ერთ წერტილს, ანუ მაგალითად ეს სისტემა თუ გაშვებულია სერვერზე და სერვერი დროებით გაითიშა სხვადასხვა მიზეზის გამო, ეს სისტემა ვერ იფუნქციონიერბს და დაკავშირებულ ინფრასტრუქტურას გამოიყვანს მწყობრიდან. ასევე თუ ბევრი მოწყობილობაა დაკავშირებული, იდენტობის სისტემის სკალირება გახდება საჭირო, რაც ზოგ შემთხვევაში ზედმეტი ხარჯია ან არასასიამოვნო პროცედურაა. ასევე ძალიან მნიშვნელოვანია უსაფრთხოება, თუ სისტემას სუსტი უსაფრთხოება აქვს, არ არის კარგად შემოწმებული, შეიძლება გახდეს უამრავი კიბერშეტევის მსხვერპლი.

აღწერილი პრობლემებისა და სირთულეების გადასაჭრელად, მნიშვნელოვანია ახალი მიდგომის/ტექნოლოგიის შემუშავება. *ბლოკჩეინი*[3](Blockchain) არის დეცენტრალიზებული ციფრული ტექნოლოგია, რომელიც საშუალებას აძლევს მასში მონაწილე მრავალ მხარეს შეინარჩუნუნ ტრანზაქციის ან ინფორმაციის საერთო ჩანაწერი უსაფრთხო და გამჭვირვალე ფორმით. იგი თავდაპირველად დაინერგა, როგორც ძირითადი ტექნოლოგია კრიპტო-ვალუტისატვის, როგორიცაა ბიტკოინი, მაგრამ მისი გამოყენება გაცილებით სცილდება ბიტკოინის გამოყენების სფეროს.

ბლოკჩეინი არის ბლოკების ჯაჭვი, სადაც თითოეული ბლოკი შეიცავს ტრანზაქციის ან მონაცემების ჩამონათვალს. ბლოკები ერთმანეთთან არის დაკავშირებული კრიპტოგრაფიული ჰეშების გამოყენებით, რაც ქმნის უწყვეტ და უცვლელ ჯაჭვს. ბლოკჩეინი მუშაობს კომპიუტერების ქსელზე, რომელიც ცნობილია როგორც კვანძი (node) და ისინი დაკავშირებულია ერთმანეთთან. თითოეული კვანძი მონაწილეობს ბლოკჩეინის ვალიდაციასა და შენარჩუნებაში.

ბლოკის შექმნის დროს “მაინერები” და ვალიდატორები ქსელში ეჯიბრებიან ერთმანეთს რთული მატემატიკური თავსატეხის გადასაჭრელად. ეს პროცესი მოითხოვს გამოთვლით ძალას, რომელიც ბლოკის შექმნის პროცესს ხდის არც ისე ადვილს და სწრაფს. როგორც კი მაინერი ამოხსნის თავსატეხს, ის გადასცემს ახალ ბლოკს ქსელში. სხვა კვანძები ამოწმებენ ამ ბლოკის ვალიდურობას, აქვს თუ არა სწორი ციფრული ხელმოწერა. მას შემდეგ, რაც ბლოკი გადამოწმებული და შეთანხმებული იქნება ქსელის მიერ, ის ემატება ბლოკების არსებულ ჯაჭვს.

ბლოკჩეინი აღწევს დეცენტრალიზაციას ინფორმაციის გადანაწილებით მრავალ კვანძზე. ეს ხდის მას უფრო მდგრადს შეტევების მიმართ, რადგან მავნე მონაწილეს დასჭირდება კონტროლის მოსაპოვებლად უფრო მეტი გამოთვილი სიმძლავრე ვიდრე

[3] სისტემა, რომელშიც ტრანზაქციები და კრიპტოვალუტაში განხორციელებული აქტივობები ინახება კომპიუტერთა ქსელში

ქსელში ჩართული კვანძების. ამიტომაც თუ ბლოკჩეინს გამოვიყენებთ იდენტობისა და წვდომის სისტემის შექმნისათვის, იგი ბევრ ზემოთხსენებულ პრობლემას გადაჭრის.

ამ ნაშრომის მთავარია არსია გამოვიკვლიოთ ტრადიციული იდენტობისა და წვდომის სისტემების სისუსტეეები და შევაფასოთ ამ სისუსტეების მნიშვნელობა. მოვიძიოთ არსებული კვლევები, რომლებიც გვთავაზობემ ბლოკჩეინ ტექნოლოგიის გამოყენებას იდენტობის სისტემებთან და რამდენად დახვეწილია არსებული იმპლემენტაციები. შემდეგი ნაბიჯი კი იქნება, შევარჩიოთ საუკეთესო იმპლემენტაცია არსებული პრობლემისათვის და შემოგთავაზოთ ამ იმპლმენტაციის გაუმჯობესების გზები.

ნაშრომის სტრუქტურა კი იქნება შემდეგნაირი: გავეცნობით საკვლევ საკითხებს, სადაც ჩამოთვლილი იქნება მნიშვნელოვანი კითხვები, რომლებსაც პასუხი უნდა გაეცეს. შემდეგ მოცემული იქნება კვლევის მიზანი და რა ნაბიჯები უნდა განხორციელდეს ამის მისაღწევად. შემდეგ ძირითადი ნაწილი დაეთმობა ლიტერატურის მიმოხლივას, სადაც შეჯამებული იქნება სხვადასხვა ნაშრომები, რომელიც გვთავაზობს ბლოკჩეინ ტექნოლოგიას ტრადიციული იდენტობის სისტემების გასაუმჯობესებლად. შემოთავაზებული იმპლემენტაციებისაგან, შევარჩევთ საუკეთესოს ამ პრობლემისათვის და შემდეგ განვიხილავთ ამ იმპლემენტაციის გაუმჯობესების გზებს.

Abstract

In today's digital world, where online interactions and transactions have become the norm, the concept of digital identity has assumed an important place. Digital identity is the uniqueness of an individual, organization or any device. It includes attributes, a collection of information that validates that identity. Digital identities play a big role in many areas, for example: online shopping, social media, finance and other services. Individuals create a digital identity, undergo authentication, and thereby assert digital rights to this or that resource.

Identity and access systems (IAM systems) play a major role in managing identity and defining access permissions in many areas. One of the big uses is the Internet of Things (IoT). When it comes to the key to the Internet of Things, the identity and access system must be as sophisticated as possible, secure, and allow for flexible authentication, identification, and authorization of these things. An identity and access system must be able to add new devices, i.e. assign an identity, must be secure, assigning to each item/device a cryptographic key that is used for the lifetime of that device. Also, this system should be capable of secure authentication and device lifecycle management ie identity assignment, identity deactivation and deletion. Auditing and records are also an important issue, i.e. which device performed what action, and with what resource it interacted with. All of this should be stored and monitored in a simple and manageable way. It is also important that the visibility and access system should be easily integrated with the Internet of Things platform and client infrastructure, if any. This mediation will facilitate the communication between the devices and the client side, ensuring security and privacy. This will allow quick and easy integration with many platforms in a short time, which is very important for some businesses or institutions. The main important features that the identity and access system should have are mentioned above, but in practice it is often difficult to achieve this and is associated with many problems (Access management of Iot devices using access control mechanism and decentralized authentication: A Review). Traditional identity and access systems are based on a central structure and this creates a single point of threat, ie if for example this system is running on a server and the server goes down temporarily for various reasons, this

system will fail and the connected infrastructure will fail. Also, if many devices are connected, the identity system will need to be scaled, which in some cases is a costly or inconvenient procedure. Security is also very important, if the system has weak security, is not well tested, it can become a victim of many cyber attacks. To solve the described problems and difficulties, it is important to develop a new approach/technology. Blockchain is a decentralized digital technology that allows multiple parties involved in it to maintain a common record of transactions or information in a secure and transparent manner. It was originally introduced as a core technology for cryptocurrencies such as Bitcoin, but its uses go far beyond the scope of Bitcoin. A blockchain is a chain of blocks where each block contains a list of transactions or data. Blocks are linked together using cryptographic hashes, creating a continuous and immutable chain. Blockchain works on a network of computers known as nodes and they are connected to each other. Each node participates in the validation and maintenance of the blockchain. During block creation, miners and validators compete in the network to solve a complex mathematical puzzle. This process requires computing power, which makes the block creation process not so easy and fast. Once a miner solves a puzzle, it transmits a new block to the network. Other nodes check the validity of this block to see if it has a valid digital signature. Once a block has been verified and agreed upon by the network, it is added to the existing chain of blocks. Blockchain achieves decentralization by distributing information across multiple nodes. This makes it more resistant to attacks, as a malicious actor would need more computing power than the nodes involved in the network to gain control. Therefore, if we use the blockchain to create an identity and access system, it will solve many of the problems mentioned above. The main point of this paper is to examine the weaknesses of traditional identity and access systems and to assess the importance of these weaknesses. Let's look at existing research that suggests using blockchain technology with identity systems and how sophisticated existing implementations are. The next step will be to select the best implementation for the existing problem and suggest ways to improve this implementation. The structure of the paper will be as follows: we will introduce the research issues, where important questions that need to be answered will be listed. Then the purpose of the study and the steps to be taken to achieve it will be given. The main part will then be devoted

to a literature review, summarizing various papers that propose blockchain technology to improve traditional identity systems. From the proposed implementations, we will select the best one for this problem and then discuss ways to improve this implementation.