თანამედროვე მიდგომები IoT ეკოსისტემაში უსაფრთხოების გაძლიერებისთვის

ნინო თოფურია[1], დემურ სიჭინავა[2], იბრაიმ დიდმანიძე[3]

[1]საქართველოს ტექნიკური უნივერსიტეტი
[2]ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი
[3]ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტი
nino.topuria@gtu.ge, demur.sichinava@tsu.ge, ibraim.didmanidze@bs.edu.ge

რეზიუმე

სტატიაში განხილულია ნივთების ინტერნეტის (IoT) ეკოსისტემაში უსაფრთხოების კრიტიკული გამოწვევები და აღწერილია Microsoft Azure Sphere-ის შესაძლებლობები, რომელიც წარმოადგენს ერთ-ერთ მნიშვნელოვან პლატფორმას IoT მოწყობილობების დაცულობის უზრუნველსაყოფად. კვლევა აერთიანებს უსაფრთხოების ინოვაციურ მიდგომებს, მათ შორის Zero Trust არქიტექტურას, Cybersecurity Mesh-ს, ბლოქჩეინზე დაფუძნებულ იდენტობის მართვასა და PUF ტექნოლოგიებს, რაც ხელს უწყობს IoT ინფრასტრუქტურის მდგრადობასა და მასშტაბურობას. წარმოდგენილი ანალიზი აჩვენებს, რომ Azure Sphere-ის ინტეგრაცია Azure IoT Central-თან ამარტივებს არა მხოლოდ მოწყობილობების უსაფრთხოებას, არამედ მონაცემთა მონიტორინგსა და ოპერატიულ ანალიტიკას. შედეგად, კვლევა მიუთითებს, რომ IoT უსაფრთხოების მომავალი ეფუძნება ინტეგრირებულ მოდელს, სადაც გაერთიანებულია ხელოვნური ინტელექტი, ღრუბლოვანი სერვისები და ახალი თაობის ავთენტიფიკაციის მეთოდები.

საკვანძო სიტყვები: ნივთების ინტერნეტი (IoT), ღრუბლოვანი გამოთვლები, IoT-ის უსაფრთხოება, Azure Sphere, Azure IoT Central.

1. შესავალი

ცნობილია, რომ ციფრული ტექნოლოგიები ქმნის ახალ შესაძლებლობებს ყველა ტიპის ორგანიზაციისთვის. რეალურად, ეს არის ახალი მიდგომა, რომელიც აერთიანებს ადამიანებს, მონაცემებს და პროცესებს ერთი საერთო მიზნის მისაღწევად და უზრუნველყოფს წარმატებას ციფრულ სამყაროში. ციფრული ტრანსფორმაცია არის ბიზნეს ინოვაცია, რომელიც ემყარება ღრუბელოვან პლატფორმას, ხელოვნურ ინტელექტს და ნივთების ინტერნეტს (IoT), რაც ორგანიზაციებს ბიზნესის მართვისა და გარდაქმნის ახალ გზებს სთავაზობს.

საწარმოთა ლიდერებმა თანდათან დაიწყეს იმის გაცნობიერება, თუ რამდენად მნიშვნელოვანია ნივთების ინტერნეტი (IoT) მათი კომპანიებისთვის. IoT-ს აქვს მუდმივი უკუკავშირი ცენტრთან და ხელს უწყობს სწორი გადაწყვეტილების მიღებას ნებისმიერ ბიზნესში. IoT პლატფორმა გარდაქმნის ისეთ ინდუსტრიებს, როგორიცაა ჯანდაცვა, ენერგეტიკა, ავტომობილები, წარმოება, ტრანსპორტი და სხვა. IoT-ი იძლევა ბიზნეს პროცესების გაძლიერებისა და გადაწყვეტილებების მიღების შესაძლებლობას სენსორებით, მოწყობილობებით და პლატფორმებით. [1-3].

ნივთების ინტერნეტისა და დაკავშირებული მოწყობილობების ბაზარი სწრაფად იზრდება. მილიონობით მოწყობილობა დაკავშირებულია ღრუბელთან, ხოლო

დაკავშირებული მოწყობილობების უმთავრესი პრობლემა უსაფრთხოებაა. ჰაკერები და თავდამსხმელები იყენებენ დაუცველ მოწყობილობებს, რომლებიც დაკავშირებულია საჯარო ინტერნეტთან. ცნობილია IoT მოწყობილობის მრავალი ფაქტი.

2016 წელს Mirai-ბოტნეტმა შეაფერხა ინტერნეტის ფუნქციონირება. 2017 წელს, ლას-ვეგასის კაზინოში ინტერნეტთან დაკავშირებული თევზის ავზი გამოიყენეს მგრძნობიარე მონაცემების მოსაპარად. 2024-2025 წლებში გამოვლენილია Mirai-ბოტნეტის ახალი მოდიფიკაცია, რომელიც DVR ტიპის (ვიდეოჩანაწერების დასათვალიერებელი მოწყობილობები) სისტემებს ესხმის თავს რისთვისაც მოწყვლად და სუსტ პაროლებს იყენებს. კვლევის მიხედვით, 2024 წელს დაფიქსირდა დაახლოებით 1.7 მილიარდი თავდასხმა IoT მოწყობილობებზე, რომლებიც Mirai-სა და მასთან მსგავს ბოტნეტებს უკავშირდება. 2024 წლის ოქტომბერში Mirai-ბოტნეტის ერთმა მოდიფიკაციამ განახორციელა რეკორდულად მასშტაბური DDoS შეტევა, რომლის სიმძლავრემ 5.6 ტბ/წმ შეადგინა. თავდასხმაში დაახლოებით 13000 IoT მოწყობილობა მონაწილეობდა და ინტერნეტსერვისების მუშაობა დროებით შეაფერხა. 2025 წელს გამოვლინდა BadBox 2.0 ბოტნეტი, რომელიც ზიანს აყენებდა სმარტ-ტელევიზორებს და სხვა IoT მოწყობილობებს. მისი გამოყენება ხდებოდა DDoS თავდასხმებისთვის, თაღლითური სქემების განხორციელებისა და მომხმარებელთა მოწყობილობების არაკანონიერი პროქსი სერვერებად ქცევის მიზნით. Nokia-ს კვლევის შედეგად გამოვლენილი Eleven11bot ბოტნეტი მიზანმიმართულად იყენებდა ვებკამერებსა და ვიდეოჩანაწერების სისტემებს, განსაკუთრებით აშშ-ში, მაღალი მოცულობის DDoS შეტევების ორგანიზებისთვის. აღნიშნული შემთხვევა კიდევ ერთხელ აჩვენებს IoT მოწყობილობების მოწყვლადობის მასშტაბებს.

2. მეთოდოლოგია.

მოცემულ სტატიაში IoT უსაფრთხოების საკითხების კვლევისთვის გამოყენებულია როგორც პრაქტიკული, ისე თეორიული ანალიზის მეთოდები. ტრადიციული უსაფრთხოების მიდგომები (Firewall, VPN, ანტივირუსი) ხშირად საკმარისი არ არის, რადგან IoT გარემო გამოირჩევა: მოწყობილობების ჰეტეროგენურობით – სხვადასხვა მწარმოებლის მოწყობილობები განსხვავებული უსაფრთხოების პროტოკოლებით მუშაობენ; მონაცემთა კონფიდენციალურობით – IoT სენსორები ხშირად აგროვებენ პირად ან კომერციულ ინფორმაციას, რომლის უსაფრთხოება აუცილებელია; რეალურ დროში მოთხოვნებით – სისტემები საჭიროებს სწრაფ რეაგირებას, ამიტომ უსაფრთხოების პროცედურებმა არ უნდა შეანელონ მონაცემთა გადაცემა.

გაანალიზებულია უახლესი სამეცნიერო წყაროები, რომლებიც იკვლევენ IoT მოწყობილობების ავთენტიფიკაციის ახალ მეთოდებს. განხილული მიდგომები მოიცავს მსუბუქ კრიპტოგრაფიას, Zero Trust პრინციპებს, ფიზიკურად არაკოპირებადი ფუნქციების (PUF) გამოყენებას, დეცენტრალიზებულ იდენტობასა და blockchain-ზე დაფუძნებულ ავთენტიფიკაციას. ყურადღება გამახვილებულია Microsoft Azure Sphere-ის პლატფორმაზე, რომელიც აერთიანებს დაცულ SoC არქიტექტურას, ოპერაციულ სისტემას და ღრუბლოვან უსაფრთხოების სერვისს.

3. მსჯელობა.

ბოლო წლებში IoT ეკოსისტემა ინტენსიური ინტეგრაციის პროცესშია ინოვაციურ ტექნოლოგიებთან, რაც ხელს უწყობს ციფრული ტრანსფორმაციის გაღრმავებას და მას ახალი ფუნქციური შესაძლებლობებისა და მდგრადი განვითარების პერსპექტივებით ამდიდრებს. IoT

მოწყობილობების მასობრივი გავრცელების გამო უსაფრთხოება გახდა ერთ-ერთი ყველაზე კრიტიკული საკითხი. უამრავი მოწყობილობა, სენსორი და ქსელის წერტილი ერთმანეთს უკავშირდება, რაც ზრდის ქსელის იერარქიულობას და მრავალდონიან რისკებს.

განვიხილოთ თანამედროვე მიდგომები IoT ეკოსისტემაში უსაფრთხოების გაძლიერებისთვის:

Zero Trust არქიტექტურა, ეს არის პრინციპი: "არავის ენდო, ყოველთვის გადაამოწმე". ყველა მოწყობილობა, მომხმარებელი და სერვისი მუდმივ ავთენტიფიკაციას გადის, რაც მნიშვნელოვნად ამცირებს ქსელში შეღწევის რისკს. მაგალითად, Cisco IoT Threat Defense იყენებს Zero Trust მიდგომას სმარტ ქალაქების ქსელში, უზრუნველყოფს მრავალდონიან დაშვებას და მუდმივ მონიტორინგს.

Cybersecurity Mesh, ეს არის ქსელის უსაფრთხოების განაწილებული მიდგომა, სადაც დაცვა ხდება არა მხოლოდ ცენტრალურ წერტილში, არამედ თითოეულ IoT მოწყობილობაზე. უპირატესობას წარმოადგენს ის ფაქტი, რომ ქსელის ნებისმიერი წერტილი დაცულია, რაც მნიშვნელოვანია მრავალი სხვადასხვა მოწყობილობის მქონე ინდუსტრიულ სისტემებში. მაგალითად, Microsoft Azure Sphere უზრუნველყოფს Microcontroller Units (MCU)-ების უსაფრთხოებას, სენსორების და IoT მოწყობილობების მუდმივ განახლებას, აერთიანებს მოწყობილობებს და ღრუბლოვან უსაფრთხოებას.

შიფრაცია და უსაფრთხო კომუნიკაციები. მონაცემები IoT ქსელში უნდა იყოს დაშიფრული ბოლო წერტილამდე (end-to-end encryption), რათა დაიცვას პირადი მონაცემები და კომერციული ინფორმაცია. მაგალითად, Amazon Web Services IoT Core იყენებს TLS/SSL პროტოკოლებს მოწყობილობიდან ღრუბლამდე ინფორმაციის გადასაცემად.

რისკების მართვა და ხელოვნური ინტელექტით მართული მონიტორინგი. ხელოვნური ინტელექტი ახდენს მოწყობილობების ქცევის ანალიზს, აფიქსირებს ანომალიებს და წინასწარ აფრთხილებს შესაძლო შეტევების შესახებ. მაგალითად, Darktrace IoT იყენებს AI-სა და მანქანური სწავლების ალგორითმებს ქსელის გაუმართლებელი აქტივობის გამოვლენისთვის.

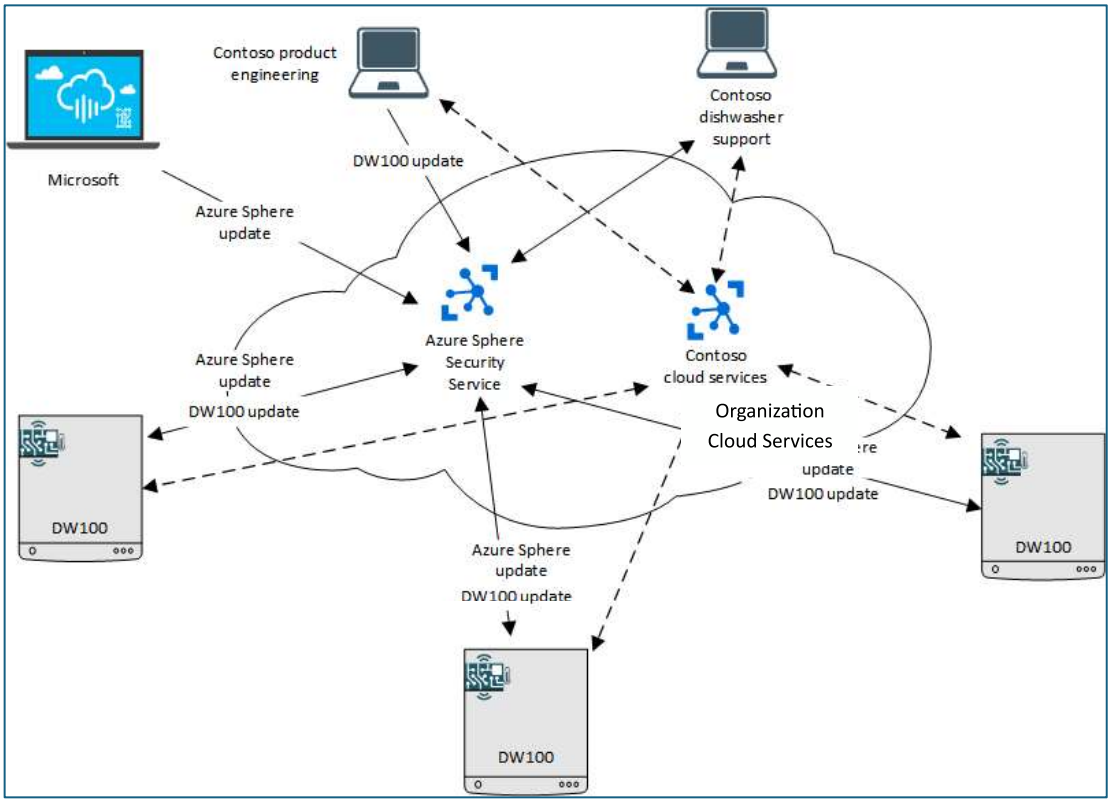
მრავალდონიანი ავთენტიფიკაცია (MFA) IoT კონტექსტში. IoT მოწყობილობები ხშირად მართავენ მნიშვნელოვან პროცესებს (მაგალითად, ენერგეტიკის ან სმარტ შენობების სისტემებს). MFA უზრუნველყოფს, რომ წვდომა მიიღონ მხოლოდ ავტორიზებულმა პირებმა.

პრაქტიკული მაგალითის სახით, განვიხილოთ ფირმა მაიკროსოფტის გადაწყვეტილება - Azure Sphere, რომელიც ქმნის სრულიად ახალ დონეს მწარმოებლებისთვის ციფრული ტრანსფორმაციის ეპოქაში შესასვლელად. ეს საშუალებას აძლევს მათ გაამახვილონ ყურადღება IoT-ზე დაფუძნებულ პროდუქტებზე, სერვისებსა და ფუნქციებზე მთელი მათი ფუნქციონირების განმავლობაში [3].

Azure Sphere - შედგება სამი კომპონენტისგან: დაცული სისტემისაგან უშუალოდ ჩიპზე (SoC), უსაფრთხო ოპერაციული სისტემისაგან და უსაფრთხო ღრუბლოვანი სერვისისაგან. სურ.1-ზე წარმოდგენილი დიაგრამა გვიჩვენებს მთლიან არქიტექტურას და როლს, რომელსაც ასრულებს Azure Sphere Security Service უფრო დიდი IoT სცენარის ფარგლებში, სადაც შესაძლებელია ათასობით Azure Sphere მოწყობილობის განთავსება.

Azure Sphere შაბლონის ტესტირება შესაძლებელია IoT Central-ის საშუალებით [4], რომელიც წარმოადგენს IoT აპლიკაციების პლატფორმას და გვაძლევს საშუალებას შევამციროთ გადაწყვეტილებების შემუშავებისა და მომსახურების ხარჯები კორპორატიულ დონეზე. მისი საშუალებით შესაძლებელია გარკვეული მოვლენების მონიტორინგი, ობიექტებზე თვალყურის დევნება და მართვა, ასევე ჩაშენებული აქვს მოწყობილობების

ანალიტიკის ფუნქციონალიც. IoT ინფრასტრუქტურის შესრულება საბოლოოდ დაეხმარება მწარმოებლებს გააძლიერონ და გააფართოვონ თავიანთი საველე სერვისები. Azure Sphere-ის ეკოსისტემა ამარტივებს პროგნოზირებადი ტექნიკური სისტემების განლაგებას, მართვას და უსაფრთხოებას [5].



სურ. 1 Azure Sphere მოწყობილობის არქიტექტურა

მაგალითისათვის, სტატიაში წარმოდგენილია მოწყობილობის შაბლონი, რომელიც განსაზღვრავს მის შესაძლებლობებს და უკავშირდება IoT Central Application-ს. მოწყობილობის შესაძლებლობებში შედის ტელემეტრია, რომელსაც აგზავნის მოწყობილობა, ასევე ის თვისებები და ბრძანებები, რომლებზეც რეაგირებს მოწყობილობა. მოწყობილობის შაბლონის საშუალებით აპლიკაციაში შესაძლებელია როგორც რეალური, ისე სიმულაციური მოწყობილობების დამატება. იმიტირებული მოწყობილობები სასარგებლოა IoT Central Application-ის ქცევის შესამოწმებლად, სანამ მოხდება რეალურ მოწყობილობებთან დაკავშირება (ნახ.2).

მოწყობილობის შაბლონი არის გეგმა, რომელიც განსაზღვრავს მოწყობილობის ისეთ მახასიათებლებს და ქცევას, როგორიცაა:

- ტელემეტრია ანუ მონაცემების ნაკადი, რომელსაც იგი აგზავნის;
- ბიზნეს თვისებები, რომელთა შეცვლაც შეუძლია ოპერატორს;
- მოწყობილობის თვისებები, რომლებსაც ადგენს მოწყობილობა;
- ოპერატორის მიერ დადგენილი თვისებები, რომლებიც განსაზღვრავენ მოწყობილობის ქცევას;
- ბრძანებები, რომლითაც ოპერატორი მუშაობს მოწყობილობაზე.

სურ. 2 Azure Sphere-ის მუშაობის პროცესი Azure IoT Cental-ის ბაზაზე

შედეგები

კვლევამ აჩვენა, რომ IoT უსაფრთხოების ეფექტიანობა იზრდება, როდესაც გამოიყენება:

- **Azure Sphere-ის ეკოსისტემა** – უსაფრთხო SoC, ოპერაციული სისტემა და ღრუბლოვანი სერვისი, რომელიც ერთიანდება IoT Central-თან;
- **Zero Trust და AI-ზე დაფუძნებული ანალიზი** – რაც ამცირებს შეტევების რისკს და ზრდის ნდობას;
- **PUF და Blockchain ავთენტიფიკაცია** – რომლებიც აუმჯობესებენ იდენტობის მართვას მცირე რესურსების მქონე მოწყობილობებშიც კი.

4. დასკვნა

IoT ეკოსისტემა განიცდის გარდაქმნას უსაფრთხოების ახალი მოდელების დანერგვით. კვლევის შედეგად დადგინდა, რომ Azure Sphere და Azure IoT Central წარმოადგენს პრაქტიკულ გადაწყვეტილებას IoT მოწყობილობების უსაფრთხოებისთვის, ხოლო ინოვაციური მიდგომები (Zero Trust, Blockchain, AI) ქმნის საფუძველს IoT-ის მდგრადი განვითარებისათვის. მომავლის პერსპექტივაში აუცილებელია მეტი კვლევა მსუბუქ კრიპტოგრაფიაზე, AI-ზე დაფუძნებულ ანომალიების აღმოჩენაზე და დეცენტრალიზებულ ავთენტიფიკაციაზე, რათა მოხდეს IoT ინფრასტრუქტურის მასშტაბური და უსაფრთხო ინტეგრაცია სხვადასხვა ინდუსტრიაში.

მომავლის პერსპექტივაში, IoT სისტემები სულ უფრო მეტად გადაიქცევა ინტეგრირებულ პლატფორმებად, სადაც გაერთიანდება ხელოვნური ინტელექტი, ღრუბლოვანი სერვისები, ბლოქჩეინი და 5G კომუნიკაციები. ამ პროცესში ცენტრალური ადგილი უჭირავს უსაფრთხოებას, მდგრად განვითარებასა და მოქნილი სერვისების მიწოდებას. კონკრეტულ სფეროებში, როგორიცაა ინდუსტრიული ავტომატიზაცია, სმარტ ქალაქები და ენერგეტიკა. უკვე ჩანს რეალური შედეგები: უფრო მაღალი ეფექტიანობა, შემცირებული დანაკარგები და ეკოლოგიურად სუფთა გადაწყვეტილებები. სწორედ ასეთი სინთეზური მიდგომები განსაზღვრავს ორგანიზაციების ციფრული ტრანსფორმაციის წარმატებას და ქმნის ბაზას ინოვაციური ეკონომიკისთვის.

გამოყენებული ლიტერატურა:

1. O. Shonia, N.Topuria, K. Kulijanovi, Collect and Analyse Log Data with Cloud Services, მოამბე საქართველოს მეცნიერებათა აკადემია, N3, v15, 2021.
2. ნ. თოფურია, დ. სიჭინავა, თ. ხატიაშვილი, ინფორმაციის უსაფრთხოების დაცვა ორგანიზაციის ციფრული ტრანსფორმაციის დროს, საერთ. სამეცნ.- პრაქტიკული კონფერენცია: „ინოვაციები და თანამედროვე გამოწვევები 2022“ სამეცნიერო შრომათა კრებული, 2022.
3. ნ. თოფურია, ბიზნეს-პროცესების ავტომატიზაცია Sharepoint Server-ის ბაზაზე. მონოგრაფია, სტუ, თბილისი, 2017. ISBN 978-9941-20-912-3.
4. Azure IoT Central documentation, https://docs.microsoft.com/en-us/azure/iot-central
5. What is Azure Sphere?, https://learn.microsoft.com/en-us/azure-sphere/product-overview/what-is-azure-sphere

Contemporary Approaches to Enhancing Security in the IoT Ecosystem

Nino Topuria[1], Demur Sichinava,[2] Ibraim Didmanidze[3]

[1]Georgian Technical University

[2]Ivane Javakhishvili Tbilisi State University

[3]Batumi Shota Rustaveli State University of Batumi

nino.topuria@gtu.ge, demur.sichinava@tsu.ge, ibraimd@mail.ru

Abstract

This article addresses critical security challenges within the Internet of Things (IoT) ecosystem and highlights the capabilities of Microsoft Azure Sphere as a robust platform for safeguarding IoT devices. The study synthesizes contemporary security approaches, including Zero Trust architecture, Cybersecurity Mesh, blockchain-based identity management, and Physically Unclonable Function (PUF) technologies, to enhance both the resilience and scalability of IoT infrastructures. The findings demonstrate that integrating Azure Sphere with Azure IoT Central streamlines device security management while enabling comprehensive data monitoring and real-time operational analytics. Overall, the analysis underscores that the future of IoT security depends on an integrated framework combining artificial intelligence, cloud services, and next-generation authentication mechanisms, thereby providing a holistic strategy for securing complex, large-scale IoT deployments.

Key words: Internet of Things (IoT), cloud computing, IoT security, Azure Sphere, Azure IoT Central.