Subjekto 2FA skaitmeninio autentifikavimo prie kritinės infrastruktūros informacinės sistemos struktūrizuotas vertinimas

Konstantinas Jurgilas

Kauno technologijos universitetas, Informatikos fakultetas,
Studentų g. 50, LT-51368 Kaunas
konstantinas.jurgilas@ktu.edu

Santrauka. Ypatingos svarbos (kitaip – kritinės) infrastruktūros informacinės sistemos apima svarbiausias visuomenės funkcionavimo sritis, reikalingas įvairių paslaugų teikimui. Šioms sistemoms egzistuoja vis didesnė grėsmė tapti skaitmeninių nusikaltimų ir atakų taikiniu, kadangi jos yra kertinės tiek valstybės, tiek visuomenės atžvilgiu. Viena iš svarbiausių priežasčių, sukeliančių grėsmę šių sistemų saugumui, yra silpna nuotolinės prieigos kontrolė – sistemos naudotojo tapatybės valdymas. Šiame straipsnyje pateikiamas pasiūlytas dviejų faktorių (2FA) skaitmeninio autentifikavimo metodas nuotolinei prieigai prie kritinės infrastruktūros informacinės sistemos ir jo struktūrizuotas kokybinių charakteristikų tyrimas bei vertinimas. Tyrimas buvo atliktas dviem etapais: 1) tiriamos metodo charakteristikos panaudojamumo, dislokavimo ir saugumo kategorijose; 2) atliekama lyginamoji tyrimo rezultatų analizė su kitų mokslininkų siūlomais metodais, šiam tikslui panaudojant skaitinį kokybinių charakteristikų vertinimo metodą. Tyrimo rezultatų pagrindu buvo nustatyta, kad siūlomas autentifikavimo metodas yra kokybiškesnis vertintų kategorijų visumos atžvilgiu.

Raktiniai žodžiai: kelių faktorių autentifikacija, kritinės infrastruktūros sistemos.

1 Įvadas

Ypatingos svarbos (kitaip – kritinės) infrastruktūros informacinės sistemos apima svarbiausias visuomenės funkcionavimo sritis, reikalingas įvairių paslaugų teikimui, įtraukiant transporto ir pašto, informacinių technologijų ir elektroninių ryšių, viešojo saugumo, valstybės valdymo, energetikos, užsienio reikalų, saugumo politikos sektorius.

Ypatingos svarbos infrastruktūrų informacinėms sistemoms egzistuoja vis didesnė grėsmė tapti skaitmeninių nusikaltimų ir atakų taikiniu, kadangi jos yra kertinės tiek valstybės, tiek visuomenės atžvilgiu ir palaiko nenu-

DOI: https://doi.org/10.15388/LMITT.2021.3

trūkstamą šių sektorių teikiamų paslaugų vykdymą. Visuomenė yra priklausoma nuo tokių paslaugų teikimo, tad bet koks jų sutrikdymas gali sukelti nepatogumų ar didelių neigiamų padarinių. Pavyzdžiui, 2015 metų gruodį įvykdytas kibernetinis išpuolis prieš Ukrainos elektros tiekimo tinklą, kuomet beveik ketvirtis milijono žmonių vidury žiemos liko be elektros energijos šešioms valandoms [1].

Viena iš svarbiausių priežasčių, sukeliančių grėsmę kritinės infrastruktūros informacinių sistemų saugumui, yra silpna nuotolinės prieigos kontrolė – sistemos naudotojo tapatybės valdymas. Autentifikacijos procesas yra vienas iš esminių komponentų subjekto (sistemos naudotojo) tapatybės valdyme, kadangi šio proceso metu yra vienareikšmiškai nustatomas sistemos naudotojo identitetas. Jei autentifikacijos procesas yra įvykdomas sėkmingai, sistema pasitiki proceso metu gautu rezultatu ir identifikuoja sistemos naudotoją tik pagal proceso metu gautą informaciją - autentifikacijos kontekstą. Jei autentifikacijos procesas bus pažeistas, egzistuoja itin didelė rizika, jog sistema neteisingai identifikuos bei autentifikuos jos naudotojus. Svarbu pabrėžti, kad esamuose subjekto skaitmeninio autentifikavimo metoduose [2] [3] yra naudojami to pačio tipo informacijos pateikimo kanalai (pvz.: tik naudotojo kompiuteris), ko pasekoje didėja rizika, jog kanalo pažeidimo (kibernetinio incidento) metu bus pažeistas visas autentifikacijos procesas. Kelių tipų kanalų panaudojimas (pvz.: naudotojo kompiuteris ir mobilusis įrenginys ar fizinis skaitmeninių žetonų generatorius) užtikrintų didesnį saugos lygį, kadangi pažeidus tik vieną iš kanalų, kitas kanalas užtikrintų autentifikacijos proceso apsaugą nuo pažeidimo. Dalyje esamų sprendimų siūlomas SMS žinučių metodas [4] [5] taip pat nebėra laikomas saugiu, o sistemos naudotojo lokacijos bei biometrinių duomenų panaudojimo realizavimas metoduose [6] [7] gana sudėtingai realizuojamas ir taikomas. Mobilaus ryšio įrenginių, kaip antro tipo informacijos kanalo, panaudojimas yra tinkama priemonė skaitmeninės autentifikacijos procese [8], tačiau toks autentifikacijos procesas turi būti praplėstas privalomu subjekto autentifikacijos užklausos patvirtinimu keliais etapais, pvz.: įtraukiant institucijos skirtingų pavaldumo lygmenų vadovus.

Esamų autentifikacijos metodų problematikos analizės pagrindu buvo nustatyta, kad kritinės infrastruktūros informacinių sistemų saugiam nuotoliniam prieigos valdymui turi būti užtikrinti esminiai saugos reikalavimai: 1) nuotolinių naudotojų autentifikacijai turi būti naudojamas stiprus kelių

faktorių autentifikacijos metodas, kuris remiasi keliais kanalais (angl. „*out-of-band authentication*“); 2) turi būti nustatyta procedūra, kuri leistų aukštesnio rango darbuotojui patvirtinti nuotolinės prieigos prašymą, siekiant išvengti neautorizuotų asmenų nuotolinės prieigos prie kritinės infrastruktūros sistemų; 3) nuotolinė prieiga bei autentifikacijos procesas turi vykti naudojant saugų kanalą (HTTPS protokolą bei VPN tunelius).

Atsižvelgiant į tai, suformuotas ir šio tyrimo tikslas - pasiūlyti dviejų faktorių (2FA) skaitmeninio autentifikavimo metodą nuotolinei prieigai prie kritinės infrastruktūros informacinės sistemos ir struktūriškai įvertinti jo kokybines charakteristikas. Tikslo įvykdymui yra keliami šie uždaviniai:

1. suprojektuoti dviejų faktorių skaitmeninio autentifikavimo metodą, kuris tenkintų kritinės infrastruktūros informacinėms sistemoms keliamus saugos reikalavimus ir realizuoti jį sistemos prototipe;
2. atlikti eksperimentinį pasiūlyto metodo veikimo tyrimą, įvertinant metodo kokybines charakteristikas.

Pasiūlyto metodo mokslinis naujumas ir praktiškumas – skaitmeninis autentifikacijos metodas, pagrįstas „*push notification*“ technologijos, skaitmeninių sertifikatų bei autentifikacijos užklausų autorizavimo sinergija, skirta valdyti nuotolinę prieigą prie kritinės infrastruktūros informacinės sistemos.

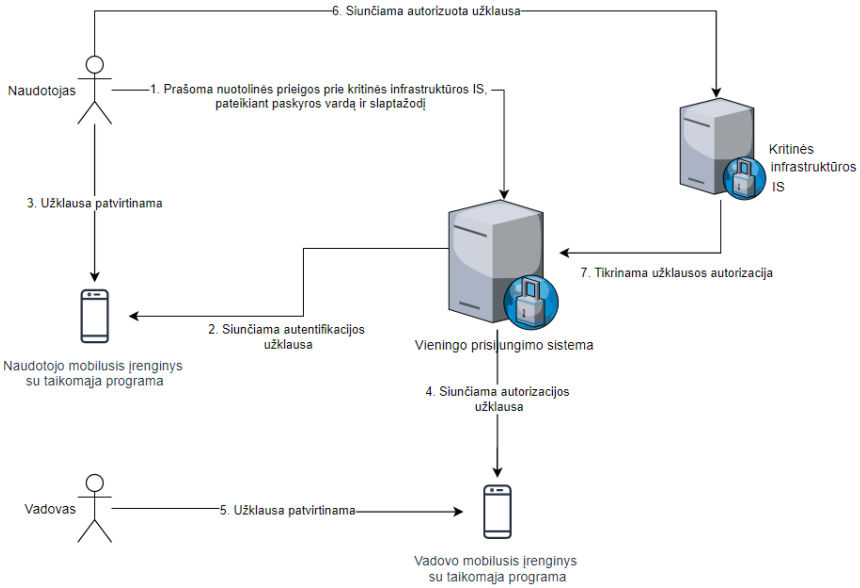
2 2FA skaitmeninis autentifikavimo metodas

Siūlomo autentifikavimo metodo koncepcinis modelis, pateiktas 1 paveikslėlyje, remiasi trijų žingsnių autentifikacijos/autorizacijos procesu.

Naudotojas, norėdamas gauti nuotolinę prieigą prie kritinės infrastruktūros informacinės sistemos, turėtų sėkmingai įvykdyti tokį procesą:

1. pateikti paskyros identifikatorių ir su juo susietą slaptažodį, kurį naudotojas gauna iš administratoriaus, kuomet šis sukuria paskyrą. Jei duomenys yra teisingi - naudotojui į jo susietą mobilaus ryšio įrenginį bus nusiunčiama autentifikacijos užklausa;
2. kuomet pats naudotojas sėkmingai patvirtina atsiųstą jam autentifikacijos užklausą, jo vadovams yra nusiunčiama autorizacijos užklausa, kurioje yra klausiama, ar pavaldiniui yra leidžiama jungtis prie tam tikros sistemos ir yra suteikiama nuotolinė prieiga;
3. jeigu vienas iš nurodytų vadovų sėkmingai patvirtina autorizacijos užklausą, naudotojui yra suteikiama nuotolinė prieiga prie apsaugo-

tos sistemos. Čia svarbu pabrėžti, kad sistema turi suteikti galimybę nurodyti kelis galimus vadovus sistemos naudotojo autorizavimui, siekiant padidinti pertekliškumą tais atvejais, kai vieno iš vadovų mobilusis įrenginys nėra pasiekiamas.



1 pav. Autentifikavimo metodo koncepcinis modelis

Realizavus tokį subjekto skaitmeninės autentifikacijos procesą, būtų užtikrinama, jog nuotolinė prieiga prie kritinės infrastruktūros informacinės sistemos yra valdoma taikant saugumo priemones, kurios yra pateikiamos tokio tipo sistemų saugos reikalavimų dokumentuose.

3 Tyrimo metodika

Siekiant nustatyti siūlomo autentifikavimo metodo kokybines charakteristikas, jis buvo tiriamas ir vertinamas pagal [9] literatūros šaltinyje siūlomą autentifikavimo schemų vertinimo metodiką. Metodikoje yra pristatomos 25 autentikavimo metodų charakteristikos, kuriomis yra įvertinami metodų

privalumai ir trūkumai. Šaltinyje nurodoma, jog metodų saugumo ir panaudojamumo savybės būna sunkiai suderinamos – suteikiant vieną savybę, yra sudėtinga pritaikyti kitą. Autoriai pabrėžia ir dislokavimo savybę, nurodančią, ar metodas gali būti pritaikytas praktiškai.

Atsižvelgus į išskirtas savybių grupes, siūlomo metodo charakteristikos buvo suskirstytos į tris kategorijas: panaudojamumas (angl. „*usability*“), dislokavimas (angl. „*deployment*“) ir saugumas (angl. „*security*“). Šioms kategorijoms priskiriamų charakteristikų tyrimas ir vertinimas atliktas panaudojant skaitinį kokybinių charakteristikų vertinimo metodą:

- Už „+“ įvertinimą skiriamas 1 balas;
- Už „–“ įvertinimą skiriama 0 balų;
- Už „±“ įvertinimą skiriama 0,5 balo.

Taip pat atsižvelgus į tai, kad pasiūlytą metodą siekiama taikyti aukšto saugos lygio reikalaujančioje kritinės infrastruktūros aplinkoje, metodo saugumo kategorijos charakteristikos turi būti svarbesnės nei kitų dviejų –- panaudojamumo ar dislokavimo, tad saugumo charakteristikų įverčių sumai yra suteikiamas didesnis koeficientas. Taikant šį vertinimą, maksimalus galimas metodo vertinimas – 30.5 balo. Bendra balų suma apskaičiuojama pagal 1 formulę:

$$Bendras\ balas = \sum_{i}^{8} U_i + \sum_{j}^{6} D_j + 1{,}5 \cdot \sum_{j}^{11} S_k \qquad (1)$$

čia: U_i – panaudojamumo kategorijos *i*-tosios charakteristikos įvertis; D_j – dislokavimo kategorijos *j*-tosios charakteristikos įvertis; S_k – saugumo kategorijos *k*-tosios charakteristikos įvertis.

4 Struktūrizuoto vertinimo eiga

Metodo charakteristikų skirtingose kategorijose apibūdinimai ir jų realizavimo poveikis siūlomo metodo veikimui ir funkcionalumui yra pateikiami 1, 2 ir 3 lentelėse. Panaudojamumo kategorijoje vertintos 8 metodo charakteristikos, dislokavimo – 6 charakteristikos, o didžiausias kiekis vertinamų charakteristikų buvo saugumo kategorijoje – 11 charakteristikų.

1 lentelė. Panaudojamumo charakteristikų vertinimo analizės rezultatai

Nr.	Charakteristika ir jos apibūdinimas	Charakteristikos įgyvendinimas siūlomame metode
U1	Nereikalaujantis atminties pastangų (angl. „*Memory-wise-Effortless*“)	Naudotojai turi prisiminti tik paskyros slaptažodį.
U2	Plečiamas tarp paskyrų (angl. „*Scalable-for-Users*“)	Metodas yra realizuotas vieningo prisijungimo sistemoje, tad naudotojas vieną paskyrą naudoja prisijungimui prie skirtingų sistemų.
U3	Nereikalaujantis papildomų nešulių (angl. “*Nothing-to-Carry*“)	Naudotojas su savimi turi turėti savo mobiliojo ryšio įrenginį, kurį dažniausiai visada nešiojasi su savimi.
U4	Nereikalaujantis fizinių pastangų (angl. „*Physically-Effortless*“)	Naudotojas autentifikavimo proceso metu turi įvesti slaptažodį, paspausti kelis mygtukus ir pateikti PIN kodą ar piršto antspaudą, jei yra sukonfigūruotas užklausos patvirtinimas.
U5	Lengvai išmokstamas (angl. „*Easy-to-Learn*“)	Vykdant autentifikacijos procesą, naudotojui yra pateikiamos išsamios instrukcijos ir paaiškinimai, kokius veiksmus jis turi atlikti, norint sėkmingai užbaigti visą procesą.
U6	Efektyviai naudojamas (angl. „*Efficient-to-Use*“)	Autentifikacijos procesas gali užtrukti, kadangi vadovas turi sureaguoti ir autorizuoti užklausą. Mobiliojo įrenginio susiejimo procesas yra pakankamai greitas.
U7	Retai klaidingas (angl. „*Infrequent-Errors*“)	Autentifikavimo schema nėra sudėtinga ir turėtų visada suveikti kuomet ją vykdo teisėtas naudotojas. Kuomet užklausa yra patvirtinama panaudojant biometrinius piršto antspaudo duomenis, yra naudojami gamykliniai mobiliųjų įrenginių mechanizmai, tad schemos patikimumas priklauso ir nuo šių technologijų patikimumo.
U8	Lengvai kompensuojamas įvykus nelaimei (angl. „*Easy-Recovery-from-Loss*“)	Sukūrus paskyrą, naudotojui yra perduodami keli vienkartiniai slaptažodžiai, su kuriais jis nelaimės atveju gali prisijungti prie paskyrų valdymo sistemos. Prisijungus prie šios sistemos, galima pasikeisti slaptažodį ar pakeisti įrenginį, su kuriuo paskyra yra susieta.

2 lentelė. Dislokavimo charakteristikų vertinimo lentelė

Nr.	Charakteristika ir jos apibūdinimas	Charakteristikos įgyvendinimas siūlomame metode
D1	Prieinamumas (angl. „*Accessibility*“)	Autentifikacijos schema remiasi WEB naršyklės ir mobiliojo ryšio įrenginio teikiamomis standartinėmis prieinamumo priemonėmis.
D2	Nežymi kaina už kiekvieną naudotoją (angl. „*Negligible-Cost-per-User*“)	Metodui realizuoti nėra reikalinga papildoma techninė įranga – yra naudojami naudotojų mobilieji įrenginiai.
D3	Suderinamas su serveriu (angl. „*Server-Compatible*“)	Metodas yra realizuotas vieningo prisijungimo sistemoje, taikančioje standartizuotą *OAuth 2.0* protokolą, kuris yra suderinamas su įvairiais paslaugų tiekėjais.
D4	Suderinamas su naršykle (angl. „*Browser-Compatible*“)	Sistemos prototipas teisingai veikia naudojant *Google Chrome* naršyklę su N-2 versijomis. Naudotojai taip pat papildomai turi įsidiegti mobiliojo ryšio įrenginio taikomąją aplikaciją.
D5	Brandus (angl. „*Mature*“)	Metodas yra dar tik siūlomas.
D6	Neapsaugotas patento (angl. „*Non-Proprietary*“)	Metodas yra pateikiamas mokslinamе darbe ir nėra patentuotas.

3 lentelė. Saugumo charakteristikų vertinimo analizės rezultatai

Nr.	Charakteristika ir jos apibūdinimas	Charakteristikos įgyvendinimas siūlomame metode
S1	Atsparus fiziniam stebėjimui (angl. „*Resilient-to-Physical-Observation*“)	Metodas yra atsparus fiziniam stebėjimui, kadangi norint atlikti autentifikacijos procesą, reikia turėti fizinį mobiliojo ryšio įrenginį ir pateikti piršto antspaudą, kuomet yra sukonfigūruotas užklausos patvirtinimas pateikiant šią biometrinę informaciją.
S2	Atsparus nutaikytam apsimetinėjimui (angl. „*Resilient-to-Targeted-Impersonation*“)	Metodas yra atsparus nutaikytam apsimetinėjimui, kadangi nėra naudojama asmeninė naudotojo informacija.
S3	Atsparus apribotam spėliojimui (angl. „*Resilient-to-Throttled-Guessing*“)	Metodas yra atsparus apribotam spėliojimui, kadangi neteisingą slaptažodį pateikus 3 kartus, paskyra yra užblokuojama.
S4	Atsparus neapribotam spėliojimui (angl. „*Resilient-to-Unthrottled-Guessing*“)	Metodas yra atsparus neapribotam spėliojimui, kadangi neteisingą slaptažodį pateikus 3 kartus, paskyra yra užblokuojama.

Nr.	Charakteristika ir jos apibūdinimas	Charakteristikos įgyvendinimas siūlomame metode
S5	Atsparus vidiniam stebėjimui (angl. „*Resilient-to-Internal-Observation*“) Piktavalis negali apsimesti naudotoju perimdamas įvestį iš naudojamų įrenginių arba perimant tinklo srautą.	Metodas yra atsparus pakartojimo atakoms, kadangi vykdant autentifikacijos procesą yra tikrinama, kad proceso žingsniai būtų atliekami tik vieną kartą. Metodas gali būti pažeistas, jei žalinga programine įranga bus paveikta naudotojo naršyklė, naudotojo ir vadovo mobiliojo ryšio įrenginiai.
S6	Atsparus informacijos nutekėjimui iš tikrintojo (angl. „*Resilient-to-Leaks-from-Other-Verifiers*“) Metodas užtikrina, jog informacijai nutekėjus iš tikrintojo, piktavaliai negalės pasinaudoti šia informacija apsimetant naudotoju.	Vieningo prisijungimo sistema (tikrintojas) naudotojų slaptažodžius saugo naudodama stiprų *bcrypt* slaptažodžių santraukos algoritmą. Vieningo prisijungimo sistema taip pat saugo tik viešąjį naudotojo kriptografinį raktą, kuris yra skirtas patvirtinti užklausų patvirtinimo parašus, tad šio rakto kompromitacija nepaveiktų metodo saugos.
S7	Atsparus apgaulės atakoms (angl. „*Resilient-to-Phishing*“)	Piktavalis apgaulės metodu galėtų perimti tik naudotojo slaptažodį, tačiau negalėtų paveikti užklausų patvirtinimo naudojant mobiliojo ryšio įrenginį.
S8	Atsparus vagystei (angl. „*Resilient-to-Theft“)* Kuomet metodas naudoja fizinį įrenginį autentifikacijos atlikimui, piktavalio perimtas įrenginys negali būti panaudotas autentifikacijos vykdymui.	Kuomet užklausų patvirtinimui yra sukonfigūruotas piršto antspaudo panaudojimas, pavogto įrenginio panaudojimas tampa labai komplikuotas. Taip pat svarbu paminėti, jog perėmus ir panaudojus tik naudotojo įrenginį, metodui apsaugą suteikia vadovo įrenginio panaudojimas autorizacijos patvirtinimui.
S9	Nenaudojantis patikimos trečios šalies (angl. „*No-Trusted-Third-Party*“)	Metodą realizuojanti vieningo prisijungimo sistema remiasi trečiosios šalies *Google Firebase* paslauga.
S10	Reikalaujantis tiesioginio patvirtinimo (angl. „*Requiring-Explicit-Consent*“)	Naudotojas turi tiesiogiai pareikšti prašymą autentifikuotis, pateikiant pradinę prisijungimo vardo ir slaptažodžio formą.
S11	Neatsiejamas (angl. „*Unlinkable*“)	*JWT* žetone yra nurodomas vieningo prisijungimo sistemos naudotojui suteiktas unikalus identifikatorius.

5 Rezultatų analizė

4 lentelėje yra pateikiama lyginamoji pasiūlyto metodo struktūrizuoto vertinimo rezultatų analizė su kitų mokslininkų siūlomais metodais. (Pastaba: lentelės stulpelyje „Nr.“ pateikiami tirti kitų mokslininkų pasiūlyti metodai [3-12], o šiame darbe siūlomas metodas atitinka Nr. 13.).

4 lentelė. Autentifikavimo metodų kokybinių charakteristikų vertinimo rezultatai

Nr.	Charakteristikų realizavimas kategorijose																								Įvertis
	Panaudojamumas (U)								Dislokavimas (D)						Saugumas (S)										
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	1	2	3	4	5	6	7	8	9	10	11	
[3]	0	1	1	0	1	1	1	0	1	1	0	1	1	1	0	1	1	0	0	0	0	1	1	1	1	19
[5]	0	1	.5	0	1	.5	1	0	1	1	0	1	1	1	1	1	1	1	.5	0	0	1	0	1	1	20.25
[6]	1	1	1	0	1	1	.5	0	1	1	0	.5	0	1	1	.5	1	1	0	1	1	1	1	1	1	23.25
[7]	0	0	1	0	1	0	0	0	1	1	0	.5	0	1	1	.5	1	1	.5	1	1	1	0	1	1	19
[8]	1	1	.5	0	1	.5	.5	0	1	1	0	.5	1	1	1	1	1	1	.5	1	1	1	0	1	1	23.25
[10]	0	1	.5	0	1	.5	1	0	0	1	0	.5	0	1	1	1	1	1	.5	0	1	0	1	1	1	19.25
[11]	1	1	.5	0	1	1	1	0	1	1	0	.5	0	1	1	1	1	1	0	1	1	.5	1	1	1	23.25
[12]	0	1	.5	0	1	.5	1	0	0	1	.5	.5	0	1	0	1	1	1	.5	1	1	1	0	1	1	19.75
13	**1**	**1**	**.5**	**0**	**1**	**0**	**.5**	**1**	**1**	**1**	**.5**	**.5**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**24**

Lyginamosios pasiūlyto metodo struktūrizuoto vertinimo rezultatų analizės pagrindu nustatyta, kad siūlomas metodas vertinamas 0 balų už U6 charakteristiką (Efektyviai naudojamas), tačiau, lyginant su kitais metodais, yra pranašesnis dėl S5 charakteristikos (Atsparus vidiniam stebėjimui). Taip yra todėl, kad pažeisti visus 3 įrenginius, naudojamus siūlomame skaitmeninės autentifikacijos procese, yra sunku ir reikalauja daug pastangų. Siūlomas autentifikacijos metodas panaudojamumo kategorijoje vertinamas 5 balais, o tai yra tik nežymiai mažesnis vertinimas (-0,5 balo), nei kitų metodų. Dislokavimo kategorijos charakteristikų realizavimas metode vertinamas net 4 balais iš maksimaliai galimų 5. Tačiau svarbiausia, kad saugumo kategorijoje siūlomo metodo charakteristikos vertinamos aukščiausiai (15 balų), lyginant su kitais tirtais metodais. To pasekoje darytina išvada, kad pasiūlytas skaitmeninis autentifikacijos metodas yra kokybiškesnis, lyginant su kitais tirtais metodais, ir gali būti naudojamas nuotolinei prieigai prie kritinės infrastruktūros informacinės sistemos.

6 Išvados

Pasiūlytas subjekto skaitmeninis autentifikacijos metodas, pagrįstas „*push notification*“ technologijos, skaitmeninių sertifikatų bei autentifikacijos užklausų autorizavimo sinergija, skirta valdyti nuotolinę prieigą prie kritinės infrastruktūros informacinės sistemos. Struktūrizuoto metodo kokybinių charakteristikų panaudojamumo, dislokavimo ir saugumo kategorijose tyrimo ir atliktos lyginamosios rezultatų analizės pagrindu nustatyta, kad siūlomas autentifikavimo metodas vertinamas 24 balais iš maksimaliai galimų 30,5 ir yra kokybiškesnis, lyginant su kitais tirtais metodais, kategorijų visumos atžvilgiu.

Literatūra

[1] “Cyber attacks targeting critical infrastructure | IEC e-tech | Issue’ 02/2019,” IEC e-tech. https://www.iecetech.org/index.php/Technology-Focus/2019-02/Cyber-attacks-targeting-critical-infrastructure (accessed Oct. 26, 2019).

[2] S. Vaithyasubramanian, A. Christy, and D. Saravanan, “TWO FACTOR AUTHENTICATIONS FOR SECURED LOGIN IN SUPPORT OF EFFECTIVE INFORMATION PRESERVATION AND NETWORK SECURITY,” vol. 10, no. 5, p. 5, 2015.

[3] “Internet Banking Login with Multi-Factor Authentication,” KSII Trans. Internet Inf. Syst., vol. 11, no. 1, Jan. 2016, doi: 10.3837/tiis.2017.01.027.

[4] "(PDF) Multi-factor Authentication as a Service for Cloud Data Security," ResearchGate. https://www.researchgate.net/publication/313647475_Multi-factor_Authentication_as_a_Service_for_Cloud_Data_Security (accessed Oct. 26, 2019).
[5] K. W. Hussein, "Design and Implementation of Multi Factor Mechanism for Secure Authentication System," vol. 11, no. 7, p. 7, 2013.
[6] N. A. Aldumiji and E. A. Khan, "Fingerprint and location based multifactor authentication for mobile applications," Int. J. Eng., p. 13.
[7] I. A. Lami, T. Kuseler, H. Al-Assam, and S. Jassim, "LocBiometrics: Mobile phone based multi- factor biometric authentication with time and location assurance," p. 4.
[8] B. Maciej, E. F. Imed, and M. Kurkowski, "Multifactor Authentication Protocol in a Mobile Environment," IEEE Access, vol. 7, pp. 157185–157199, 2019, doi: 10.1109/ACCESS.2019.2948922.
[9] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, May 2012, pp. 553–567, doi: 10.1109/SP.2012.44.
[10] A. Abdellaoui, Y. I. Khamlichi, and H. Chaoui, "A Novel Strong Password Generator for Improving Cloud Authentication," Procedia Comput. Sci., vol. 85, pp. 293–300, Jan. 2016, doi: 10.1016/j.procs.2016.05.236.
[11] X. Fang and J. Zhan, "Online Banking Authentication Using Mobile Phones," in *2010 5th International Conference on Future Information Technology*, Busan, Korea (South), 2010, pp. 1–5, doi: 10.1109/FUTURETECH.2010.5482634.
[12] M. Misbahuddin, R. Vs, A. Thomas, and U. Kumar, "A Unique-ID based Usable Multi-Factor Authentication Scheme for e-Services," p. 7.