(19) Lietuvos Respublikos valstybinis patentų biuras

(10) **LT 6793 B**

(12) **PATENTO APRAŠYMAS**

(11) Patento numeris: **6793**

(51) Int. Cl. (2020.01): **G06N 3/00**

(21) Paraiškos numeris: **2020 525**

(22) Paraiškos padavimo data: **2020-05-18**

(41) Paraiškos paskelbimo data: **2020-11-25**

(45) Patento paskelbimo data: **2020-12-28**

(62) Paraiškos, iš kurios dokumentas išskirtas, numeris: —

(86) Tarptautinės paraiškos numeris: —

(86) Tarptautinės paraiškos padavimo data: —

(85) Nacionalinio PCT lygio procedūros pradžios data: —

(30) Prioritetas: —

(72) Išradėjas:

**Timofey MOCHALOV, RU**

(73) Patento savininkas:

**Timofey MOCHALOV, Kirova 18a-47, Sosensky, Kaluga, RU**

(74) Patentinis patikėtinis/atstovas:

**Aušra PAKĖNIENĖ, AAA Law, A. Goštauto g. 40B, Verslo centras „Dvyniai", LT-03163 Vilnius, LT**

LT 6793 B

(54) Pavadinimas:

# Duomenų perdavimo apsaugos būdas naudojant dirbtinį neuroninį tinklą

(57) Referatas:

Duomenų šifravimo ir dešifravimo per tinklą, naudojant dirbtinį neuroninį tinklą, įdiegtą kiekviename tinklo mazge, būdas. Duomenų apsaugos elementai - šifravimo raktai, šifravimo algoritmai ir šifravimo painiava - generuojami arba pasirenkami, atitinkamai pradedant naują ryšio seansą tinkle ir per tinklą neperduodami jokie duomenų apsaugos elementai. Dirbtinis neuroninis tinklas mokomas, naudojant blokinę grandinę ir pridedant prie blokinės grandinės kiekvieną naują bloką bei naudojamas šifravimo raktų baigtinei aibei vienu metu generuoti kiekviename mazge. Tokie elementai - šifravimo raktai, šifravimo algoritmai ir šifravimo painiava - susiejami su neuroniniu tinku kiekviename mazge ir po to naudojami perduotiems duomenims dešifruoti.

IŠRADIMO SRITIS

Šis išradimas susijęs su kriptografijos būdu, tiksliau – su kompiuterinio duomenų šifravimo ir dešifravimo, naudojant dirbtinį neuroninį tinklą bei duomenų struktūros apsaugos blokinę grandinę, būdu.

TECHNIKOS LYGIS

Duomenų saugumas yra svarbiausias dalykas duomenų perdavimo sistemose. Neuroninė kriptografija – tai duomenų šifravimo ir dešifravimo, naudojant dirbtinį neuroninį tinklą, būdas. Dirbtiniai neuroniniai tinklai (toliau – ANN) yra gerai žinomi dėl savo gebėjimo selektyviai ištirti tam tikros problemos sprendimų erdvę. Ši ypatybė turi natūralią taikymo nišą kriptoanalizės srityje. Tuo pat metu neuroniniai tinklai teikia naują požiūrį į atakas prieš šifravimo algoritmus. Tai pagrįsta principu, kad bet kuri funkcija gali būti atkuriama, naudojant neuroninį tinklą – galingą ir išbandytą skaičiavimo priemonę, kuri gali būti naudojama bet kurio šifravimo algoritmo atvirkštinei funkcijai rasti. Neuroninė kriptografija paprastai grindžiama viešojo ir privačiojo raktų poros sukūrimu, naudojant neuroninius tinklus; naudojant blokinę grandinę maišos pavidalo šifravimo raktams saugoti arba naudojant blokinę grandinę ANN elementams saugoti. Paprastai neuroninė kriptografija naudojama duomenų mainų tarp dviejų neuroninių tinklų problemai spręsti, taikant abipusio mokymosi koncepciją. Du tinklai keičiasi savo išvestimis (bitais) ir raktas tarp dviejų ryšį palaikančių šalių galiausiai atspindimas galutiniuose išmoktuosiuose rodikliuose, t.y. kai tariama, kad du tinklai yra sinchronizuoti. Neuroninės sinchronizacijos saugumui kyla pavojus tada, kai puolantysis geba sinchronizuotis su bet kokiomis dviem šalimis apmokymo metu.

Kriptografijos, naudojant dirbtinį neuroninį tinklą, būdas yra atskleistas mokslinėje publiakcijoje Apdullah Yayık ir Yakup Kutlu: „Neural Network Based Cryptography“, 2014 gegužės mėn., Neural Network World, pp. 177–192, DOI: 10.14311/NNW.2014.24.011. Būdas apima du etapus. Pirmojo etapo metu generuojami neuroninio tinklo pseudoatsitiktiniai skaičiai (NPRNG). Jų atsitiktinumas yra tikrinamas, naudojant Nacionalinio standartų ir technologijų instituto (NIST) atsitiktinumo testus. Antrojo etapo metu sukuriama neuroninio tinklo šifravimo sistema, naudojant NPRNG. Šioje šifravimo sistemoje duomenis, kurie užšifruoti naudojant netiesinius būdus, mėginama iššifruoti naudojant du identiškus dirbtinius

neuroninius tinklus. Pirmajame neuroniniame tinkle modeliuojamas netiesinis šifravimas, naudojant ryšių kūrimo funkciją. Antrajame neuroniniame tinkle užšifruoti duomenys dešifruojami, naudojant sprendimų priėmimo funkciją.

Blokinės grandinės naudojimo kartu su dirbtiniu neuroniniu tinklu būdas aprašytas straipsnyje Konstantinos Sgantzos ir Ian Grigg: „Artificial Intelligence Implementations on the Blockchain. Use Cases and Future Applications“, Future Internet 2019, 11, 170; doi:10.3390/fi11080170.

Pagrindiniai ankstesnio išradimo trūkumai yra tai, kad neuroniniai tinklai naudojami šifravimo raktui ar asimetrinių šifravimo raktų porai sukurti arba šifravimo raktams saugoti blokinėje grandinėje vienu ar kitu pavidalu.

Šis išradimas skirtas ankstesnio išradimo trūkumams pašalinti ir kitiems privalumams, lyginant su ankstesniu išradimu, sukurti.

TRUMPAS IŠRADIMO APRAŠYMAS

Atskleidžiamas duomenų šifravimo ir dešifravimo būdas per tinklą, naudojant dirbtinį neuroninį tinklą, įdiegtą kiekviename tinklo mazge. Duomenų apsaugos elementai (šifravimo raktai, šifravimo algoritmai ir šifravimo painiava) generuojami arba pasirenkami atitinkamai pradedant naują ryšio seansą tinkle. Per tinklą neperduodami jokie duomenų apsaugos elementai. Dirbtinis neuroninis tinklas yra apmokomas blokinėje grandinėje, pridedant prie blokinės grandinės kiekvieną naują bloką, bei naudojamas šifravimo raktų baigtinei aibei generuoti, vienu metu kiekviename mazge. Tokie elementai (šifravimo raktai, šifravimo algoritmai ir šifravimo painiava) yra susiejami su neuroniniu tinku kiekviename mazge ir vėliau naudojami perduotiems duomenims dešifruoti.

TRUMPAS BRĖŽINIŲ APRAŠYMAS

Išradimo požymiai, kurie yra nauji ir neakivaizdūs, yra išsamiai išdėstyti apibrėžtyje. Nepaisant to, patį išradimą galima geriau suprasti pasinaudojant nuorodomis į toliau pateiktą išsamų išradimo aprašymą, kuriame aprašyti išradimo įgyvendinimo pavyzdžiai, naudojant neapibrėžtinius išradimo įgyvendinimo pavyzdžius kartu su pridėtais brėžiniais, kur:

1 paveiksle yra pavaizduota pirminio tinklo kliento atpažinimo schema. Serveris išsiuntinėja kliento identifikatorius ir asmenines paslaptis (asmeninių

duomenų rinkinius arba šifro blokus) kiekvienam klientui.

2 paveiksle yra pavaizduota perduodamų duomenų šifravimo schema, šifravimo algoritmo parinkimas ir kiekvieno duomenų perdavimo seanso šifravimo raktas.

3 paveiksle yra pavaizduotas neuroninių tinklų sinchronizavimo ir apmokymo iš naujo principas šifravimo algoritmų pasirinkimo loginei schemai (mokymo duomenų iš blokinių grandinių tinklo pasirinkimui) keisti bei naujo šifravimo raktų kūrimo būdo pasirinkimas.

Geriausių išradimo įgyvendinimo variantų aprašymas pateiktas po nuorodų į brėžinius.

IŠSAMUS IŠRADIMO APRAŠYMAS

Turėtų būti suprantama, kad daugybė aprašytų specifinių smulkmenų yra pateikta siekiant pateikti išbaigtą ir išsamų išradimo įgyvendinimo aprašymą. Nepaisant to, šios srities specialistas supras, kad išradimo naudojimo sritis, kurioje jis gali būti įgyvendintas be šių išsamių nurodymų, neapsiriboja pateiktais įgyvendinimo pavyzdžiais. Gerai žinomi būdai, procedūros ir komponentai nėra išsamiai aprašyti, kad įgyvendinimo aprašymas nebūtų klaidinantis. Be to, aprašymas neturi būti traktuojamas kaip apribojantis išradimą pateiktais įgyvendinimo pavyzdžiais, jie atspindi tik kelis galimus išradimo įgyvendinimo būdus.

Nors šis išradimo aprašymas apima daug charakteristikų ir pranašumų bei konstrukcinių elementų ir ypatybių, jis yra pateiktas kaip išradimo realizavimo pavyzdys. Nenukrypstant nuo išradimo esmės, galimi daliniai pakeitimai, ypač susiję su forma, dydžiu bei schema, pagal plačiausiai suprantamą apibrėžtyje pateiktų sąvokų ir apibrėžimų traktuotę.

Trumpas sąvokų paaiškinimas

Duomenys – tai grynasis tekstas ir kita netrumpalaikė kompiuteryje saugoma medija.

Klientai – tai kompiuteriniai įrenginiai, tokie kaip belaidžiai įrenginiai, kompiuterių procesoriai, jutikliai ir kiti įrenginiai, gebantys apdoroti duomenis.

Mazgai – tai klientai, serveriai.

Siuntėjas ir gavėjas – kiekvieno duomenų perdavimo seanso metu vienas kliento mazgas siunčia duomenis ir yra siuntėjas, ir bent vienas kliento mazgas gauna duomenis ir yra gavėjas.

Kliento identifikatorius – tai unikalus 256–512 bitų raktas, X509 sertifikatas arba jie abu.

Duomenų perdavimo seansas – tai laikotarpis, kurio metu vienas kliento mazgas yra siuntėjas ir bent vienas kliento mazgas yra gavėjas bei visi mazgai turi sinchronizuotus atpažinimo raktus.

Dirbtinis neuroninis tinklas (ANN) – tai informacijos apdorojimo ir modeliavimo sistema, kuri imituoja biologinių sistemų gebėjimą mokytis suprasti nežinomus procesus arba jų dinamiką. Dirbtinis neuroninis tinklas yra tinklas, apimantis daug labai paprastų procesorių, kiekvienas iš kurių gali turėti (nedidelę) vietinę atmintį. Procesoriai yra sujungti vienakrypčiais ryšio kanalais, kuriais perduodami skaitiniai duomenys. Procesoriai operuoja tik savo vietiniais duomenimis ir įvestimis, kurias jie gauna per jungtis.

Blokinė grandinė – tai pilnutinai bendrinamas registras, kuris globaliai matomas visoms šalims, kai jame registruojama operacija, be jokios autoritetingos centrinės valdžios dalyvavimo.

Simetrinis šifravimas – tai šifravimas simetriniu raktu, kur slaptasis raktas yra bendras siuntėjo ir gavėjo klientams. Žodis „simetrinis“ reiškia, kad tiek siuntėjas, tiek gavėjas naudoja tą patį raktą informacijai šifruoti ir dešifruoti.

Asimetrinis šifravimas – tai neuroninio šifravimo ir dešifravimo būdas, apimantis neuroninių tinklų naudojimą kartu su simetrinio šifravimo algoritmais kompiuterių tinkle. Kompiuterių tinklas, pageidautina, yra blokinės grandinės tipo kompiuterių tinklas.

Šifravimo painiavos būdai – kai grynasis tekstas šifruojamas, naudojant vieną šifravimo algoritmą bei simetrinį šifravimo raktą ir kai po to jis šifruojamas, naudojant kitą šifravimo algoritmą bei simetrinį šifravimo raktą, atsitiktine tvarka pridedant atsitiktines „šiukšles“ (nešifruotus simbolius arba atsitiktinius bitus) prie grynojo teksto prieš šifruojant, pridedant „šiukšles“ (atsitiktinius bitų rinkinius skirtingose vietose) prie jau užšifruotų duomenų arba atskirų blokų, paslenkant užšifruotą tekstą per tam tikrą vektorių ir pan.

Pagal vieną išradimo įgyvendinimo pavyzdį, yra atskleidžiamas kompiuteriu įgyvendinamas neuroninės kriptografijos būdas, skirtas apsaugoti per tinklą perduodamiems duomenims, naudojant sinchronizuotas ANN kopijas kiekviename mazge. Tokiu būdu yra eliminuojamas duomenų apsaugos parametrų perdavimas per tinklą. Tinklas – tai internetinis arba vietinis kompiuterių tinklas, apimantis bent du kliento mazgus, skirtus duomenų siuntimui bei gavimui ir bent vieną serverio mazgą. Kiekviename mazge saugoma ANN kopija.

Serveris siunčia kliento identifikatorius kliento mazgams pačioje darbo, kuriuo suformuojamas tinklas, pradžioje. 1 paveiksle yra pavaizduota ši tinklo identifikacijos schema, skirta pradėti duomenų perdavimo seansą.

Tinklo viduje, ANN yra sinchronizuojami kiekviename mazge, naudojant kliento identifikatorius ir atsitiktinius bitus (kuriuos perduoda serveris), duomenų perdavimo seanso pradžioje tam, kad būtų suformuotas vienas raktų ir algoritmų, kuriuos naudoja siuntėjas, gavėjas bei serveris, rinkinys. Kiekvieno duomenų perdavimo seanso metu, šifravimo raktai yra generuojami vienu metu visuose mazguose naudojant ANN. Šifravimo algoritmai ir painiojimo procedūros vienu metu pasirenkamos visų mazgų ANN iš šifravimo protokolų baigtinės aibės.

Duomenys užšifruojami siunčiančiajame mazge ir po to perduodami į identifikuotąjį serverį dešifruoti bei iš naujo užšifruoti (atsižvelgiant į kliento identifikatorių ir atsitiktinius bitus, kurie naudojami kaip serverio ANN neuronų įvesties duomenys) prieš galutinį šifruotų duomenų perdavimą galutiniam mazgui (gavėjui).

ANN naudoja sugeneruotus šifravimo raktus ir pasirinktus šifravimo algoritmus bei painiojimo procedūras duomenims šifruoti bei dešifruoti, perduodant juos tarp siuntėjo, gavėjo bei serverio mazgų.

Kiekvienas ANN naudoja skirtingą šifravimo raktų ir šifravimo algoritmų bei painiojimo procedūrų rinkinį iš šifravimo protokolų baigtinės aibės duomenims, perduodamiems tarp serverio ir gavėjo mazgų tinkle, šifruoti bei dešifruoti atskirai kiekvieno seanso metu, kaip pavaizduota 2 paveiksle.

3 paveiksle pavaizduotas nenutrūkstamai sinchronizuojamų ir savaime besimokančių ANN, tarp serverio bei visų kitų tinklo mazgų, įgyvendinimo pavyzdys. Naudojami savaiminio atpažinimo naudotojo raktai (kliento identifikatoriai) ir blokinės grandinės duomenys. ANN mokymas iš naujo vyksta, pasirodant kiekvienam naujam

blokui blokinėje grandinėje, prieš pradedant duomenų perdavimą. Naujinimo arba naujų blokų pasirodymo blokinėje grandinėje dažnis priklauso nuo užduoties ir specifinės tinklo struktūros. Tai gali būti daroma kartą per savaitę, kartą per dieną, kartą per valandą ir pan.

„Visiškai uždaros blokinės grandinės“ arba „Ekskliuzyvinių privačiųjų registrų“ tipo blokinės grandinės naudojamos tada, kai serveris veikia kaip vienintelis blokinės grandinės mazgas. Kiekvienas kitas mazgas, siuntėjo mazgas ir bent vienas gavėjo mazgas, turi blokinės grandinės duomenų kopiją. Serveris užsiima naujų blokų kūrimu, blokinė grandinė atnaujinama serverio iniciatyva, t. y. centralizuotai. Kiekvieną kartą pasikeitus blokinei grandinei (pridėjus naują bloką), ANN yra iš naujo mokomas serverio mazge, po to – visuose kituose mazguose. Duomenys iš blokinės grandinės naudojami kaip įvestis ANN rodikliams visuose kituose mazguose pakeisti. Mokymo iš naujo procesas valdomas iš serverio, kuriant naujus blokus ir naujinant blokinę grandinę.

Pagal vieną išradimo įgyvendinimo pavyzdį, sprendimai dėl visų duomenų apsaugos parametrų priimami, naudojant specialiai mokomus ir konfigūruojamus ANN, kurie kopijuojami kiekviename tinklo mazge ir visos ANN kopijos sinchronizuojamos tarpusavyje.

Pagal kitą išradimo įgyvendinimo pavyzdį, kai būdas naudojamas tinkle su centriniu serverio mazgu, apmokytas ANN yra naudojamas siuntėjo (arba gavėjo) mazgo pusėje ir serverio identifikavimo mazgo pusėje.

Šifravimo raktas sukuriamas tuo pat metu siuntėjo (arba gavėjo) mazgo pusėje ir tuo pat metu serverio mazge. Taip eliminuojamas šifravimo rakto perdavimo per tinklą etapas. Šiuo atveju duomenų perdavimas vyksta pagal centralizuotą žvaigždinę schemą,per jos identifikuojantjjį serverį, kuris gali būti tiek internete, tiek vietiniame tinkle. Kai duomenys per identifikuojantjjį serverį yra perduodami iš siuntėjo mazgo į bent vieną gavėjo mazgą, po informacijos gavimo iš siuntėjo mazgo, serverio mazge duomenys yra dešifruojami ir iš naujo užšifruojami, naudojant kitus parametrus, tokius kaip šifravimo algoritmas, kitas šifravimo raktas, papildomus duomenų apsaugos parametrus iš specifinio veiksmų rinkinio, skirtų duomenims perduoti galutiniam gavėjui.

Šiame įgyvendinimo pavyzdyje šifruojantysis ANN parenka šifravimo

algoritmą ir kitus veiksmus (šifravimo painiojimą) mazge, kuris šifruoja perduoti skirtus duomenis. Siuntėjo ANN tam tikru laiko tarpu parenka šifravimo algoritmą ir šifravimo raktą bei papildomus painiojimo ir duomenų srauto apsaugos būdus, sinchronizuodamasis su serverio ANN. ANN serverio mazge dešifruoja ir iš naujo užšifruoja duomenis raktu, sinchronizuotu su gavėjo ANN, kur ANN gavėjo mazge naudoja tą patį šifravimo algoritmą ir parenka šifravimo raktą iš tos pačios baigtinės aibės, kaip ir raktas, kuriuo buvo užšifruoti iš identifikuojančiojo serverio mazgo siunčiami duomenys.

Geriausiame įgyvendinimo pavyzdyje naudojami simetriniai šifravimo algoritmai, tokie kaip AES 256, 3DES, ChaCha, Salsa20, Blowfish, Twofish, DES, Kuznechik ir kt.

Kitame įgyvendinimo pavyzdyje ANN kiekviename mazge yra sinchronizuojami du kartus. Pirmasis ANN sinchronizavimas vyksta pasirodant naujam blokui blokinėje grandinėje (ji atskirai konfigūruojama kiekvienoje sistemoje). Antrasis, pakartotinis sinchronizavimas, vyksta centralizuotai perduodant identifikavimo raktus (kliento identifikatorius) visuose tinklo mazguose, t. y. siuntėjo, gavėjo ir visų klientų identifikatorių buvimo serverio mazge atveju. Kliento identifikavimo duomenys yra įtraukiami į duomenų rinkinį, perduodamą į tinklo įvestis, naujo duomenų perdavimo seanso pradžios momentu. ANN kiekviename tinklo mazge nuolat keičia bendrąją šifravimo loginę schemą per savimoką, kuriai įgyvendinti naudojamas savaime identifikuojantis naudotojo raktas (kliento identifikatorius) ir blokinės grandinės duomenys. Savimoka ir tinklo sinchronizacija vyksta pagal naujus blokinės grandinės blokus. Tam tikro mazgo sinchronizacija, seanso pradžioje, yra vykdoma naudojant atsitiktinius duomenis, kurie yra perduodami iš serverio (atsitiktiniai bitai) ir mazgo kliento identifikatorių.

Kitame įgyvendinimo pavyzdyje, patys šifravimo algoritmai ir įvairios painiojimo bei vieno šifravimo algoritmo naudojimo schemos įgyvendinamos programiškai, atskirai nuo neuroninio tinklo ir atskirame programinės įrangos modulyje. Kuriant naują duomenų perdavimo „klientas–serveris“ seansą, gaunama baigtinė šifravimo raktų ir veiksmų aibė, kuri taikoma specifiškai tik to seanso metu.

Dar kitame įgyvendinimo pavyzdyje, mokymas iš naujo kliento mazge, pagal blokinės grandinės duomenis (kurie gali būti maišos iš blokų rinkinio, maišų medžio arba Merklio medžio), vyksta blokinėje grandinėje pasirodžius naujam blokui. Po

mokymo iš naujo, pasikeičia ANN rodikliai ir išvesties vertės, kuriuos ANN generuoja duomenų perdavimo seanso pradžioje. Atitinkamai, valdant neuroninio tinklo rodiklių keitimo (mokymo pagal duomenis iš blokinės grandinės) procesą ir pateikiant unikalius duomenis į neuroninio tinklo įvestį, kiekvieno nuspėjimo atveju yra gaunami unikalūs kiekvieno seanso bei kliento šifravimo raktai ir su šifravimu susijusių veiksmų rinkinys. Minėti su šifravimu susiję veiksmai yra tokie kaip šifravimo algoritmų parinkimas bei jų keitimo procedūra, vieno šifravimo algoritmo taikymas kitam, „šiukšlių" pridėjimas prie šifruotų duomenų. Minėti veiksmai yra naudojami tik šio seanso metu ir tik šiam klientui. Naujo duomenų perdavimo seanso atveju ANN išvesties rinkinys bus kitoks.

Visi tinklo elementai, klientų mazgai ir serverio mazgai, turi analogišką architektūrą, blokinę grandinę, identiškos būsenos ANN, programinės įrangos modulį, kuris apdoroja ANN išvesties parametrus galutiniam sprendimui, dėl algoritmo pasirinkimo bei šifravimo raktų naudojimo, priimti.

Kiekvieno duomenų perdavimo seanso pradžioje serverio mazgas sukuria ir išsiunčia atsitiktinių parametrų (256–512 bitų) rinkinį kliento ANN įvesčiai. Be to, serverio mazgas sukuria ir išsaugo visus kliento identifikatorius, tad pradedant duomenų perdavimo seansą iš serverio mazgo su tam tikru kliento mazgu, jis gali dubliuoti ANN būseną ir jo išvesties duomenis savo pusėje, parinkdamas tą patį raktų rinkinį, tą pačią veiksmų seką ir tuos pačius šifravimo algoritmus, kurie buvo parinkti šiam seansui kliento pusėje. Vadinasi, parametrų rinkinio ir ANN būsenos sinchronizavimas bei duomenų perdavimas ANN pirmiausiai vyksta serverio mazge ir kliento mazge, su kuriuo keičiamasi duomenimis.

Toliau pateikti kompiuterinio neuroninės kriptografijos būdo duomenų perdavimui apsaugoti pavyzdžiai.

Pavyzdžiui, ANN yra apmokytas naudojant tam tikrą duomenų rinkinį. ANN apima tam tikrą skaičių įvesties neuronų, pageidautina, lygų įvesties duomenų apimčiai, kuri reikalinga nuspėjimui vykdyti, naudojant ANN. Pavyzdžiui, gali būti naudojami du duomenų rinkiniai. Pirminis 256–512 bitų atsitiktinių duomenų rinkinys perduodamas per tinklą iki kliento–serverio susijungimo iš serverio, antrasis duomenų rinkinys yra personalinis kliento identifikatorius, kuris gali būti unikalus 256–512 bitų raktas, X509 sertifikatas arba jie abu, priklausomai nuo galutinės užduoties. Duomenų rinkinio parametrai, papildomai identifikuojantys klientą, yra naudojami kaip

ANN apmokymo duomenų rinkinys.

Kliento–serverio susijungimo momentu, duomenų perdavimo seansas, per ANN paleidžiami du, bendrojo 512–1024 įvesties dydžio, duomenų rinkiniai. Neuronų išvesties sluoksnyje gaunami trys duomenų rinkiniai, kurie yra 256–512 bitų šifravimo rakto elementai, priklausantys nuo galutinio tikslo ir neuroninio tinklo naudojimo užduoties. Antrasis duomenų rinkinys yra elementų poslinkio pirmajame duomenų rinkinyje seka, skirta raktų intervalui pagal duomenis, gautus pirmajame verčių duomenų rinkinyje, sukurti.

Pavyzdžiui, duomenų rinkinys, sudarytas iš 256–512 bitų pirmajame duomenų rinkinyje (šifravimo rinkinyje), antrajame duomenų rinkinyje yra poslinkio parametrų rinkinys, taikant jį kaip kaukę arba poslinkio vektorių pirmajam duomenų rinkiniui, galima gauti 256 poslinkio variantus raktuose iš gautų bitų (arba didesnį variantų skaičių priklausomai nuo nustatytos galutinės užduoties). Po to, programinio apdorojimo ir raktų gavimo metu, bus naudojami lygiai tokie pat raktai, gauti pagal pirmąjį duomenų rinkinį, atsižvelgiant į poslinkį per užklotą iš antrojo duomenų rinkinio.

Taigi, duomenų perdavimo seanso pradžioje bus naudojamas pirmasis iš gautųjų raktų rinkinių, po to – antrasis ir t.t. iki 256 poslinkio variantų (arba didesnio skaičiaus variantų, nustatyto pirminio ANN kūrimo metu).

Pagal trečiąjį ANN duomenų rinkinį pasirenkamas šifravimo algoritmas, šifravimo algoritmų keitimo seka ir kitos užduotys, susijusios su šifravimo proceso painiojimu.

Pavyzdžiui, gali būti naudojamas ne mažiau kaip 3 simetrinius šifravimo algoritmus apimantis algoritmų rinkinys, keičiant jų seką ir loginę darbo su jais schemą pagal trečiąjį parametrų duomenų rinkinį, gautą iš neuroninio tinklo.

Būdas taip pat gali būti naudojamas decentralizuotoje sistemoje, tokioje kaip blokinė grandinė be centrinio identifikuojančiojo serverio, su daug blokinės grandinės mazgų (o ne vienu mazgu, kaip centralizuotoje schemoje). Naudojama „Visiškai uždaros blokinės grandinės“ arba „Ekskliuzyvinių privačiųjų registrų“ tipo blokinė grandinė. Kiekvienas mazgas turi blokinės grandinės duomenų kopiją. Centralizuotoje schemoje serveris naudojamas naujiems blokinės grandinės blokams kurti. Decentralizuotoje schemoje blokams kurti naudojamas kiekvienas atskiras

blokinės grandinės tinklo mazgas. Kiekvieną kartą pasikeitus blokinei grandinei (pridėjus naują bloką), ANN iš naujo mokomi kliento pusėje ir kiekviename kitame mazge, duomenys iš blokinės grandinės naudojami kaip įvestis ANN rodikliams keisti.

ANN nenutrūkstamai keis bendrąją šifravimo loginę schemą per nenutrūkstamą savimoką, kuriai įgyvendinti naudojamas savaime identifikuojantis naudotojo raktas (kliento identifikatorius) ir duomenys iš blokinės grandinės tinklo, kurie naudojami kaip duomenų rinkinys neuroniniam tinklui iš naujo mokyti, tačiau ne raktams saugoti ar jiems generuoti, priklausomai nuo blokinės grandinės.

Būdas gali būti naudojamas apsisaugoti nuo kvantinės skaičiavimo technikos dėl kintamos duomenų šifravimo loginės schemos, dėl to, kad nereikia per tinklą perduoti rakto ir naudoti simetrinių šifravimo algoritmų, kurie yra neįveikiami kvantinei skaičiavimo technikai.

Nors šis išradimo aprašymas apima daug charakteristikų ir pranašumų bei konstrukcinių elementų ir ypatybių, jis yra pateiktas kaip išradimo realizavimo pavyzdys. Nenukrypstant nuo išradimo esmės, galimi daliniai pakeitimai, ypač susiję su forma, dydžiu bei schema, pagal plačiausiai suprantamą apibrėžtyje pateiktų sąvokų ir apibrėžimų traktuotę.

IŠRADIMO APIBRĖŽTIS

1. Kompiuterinio duomenų šifravimo ir dešifravimo būdas tinkle, apimančiame tinklo mazgus, kur yra naudojamas dirbtinis neuroninis tinklas, besiskiriantis tuo, kad būdas apima:

dirbtinio neuroninio tinklo kopijų saugojimą bent pirmojo mazgo kliento kompiuteriniame įrenginyje, bent vieno kito mazgo kliento kompiuteriniame įrenginyje ir bent viename tinklo serverio mazge;

įvesties parametrų rinkinio siuntimą iš bent vieno tinklo serverio mazgo į pirmojo mazgo kliento kompiuterinį įrenginį ir bet vieną kitą mazgą;

dirbtinio neuroninio tinklo sinchronizavimą kiekviename mazge, naudojant įvesties parametrus;

šifravimo raktų kūrimą, naudojant dirbtinį neuroninį tinklą ir įvesties parametrus kiekviename tinklo mazge;

išvesties parametrų kūrimą, naudojant dirbtinį neuroninį tinklą, blokinės grandinės duomenis ir šifravimo raktus;

šifravimo algoritmo parinkimą, naudojant dirbtinį neuroninį tinklą ir išvesties parametrus;

šifravimo painiojimo tipo parinkimą, naudojant dirbtinį neuroninį tinklą ir išvesties parametrus;

šifravimo raktų, šifravimo algoritmų iš šifravimo painiojimo sinchronizavimą kiekviename tinklo mazge;

duomenų šifravimą, naudojant šifravimo raktus, parinktą šifravimo algoritmą ir parinktą šifravimo painiojimą;

šifruotų duomenų perdavimą iš pirmojo kliento kompiuterinio įrenginio į bent vieną tinklo serverį;

duomenų dešifravimą, naudojant šifravimo raktus, parinktą šifravimo algoritmą ir parinktą šifravimo painiojimą serveryje;

duomenų šifravimą iš naujo naudojant kitus parametrus, tokius kaip šifravimo algoritmas, kitas šifravimo raktas ir šifravimo painiojimas, serveryje;

iš naujo užšifruotų duomenų perdavimą galutinio naudotojo mazgui;

naujo blokinės grandinės bloko apskaičiavimą bent viename tinklo serverio mazge;

naujintos blokinės grandinės perdavimą iš bent vieno serverio mazgo į pirmąjį mazgą ir kiekvieną kitą tinklo mazgą;

dirbtinio neuroninio tinklo kiekviename tinklo mazge mokymą iš naujo, naudojant naujintą blokinę grandinę.

2. Būdas pagal 1 punktą, kur tinklas yra internetas arba vietinis tinklas.

3. Būdas pagal 1 punktą, kur vienas iš bent dviejų įvesties parametrų rinkinių yra generuojamas atsitiktine tvarka.

4. Būdas pagal 1 punktą, kur vienas iš bent dviejų įvesties parametrų rinkinių yra unikalus 256–512 bitų raktas, X509 sertifikatas arba jie abu.

5. Būdas pagal 1 punktą, kur šifravimo raktai vienu metu kuriami pirmajame mazge ir bent viename kitame mazge.

6. Būdas pagal 1 punktą, kur šifravimo algoritmas yra simetrinis šifravimo algoritmas.

7. Būdas pagal 6 punktą, kur šifravimo algoritmas yra parinktas iš grupės, apimančios AES 256, 3DES, ChaCha, Salsa20, Blowfish, Twofish, DES, Kuznechik.

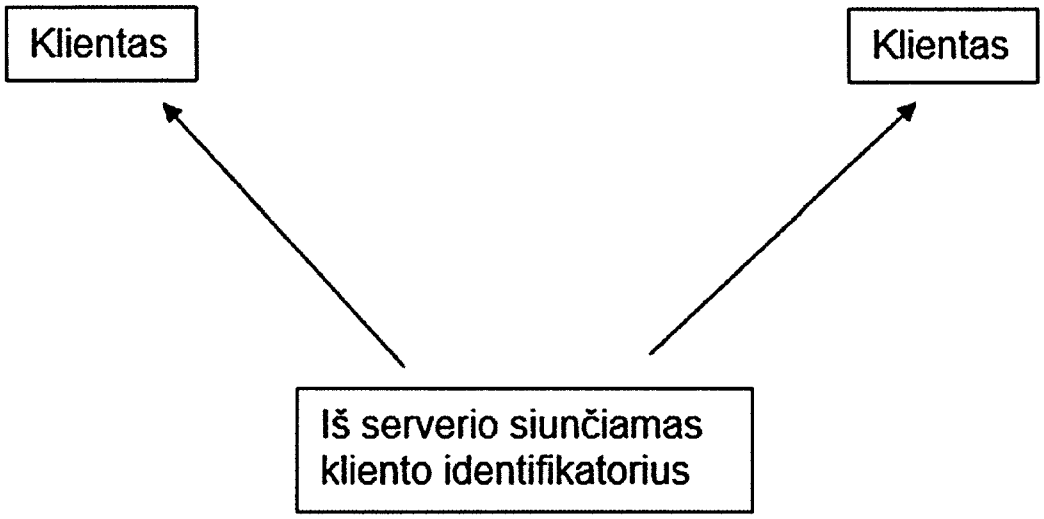
8. Būdas pagal 1 punktą, kur šifravimo raktas nėra perduodamas per tinklą.

9. Būdas pagal 1 punktą, kur duomenų perdavimas vyksta pagal centralizuotą žvaigždinę duomenų perdavimo schemą.

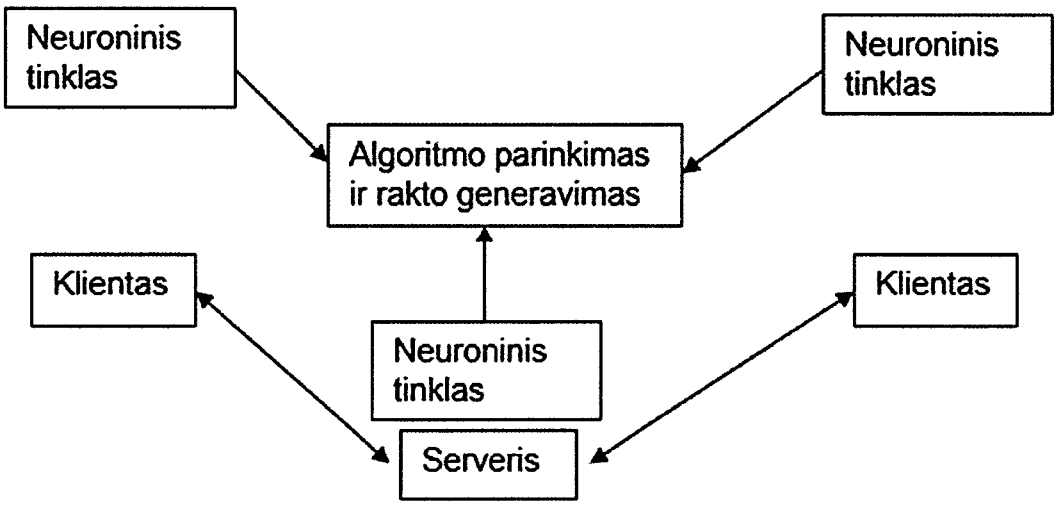
10. Būdas pagal 1 punktą, kur dirbtinis neuroninis tinklas mokomas, naudojant blokinę grandinę.

11. Būdas pagal 1 punktą, kur šifravimo raktas nėra saugomas blokinėje grandinėje.

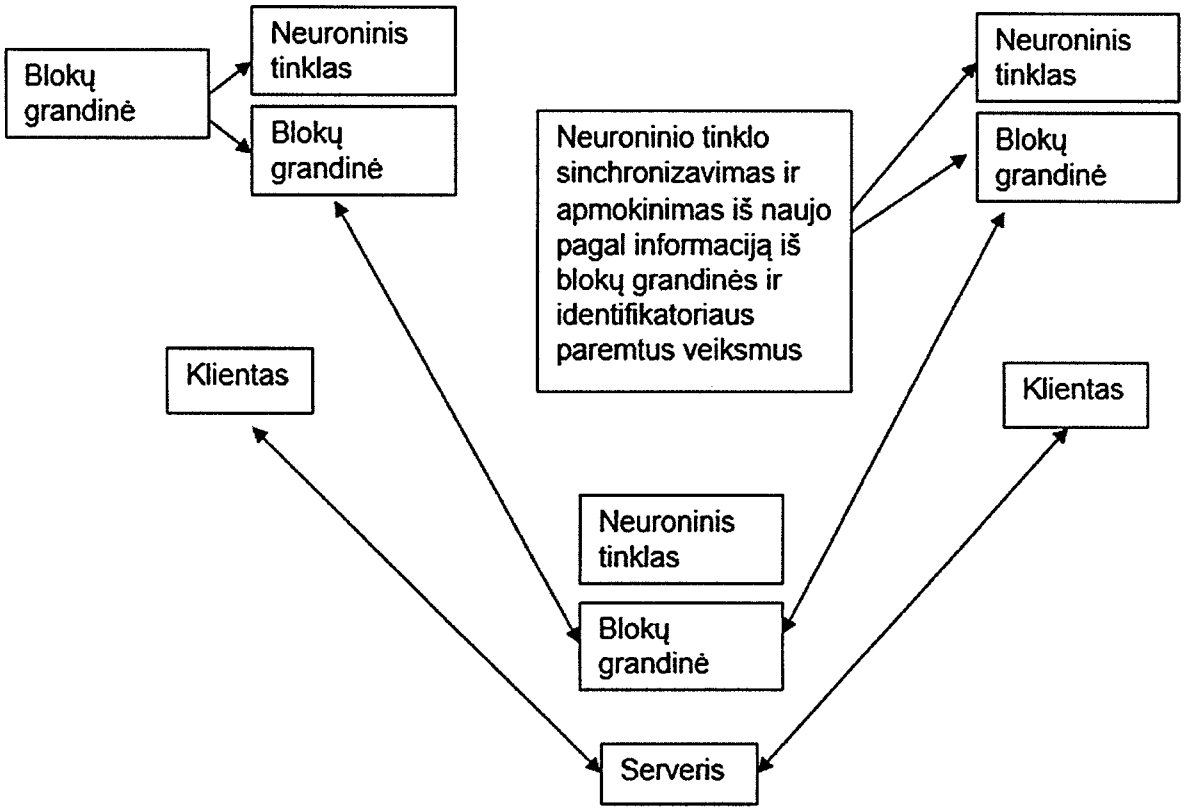
12. Būdas pagal 11 punktą, kur blokinėje grandinėje nėra saugomi jokie dirbtinio neuroninio tinklo elementai.


Klientas
Klientas
Iš serverio siunčiamas kliento identifikatorius

Pav. 1


Neuroninis tinklas
Neuroninis tinklas
Algoritmo parinkimas ir rakto generavimas
Klientas
Klientas
Neuroninis tinklas
Serveris

Pav. 2


Blokų grandinė
Neuroninis tinklas
Blokų grandinė
Neuroninio tinklo sinchronizavimas ir apmokinimas iš naujo pagal informaciją iš blokų grandinės ir identifikatoriaus paremtus veiksmus
Neuroninis tinklas
Blokų grandinė
Klientas
Klientas
Neuroninis tinklas
Blokų grandinė
Serveris

Pav. 3