LV 13618

(19) LATVIJAS REPUBLIKAS
PATENTU VALDE

(11) LV 13618 B

(51) Int.Cl G06F15/16
H04L9/00

Latvijas patents uz izgudrojumu
2007.g. 15.februāra Latvijas Republikas likums

(12) Īsziņas

(21) Pieteikuma numurs: P-07-46

(22) Pieteikuma datums: 25.04.2007

(41) Pieteikuma publikācijas datums: 20.09.2007

(45) Patenta publikācijas datums: 20.12.2008

(30) Prioritāte:
10/957,081 01.10.2004 US

(86) PCT pieteikums:
PCT/US2005/031353, 01.09.2005

(87) PCT publikācija:
WO2006/039053, 13.04.2006

(73) Īpašnieks(i):
WIDEVINE TECHNOLOGIES, INC., 900 Fourth Avenue, Suite 3400, Seattle WA 98164, US

(72) Izgudrotājs(i):
Glenn MORTEN (US),
Brian BAKER (US)

(74) Pilnvarotais vai pārstāvis:
Svetlana MAKEJEVA, Intelektuālā īpašuma juridiskā firma LATISS, Vidus iela 4-10, Rīga LV-1010, LV

(54) Virsraksts: **PROCESS UN STRAUMES SERVERIS DATU STRAUMES ŠIFRĒŠANAI KLIENTA VIRTUĀLĀS VIEDKARTES SISTĒMĀ**

(57) Kopsavilkums: Piedāvāts process, kas nodrošina datu straumes šifrēšanu, lai padarītu drošu datu straumi vienreizējai apskatei un aizsargātu autortiesības uz datu straumi. It īpaši tiek piedāvāts process, lai aizsargātu multivides, izklaides un komunicēšanas datu pārraides procesu (straumēšanu) interneta vidē. Tiek piedāvāts straumes servera sastāvdaļas, kas ir operatīvi savienotas ar straumes serveri un mijiedarbojas ar lietotāja sistēmu, kura ietver virtuālo viedkarti rodošā procesa efektivitātes palielināšanai.

PROCESS UN STRAUMĒŠANAS SERVERIS DATU STRAUMES ŠIFRĒŠANAI KLIENTA VIRTUĀLĀS VIEDKARTES SISTĒMĀ

Izgudrojuma tehniskais lauks

Šis izgudrojums nodrošina datu straumēšanas šifrēšanas procesu, lai padarītu drošu datu straumi vienreizējai apskatei un aizsargātu datu plūsmas autortiesības. Izgudrojums nodrošina multivides, izklaides un sakaru straumēšanas aizsardzības procesu, pārraidot interneta vidē. Turklāt šis izgudrojums klienta sistēmā papildus nodrošina virtuālu viedkarti, kas mijiedarbojas ar straumēšanas servera komponentu, lai ietekmētu rodošo procesu.

Iepriekšējais tehnikas līmenis

Internets ir nodrošinājis atšķirīgu saziņas veidu, kurā dati var tikt straumēti no servera klientam. Klients ir atbildīgs par straumēto datu, vēlams straumētās multivides, parādīšanu lietotājam. Serveris ir atbildīgs par datu straumēšanas nogādāšanu klientam. Real Networks un Microsoft Solutions sūta datu straumi, izmantojot UDP (bezsavienojuma interneta protokolu) kopā ar citu savienojumu starp klientu un serveri, kas kontrolē datu straumējuma pārraidi. Kontroles savienojuma elements funkcionē tā, lai apturētu bufera pārņemšanu, un tas var pielāgot straumēšanas pārraidi, lai kompensētu frekvenču joslas platuma latentumus. Taču šajā sistēmā ir viena problēma – no servera klientam straumētie dati nav aizsargāti un visiem tīklā pieejami. Tāpēc ir radusies nepieciešamība pēc labākas aizsardzības no pārtveršanas tādos plaša diapazona tīklos kā internets. Šī nepieciešamība specifiski attiecas uz spēju nodrošināt aizsardzību pret neatļautu pārtveršanu un iespēju kopēt datu straumējumu internetā. Pašlaik nav neviena aizsargmehānisma, kas aizsargātu datus ar autortiesībām.
Tiklīdz serveris nosūta datus un lietotājs tos saņem vai lietotājs tos saņem pēc pārtveršanas, nav iespējams ierobežot šo datu pārsūtīšanu tiklīdz tie tiek palaisti internetā. Pat ja datu straumēšanas autortiesības ir aizsargātas, nav iespējams aizsargāt vai īstenot datu straumēšanas autortiesību aizsardzību. Iestāde, kurai pieder autortiesības un kura straumē šādu saturu, apzinās, ka nav iespējams kontrolēt to, kas tiek darīts ar šo saturu pēc tā palaišanas. Tāpēc ir radusies nepieciešamība nodrošināt līdzekļus satura autortiesību aizsardzībai pēc tā straumēšanas internetā. Izgudrojums tika izstrādāts abām vajadzībām.

Pašlaik faktiski neviens mediju straumēšanas risinājums nešifrē datus, kas tiek sūtīti no servera klientam. Šai problēmai pastāv viens risinājums, ko var sasniegt, izmantojot esošās tehnoloģijas, piemēram, apvienojot standarta SSL drošligzdu HTTP ar tādu straumēšanas programmatūras pakotni kā Quicktime. Diemžēl programmatūras pakotnē Quicktime nav pieejama pilnekrāna skata opcija. Tāpēc nepieciešams izstrādāt labāku video datu straumēšanas metodi.

Izgudrojuma izvērsts kopsavilkums

Izgudrojums nodrošina datu straumēšanas šifrēšanas procesu, lai aizsargātu datu straumi, iespējojot tikai vienu apskati, tas ir:

(a) nodrošina klienta atlasi datu straumējuma pārraidei;
(b) atver savienojumu ar straumēšanas serveri un nosūta straumēšanas serverim informāciju par URI, marķieri un lietotāju, kur straumēšanas serveris sastāv no klienta datu savienojuma moduļa, lai sūtītu datu pakotnes klientam, šifrēšanas moduļa, lai izmantotu ar klientu saskaņotas šifrēšanas atslēgas datu straumēšanas, un datu savienojuma moduļa, kas savienots ar klientu šifrēšanai, un plūsmas kontroles moduļa datu straumēšanas plūsmas ātruma kontrolēšanai, lai pilnībā uzturētu klienta buferi;
(c) Apstiprina vai neatzīst derīgu vai nederīgu URI un marķiera kombināciju transakcijas serverī, kur transakcijas serveris sastāv no klienta mijiedarbības moduļa lietotāja savienošanai ar transakcijas servera komponentu, lietotāja verifikācijas modulim ir

lietotāja datubāze, kur lietotāja verifikācijas modulis ir saistīts ar klienta mijiedarbības moduli un pārbauda, vai lietotājs ir derīgs, un URI un marķiera izveides moduļa, kas ir saistīts ar lietotāja verifikācijas moduli jauna URI un marķieru izveidei pēc lietotāja pieprasījuma;

(d) Nodrošina nepārtraukti šifrētu datu plūsmu klientam, ja tiek atrasts derīga URI un marķiera kombinācija.

Straumēšanas servera komponents var papildus saturēt operējamu lasīšanas bufera moduli savienotu ar plūsmas vadības moduli datu lasīšanai no avota metrāžas glabāšanas vidē. Taču šādā izkārtojumā dati nav ierobežoti un tajos varbūt iekļauti dati no dažādiem citiem avotiem, iekļaujot e-komercijas transakciju, interaktīvu televīzijas avotu, multiraides pakalpojumu, uniraides pakalpojumu un līdzīgus. Straumēšanas servera komponents papildus var sastāvēt no lietotāja interfeisa moduļa, kas savienots ar failu sistēmas moduli vai plūsmas kontroles moduli serveru opciju iestatīšanai. Straumēšanas serveris papildus var sastāvēt no klienta servera komponenta, kurā ir datu straumēšanas kontroles protokola moduļi, lai izveidotu sākotnējo savienojumu ar straumēšanas servera komponentu, atšifrēšanas moduļa, lai atšifrētu ienākošo datu straumi, ievades bufera, lai buferētu ienākošās datu straumēšanas, un rādīšanas kontroles moduļa, lai kontrolētu datu straumējuma rādīšanu. Klienta servera komponents var papildus sastāvēt no rādīšanas moduļa, lai rādītu audio un video datus.

Nodrošinot nepārtraukti šifrētus datus, solis (d) papildus var sastāvēt no lietotāja interfeisa moduļa straumēšanas serverī, lai atļautu pauzēt, apturēt, atskaņot, restartēt datu straumi vai citādi mijiedarboties ar datu straumi un/vai datu straumēšanas avotu. Citos gadījumos transakcijas serveri datu šifrēšanai kompensē ASP skripti.

Izgudrojums papildus ietver straumēšanas serveri datu straumēšanas šifrēšanai, lai nodrošinātu datu straumi un tā būtu skatāma tikai vienreizēji, tas ietver:

(a) straumēšanas servera komponenta, pie kam straumēšanas servera komponents ietver klienta datu savienojuma moduļi, lai klientam sūtītu datu pakotnes, un šifrēšanas moduļi, lai datu šifrēšanai izmantotu ar klientu saskaņotas šifrēšanas atslēgas, un klientu datu savienojumam pievienotu moduļi, plūsmas vadības moduļi datu straumēšanas plūsmas ātruma kontrolēšanai, lai vienmēr uzturētu pilnu klienta buferi; un

(b) transakcijas servera komponenta, pie kam transakcijas servera komponents ietver klienta mijiedarbības moduļi lietotāja savienošanai ar transakcijas servera komponentu, lietotāja verifikācijas moduļi, kurā ir lietotāju datubāze, pie kam lietotāja verifikācijas modulis ir saistīts ar klienta mijiedarbības moduli un tas pārbauda lietotāja derīgumu, un URI un marķiera izveides moduļi, kas saistīts ar lietotāja verifikācijas moduli jaunu URI un marķiera izveidei pēc lietotāja pieprasījuma.

Straumēšanas servera komponents papildus var sastāvēt no lasīšanas bufera moduļa saistīta ar plūsmas vadības moduli datu lasīšanai no avota metrāžas glabāšanas vidē. Taču datos var būt iekļauti dati no interaktīva avota, tāda avota kā interaktīvās televīzijas pakalpojumiem utt. Straumēšanas servera komponents var papildus sastāvēt no lietotāja interfeisa moduļa, kas saistīts ar failu sistēmas moduli vai plūsmas vadības moduli servera opciju iestatīšanai. Straumēšanas serveris var papildus sastāvēt no klientu servera komponenta, kas sastāv no datu straumēšanas vadības protokola moduļa, lai izveidotu sākotnēju savienojumu ar straumēšanas servera komponentu, atšifrēšanas moduļa, lai atšifrētu ienākošo datu straumi, ievades bufera moduļa, lai buferētu ienākošu datu straumēšanas, un rādīšanas vadības moduļa, lai vadīt datu straumējuma rādīšanu. Klientu servera komponents var papildus sastāvēt no rādīšanas moduļa, lai rādītu audio un video datus.

Īss attēlu apraksts

Attēlā 1 ir parādīta klienta komponenta shēma, kas var saņemt un skatīt šifrēto datu plūsmu. Klienta komponents sastāv no marķieru glabāšanas moduļa 100, straumēšanas vadības protokola moduļa 120 un atšifrēšanas moduļa 160.

Attēlā 2 ir attēlota straumēšanas servera komponenta shēma, kuram ir vismaz šifrēšanas modulis 220 un klienta vadības savienojuma modulis 200 atslēgu saskaņošanai un marķieru verifikācijai.

Attēlā 3 ir attēlota transakciju servera komponentu shēma, kuriem ir marķieru izveides modulis 330 un lietotāja verifikācijas modulis 310.

Attēlā 4 ir attēlota dažādu klientu scenāriju shēma, kurā parādīta nepieciešamība pēc marķiera, nolūkā atvert (atšifrēt) datu straumes aplūkošanai.

Attēlā 5 ir attelota straumēšanas servera procesa shēma, kas atspoguļo lietotāja marķiera saņemšanu, kas savukārt iedarbinā šifrēšanas atslēgu saskaņošanu, lai padarītu pieejamu datu straumes apskati un saņemšanu.

Attēlā 6 ir attēlota transakcijas servera procesa shēma, kas nodrošina lietotāju novietņu konfigurāciju un marķiera izveidi.

Attēlā 7 ir attēlota virtuālā viedkarte (VSC) klienta ierīcē, kas konfigurēta, lai mijiedarbotos ar transakcijas serveri ar mērķi vadīt datu straumi atbilstoši šim izgudrojumam.

Detalizēts izgudrojuma īstenošanas labāka varianta apraksts

Izgudrojums nodrošina šifrēšanas procesu tādām datu straumēm kā multivides izklaidēm un komunikācijām, izmantojot internetu. Šifrēto datu plūsma ļauj ar autortiesībām aizsargātus materiālus un multivides komunikācijas (piemēram, analītiķu sapulces, interaktīvā televīzija, filmas) droši pārraidīt, piemēram, pēc principa – maksa par vienu skatīšanas reizi, un tml. Datu straumi nevar saglabāt klienta aparatūrā, lai to atskaņotu turpmāk, vai pārsūtīt. Taču klients var skatīt datu straumi neierobežotas reizes noteiktā laika posmā.

Šifrēšanas protokols nodrošina, piemēram, šifrēšanas 192 bitu atslēgas algoritmu (piemēram, Triple DES), UDP paketes protokolu, RTSP (2326 rcf) paketes pārsūtīšanas protokolu, RTP (1889 rcf) paketes pārsūtīšanas kontroles protokolu un MPEGI video atmiņas saspiešanu. Taču turpmāk norādītais vēlamā šifrēšanas protokola piemērs mainīsies tā kā šādas tehnoloģijas tiek nemitīgi uzlabotas. Piemēram, vienā salikumā var būt Advanced Encryption Standard (uzlabotais šifrēšanas standarts – AES) vai līdzīgs šifrēšanas algoritms.

Viena no izgudrotā procesa priekšrocībām, izmantojot izgudroto straumēšanas serveri un transakcijas serveri, ir tāda, ka klientam faktiski nav jābūt pilnībā optimizētam aprīkojumam. Parasti viens klients izmanto jebkuru ierīci jebkurā laikā. Klients var būt konfigurēts tā, lai atskaņotu, piemēram, 30fps 320x240 video un audio bez trīces. Tādējādi ir iespējama apmēram 250-300 kpa datu straume, liels datu buferis (vismaz daži megabaiti) un 350 MHz Pentium II procesors vai jaudīgāks, ar Windows 98 vai Windows NT. Taču klienta sistēmai nav tādu ierobežojumu un faktiski var izmantot jebkuru klienta sistēmas konfigurāciju. Piemēram, klientu sistēmā var būt iekļauta televizora pierīce, interaktīvā televīzijas iespēja utt.

Serveris, piemēram, var būt pilnībā optimizēts, vairākpavedinošanas (pavedienu pūls) Windows NT pakalpojums. HTTP serveris darbojās otrādi, proti, tas ļauj klientu sesijām tikt notvertām un serverim jāuztur stāvoklis attiecībā uz visiem klientiem.

Definīcijas

Šie termini tiek izmantoti ar šeit definētu nozīmi.
Klients vai klientu sistēma ir dators, uz kuru tiek sūtīta datu straume.
Lietotājs ir persona, kura pilda klienta instrukcijas.

Modulis ir kompilētu kodu kopums, kas paredzēts noveiktas funkcijas vai funkciju kopas veikšanai.

URI (Universal Resource Identifier – universāls resursu identifikators) ir identifikators, kas saistīts ar straumēšanas servera atrašanās vietu.

Marķieris ir bināra informācijas daļa, kurā ir iekļautas atļaujas, kas lietotājam ir piešķirtas noteiktai datu straumei.

Autentifikācija nodrošina konfidencialitātes līmeni, kurš tiek noteikts komponentam, ierīcei, personai vai citai entītijai. Dažos gadījumos autentifikācija var tikt uztverta kā sinonīms vārdam identifikācija.

Autorizācija nodrošina piekļuves kontroles līmeni un tā ir paredzēta, lai atbildētu uz jautājumu par to, kādas darbības entītijai ir tiesības veikt. Piemēram, autorizācija ir atbildīga par to, vai entītijai ir atļauja piekļūt atlasītajiem datiem un kad tiem var piekļūt, kā arī uz cik ilgu laiku.

CAS (Conditional Access System – nosacījuma piekļuves sistēma). CAS iekļauj tehnoloģijas, kas paredzētas piekļuves kontrolei tādiem pakalpojumiem kā ciparu televīzija utt., šifrējot pārraidīto programmējumu. Taču CAS neattiecas tikai uz televīziju. Tā var iekļaut ciparu radio pārraidi, ciparu datu pārraidi, netranslējamo informāciju, interaktīvos pakalpojumus utt. Tāpēc CAS var būt iekļauta tāda datu straumējuma piekļuve, kā aprakstīta šeit.

Ātrā atjaunošana nodrošina klienta ierīcei, sistēmai utt. atslēgu ģenerēšanu, jaunu atslēgu un jaunu drošības mehānismu. Vienā salikumā dinamiskā ātrā atjaunošana nodrošina drošības mehānisma atjaunošanu pēc nejaušības principa, lai izveidotu neparedzamu vidi un mērķētu to uz citiem, piemēram, hakeriem.

DRM (Digital Rights Managment – ciparu tiesību pārvaldība) ir fails, kas balstīts uz alternatīvu mehānismu vides aizsardzībai. DRM iekļauj, piemēram, paša satura, piemēram, datu straumes, aizsardzību. Vienā salikumā licences fails vai kaut kas līdzīgs var tikt izdots, lai dotu lietotājam iespēju atskaņot saturu, vai nu kopā ar saturu vai tad, kad lietotājs mēģina atskaņot saturu. Saturs, piemēram, datu straume, var būt šifrēts un šifrēšanas detaļas var būt saglabātas, saturam ceļojot starp tīkliem, serveriem un klientiem. DRM, kā aprakstīts šeit, var izmantot virtuālo viedkarti, lai iedarbinātu satura pārvaldību un aizsardzību.

ECM (Entitlement Control Messages – pilnvaru kontroles ziņojumi) iekļauj šifrētos datus, kas saistīti ar pilnvaram, tādiem kā marķieri, piekļuves ierobežojumi, satura/šifrēšanas atslēgām utt.

EMM (Entitlement Management Messages – pilnvaru vadības ziņojumi) iekļauj tādus šifrētos datus kā pilnvaras, tādus kā marķieri, satura/šifrēšanas atslēgas utt.

Ielaušanas gadījumu noteikšana iekļauj mehānismus gadījumu noteikšanai, kad var tikt lauzta drošības politika un cita aizsardzība.

Dalības nolieguma neiespējamība iekļauj mehānismus, kas nodrošina, ka lietotājs, patērētājs, klients utt. nevar noliegt ciparu paraksta derīgumu. Viens salikums izmanto divas atšķirīgas

atslēgas. Viena atslēga var deponēta un to var izmantot darbībām, kurām nav nepieciešams paraksts. Otra atslēga var būt bez atkopšanas mehānisma un to var izmantot parakstam. Šādā salikumā, kur lietotājs var vienpersoniski kontrolēt parakstīšanās atslēgu, dalības nolieguma neiespējamību var panākt, izmantojot noslēpumu, kas pieder vienai personai un ir pārbaudāms. Ja parakstīšanās derīgums ir kritisks, var izmantot atsevišķu atslēgu un šī atslēga var piederēt tikai atslēgas īpašniekam, un tā ir pārbaudāma. Citā salikumā, atslēgas īpašnieks var atteikt paraksta derīguma pārbaudi balstoties uz veiksmīgi priviliģētu entītiju, kura spēj pavairot slepeno atslēgu.

Vienā radošā procesa un straumēšanas servera salikumā video objekts var tikt glabāts servera ierīcēs nešifrēts – faili tiek izgūti tikai, izmantojot servera programmatūru. Izgudrotais serveris būs atbildīgs par (1) šifrēšanas atslēgu kopas saskaņošanu un (2) datu straumes šifrēšanu „uz vietas", tādējādi padarot datu kopas, kas tiek palaistas tīklā, derīgas tikai paredzētajai ierīcei un nederīgas citiem datoriem. Viens no šifrēšanas standartiem ir TRIPLE-DES ar (168) bitu atslēgu. Serveris datu pārsūtīšanai izmantos UDP. Šis protokols izmanto ievērojami mazāk tīkla resursu nekā citi TCP protokoli (piemēram, http).

Pamatprogrammatūra būs atbildīga par datu straumēšanas atšifrēšanu un reproducēšanu. Izmantotās šifrēšanas atslēgas var atšķirties katru reizi, piekļūstot datu straumei. Katru reizi, kad tiek iedarbināta programma, tiek izveidota atšķirīga šifrēšanas atslēga, tāpēc programma nevar reproducēt iepriekšējās datu straumes, ja tās tika kaut kādā veidā saglabātas uz diska.

Ilustratīvā vide

Attēlā 1 ir parādīta shēma vienam salikumam ar radošā procesa klienta komponentu un straumēšanas serveri, kas var saņemt, skatīt un/vai citādi piekļūt šifrēto datu straumei. Pragrammatūra glabā visu pašreizējo datu straumju un atbilstošu marķieru sarakstu. Šī informācija tika glabāta marķieru glabāšanas modulī (100). Šis saraksts iekļaus šādus objektus: (1) URI; (2) URI marķieris un (3) servera norādītais termiņa datums. Vienā salikumā nav vēlams, lai klientam būtu jebkāda iespēja noteikt marķiera derīgumu. Tamdēļ un arī nolūkā izņemt novecojošos marķierus, serveris atgriež beigu datumu. Šo informāciju izmanto programma informācijas rādīšanai. Beigu datums pats par sevi var arī netikt sūtīts atpakaļ uz serveri, un serveris pārbauda vai marķieris ir derīgs. Moduļa ierīces, varētu būt izmantoti kā marķieru glabāšanas moduļi, ietver, piemēram, brīvpiekļuves atmiņu (RAM) un tīkla interfeisa karti vai modemu, kas savienojumā ar programmu nodrošina marķieru beigu datumu pārbaudi un izsekošanu..

Klients sazinās ar lietotāja interfeisu (110). Klientam var būt standarta lietotāja interfeiss, kas nodrošinās pienācīgu lietošanas pieredzi. Interfeisam ir iespēja pārskatīt esošās derīgas straumes vai savienoties ar serveri lai meklētu citas straumes, kas var būt redzamas. Klienta lietotāja interfeiss (110) sazinās ar moduli (130) ar lokālo displeja kontroli un moduli (120) ar straumes kontroles protokolu. Klientam ir jāspēj uzstādīt komunikācijas sesijas ar serveri, kā arī kontrolēt datu plūsmu no servera tiklīdz plūsma ir skatāma. Modulis (120) ar straumes kontroles protokolu veido sākotnējo savienojumu, savienojoties ar serveri, nododot pieprasīto URI, marķieri, un lietotāja informāciju. Modulis (120) ar straumes kontroles protokolu tālāk ģenerē šifrēšanas atslēgu rindu un kontrole datu plūsmu no servera. Ierīču ar moduļu (120) ar straumes kontroles protokolu piemēri klienta ietvaros, kas var būt izmantojami, lai ģenerētu šifrēšanas atslēgu rindu un kontrolētu datu plūsmu no servera ietver, piemēram, brīvpieejas atmiņu (RAM) un tīkla interfeisu vai modemu. Programmatūra var uzraudzīt saņemamo datu līmeni, nosūtot tīkla statistiku, informāciju, kas ir attiecināma uz buferi, ieskaitot kopīgo procentu, atliekošo procentu un līdzīgus, kā arī citas klienta raksturlielumus straumēšanas serverim. Modulis (130) ar lokālo displeja kontroli kontrolē datu rādījumu un ir spējīgs apstādināt, apturēt un palaist datu plūsmu. Moduļu (130) ar lokālo displeja kontroli piemēri piemēroti izmantošanai klienta ietvaros ietver

brīvpieejas atmiņu un videoplati. Programmatūra izmantojama šajā modulī pārvērš datus, kas tiek sūtīti no servera formātā, kas var būt rādīts lietotājam.

Rādīšanas modulis (140) rāda video un audio datus. Ievades bufera modulis (150) ir modulis, kurā ir iekļauts straumēšanas buferis. Straumēšanas buferī var būt atšifrēto datu cirkulārs buferis, no kura rādīšanas vadības buferis nolasa un uz kuru atšifrēšanas modulis ieraksta. Straumēšanas bufera moduļa ierīces, kuras var izmantot, lai iekļautu atšifrēto datu cirkulāro buferi, var būt, piemēram, brīvpieejas atmiņa (RAM). Tā kā paketes tiek saņemtas no servera pirms dati tiek ievietoti ievades buferī, dati transportēšanas paketē tiek atšifrēti ar atšifrēšanas moduli (160), izmantojot ar straumes vadības protokola moduli 120 saskaņotas atslēgas.

Atšifrēšanas moduli (160) var tikt ieviests, izmantojot faktiski jebkuru atšifrēšanas mehānismu, iekļaujot tos, kas tiek izmantojami rūpnieciskos apjomos. Piemēram, SSL, DES un RSA moduļi var būt pieejami un piemēroti izmantošanai kā atšifrēšanas modulis. Visbeidzot klienta komponenta pusē ir datu straumes saņemšanas modulis 170. Šis modulis nodrošina servera sūtīto datu pakešu saņemšanu.

Atbilstošas moduļa ierīces, kuras var izmantot kā datu straumes saņemšanas moduļus klienta komponentā, var būt, piemēram, brīvpieejas atmiņa (RAM). Šajā modulī iekļautā programmatūra var saglabāt klienta saņemtos datus formātā, kas varēs izmantot nākamie moduļi.

Attēlā 2 klienta kontroles savienojuma modulis (200) nodrošina kontroles komunikācijas starp klientu un serveri. Klients un serveris saskaņos šifrēto atslēgu kopu. Klients nosūta uz serveri lietotāja informāciju, URI un marķieri, izmantojot klienta vadības savienojuma moduli (200). No šī moduļa (200) klientam straumētie dati var tikt kontrolēti (tas ir, uz laiku apstādināti, apturēti vispār un atsākti). Aparatūras ierīces, kuras var tikt izmantoti kā klienta vadības savienojuma modulis straumēšanas serverī, var būt brīvpieejas atmiņa (RAM). Šādi aparatūras komponenti ļauj izpildīt operācijas, kas nav izpildāmi ar specifisko aparatūru. Šāda programmatūra ir iegulta klienta vadības savienojuma modulī vai tajā augšupielādēta. Programmatūra darbojas, lai izveidotu procesu, kurā klients un serveris apmaiņas ar datiem par pašreiz esošiem tīkla nosacījumiem un atbilstoši modificē datu straumi.

Klienta datu savienojuma modulis (210) darbojas, lai sūtītu datu paketes klientam, izmantojot bezsavienojuma protokolu, lai mazinātu servera virstēriņu. Aparatūras ierīces, kas piemērotas izmantošanai par klienta datu savienojuma moduliem straumēšanas serverī, var būt brīvpieejas atmiņas (RAM) un un tīkla interfeisa kartes (Network Interface Cards). Šāda programmatūra ir iegulta klienta datu savienojuma modulī vai tajā augšupielādēta. Programmatūra darbojas, lai izveidotu procesu, kurā šifrēties dati tiek sūtīti uz klienta ierīci, izmantojot tīkla pakotnes.

Šifrēšanas modulis (220) izmanto ar klientu/serveri saskaņotas atslēgas, lai šifrētu datu straumi, sūtot to klientam. Tādējādi ir iespējama šifrēšana „uz vietas", un šifrēšanas atslēgas būs unikālas visiem klientu/serveru savienojumiem. Tādējādi avota metrāžu var glabāt serverī nešifrētu, kur tas piemērojams. Aparatūras ierīces, kas piemērotas izmantot kā šifrēšanas moduli straumēšanas serverī, var būt brīvpieejas atmiņa (RAM) un īpašniekaparatūras šifrēšanas ierīces. Šādi aparatūras komponenti iekļauj programmatūru, kas darbojas, lai veiktu datu šifrēšanu. Šāda programmatūra var būt iegulta šifrēšanas modulī vai tajā augšupielādēta. Programmatūra darbojas, lai izveidotu procesu, kurā dati, kas tiek sūtīti uz ierīci, ir šifrēti ar atslēgām, kas sākotnēji saskaņotas ar klientu un izvades dati ir tādā formātā, ko var lasīt tikai pēc tam, kad klients tos atšifrējis.

Plūsmas vadības modulis (230) nodrošina, ka servera sūtītā datu straume ir tādā ātrumā, kādā datus izmanto klients. Klienta buferim jābūt visu laiku pilnam, bet datu straumējums nevar tikt pārrakstīts. Tāpēc plūsmas vadības modulis komunicē ar šifrēšanas moduli (220) un izmanto atgriezenisko saiti, ko ieguvis no klienta vadības savienojuma moduļa (200). Aparatūras ierīces,

kas piemērotas izmantošanai par plūsmas vadības moduli straumēšanas serverī, iekļauj brīvpieejas atmiņu (RAM). Šāda programmatūra var būt iegulta plūsmas vadības modulī vai tajā augšupielādēta. Programmatūra darbojas, lai izveidotu procesu, kurā tiek regulēta datu plūsma no servera klientam.

Failu sistēmas lasīšanas buferis (240) ir paredzēts servera darbībām. Mazi datu apjomi, kas tiek nolasīti no faila, var tikt glabāti atmiņā un failam nav jābūt visu laiku atvērtam failu sistēmā. Failu sistēmas modulis (250) ir atbildīgs par datu lasīšanu no avota metrāžas glabāšanas vidē vai citur. Failu sistēmu modulis komunicē ar klienta vadības savienojuma moduli (200), lai atvērtu URI un lietotāja interfeisa moduli (260) un lai reģistrētu ceļa konfigurācijas. Programmatūras ierīces, kas piemērotas izmantošanai par failu sistēmas moduli straumēšanas serverī, iekļauj brīvpieejas atmiņu (RAM). Šāda programmatūra var būt iegulta failu sistēmas modulī vai tajā augšupielādēta. Programmatūra darbojas, lai izveidotu procesu, kurā sekundārajā glabāšanas ierīcē glabātie dati var tikt ielādēti brīvpieejas atmiņā (RAM), lai tos var nogādāt šifrēšanas modulī.

Straumēšanas serveris papildus nodrošina vienkāršu lietotāja interfeisa moduli (260) servera opciju konfigurācijai, piemēram, ar kuru tīkla portu sasaistīt un avota metrāžas atrašanās vietas iestatīšanai. Aparatūras ierīces, kas piemērotas izmantot kā failu sistēmas moduli straumēšanas serverī, iekļauj brīvpieejas atmiņu (RAM). Šāda programmatūra ir iegulta failu sistēmas modulī vai tajā augšupielādēta. Programmatūra darbojas, lai izveidotu procesu, kurā servera aparatūras lietotājs var norādīt failu sistēmas modulim, kur doties, lai atrastu datu straumes.

Attēlā 3 transakcijas serveris satur četrus moduļa komponentus. Lai piekļūtu video straumei, klientam vispirms jāiegūst transakcijas marķieris. Transakcijas marķieris var tikt balstīts uz shēmu „maksā par katru pārlūkošanas reizi", kurā marķieris ir derīgs noteiktam laika periodam. Marķiera derīguma laiks ir atkarīgs no lietotāja veiktās atlases un atlasītās straumes pieejamajām opcijām. Lietotājs sazinās ar transakcijas serveri, izmantojot klienta mijiedarbības moduli (300) ar lietotāja informāciju un URI. Transakcijas serveris nosaka marķierim un lietotājam pieejamās laika opcijas. Pēc tam, kad lietotājs ir atlasījis laika ierobežojumu, pieprasījums tiek nodots lietotāja verifikācijas modulim (310). Aparatūras ierīces, kas piemērotas izmantošanai par klienta transakcijas moduli straumēšanas serverī, iekļauj brīvpieejas atmiņu (RAM). Šāda programmatūra var būt iegulta klienta mijiedarbības modulī vai tajā augšupielādēta. Programmatūra darbojas, lai izveidotu procesu, kurā lietotāja informācija tiek salīdzināta ar datu bāzi un tiek izveidots derīgs marķieris, balstoties uz lietotāja pieprasītajām opcijām.

Lietotāja verifikācijas modulis (310) pārbauda lietotāja informāciju, kas nodota lietotāju datu bāzē, lai noskaidrotu, vai lietotājs ir derīgs vai nē. Lietotāja datu bāze atrodas lietotāja verifikācijas moduļa atmiņā. Aparatūras ierīces, kas piemērotas izmantošanai par lietotāja verifikācijas moduli transakcijas serverī, iekļauj brīvpieejas atmiņu (RAM). Šāda programmatūra ir iegulta lietotāja verifikācijas modulī vai tajā augšupielādēta. Programmatūra darbojas, lai izveidotu procesu, kurā nodots marķieris tiek verificēts. URI izveides modulis (320) un marķiera izveides modulis (330) ir saistīti un marķieris ir balstīts uz pieprasīto URI. Tas nozīmē, ka marķieris ir unikāls pieprasītajam URI un to nevar izmantot citai straumei. Šī informācija pēc tam tiek nodota atpakaļ klientam, izmantojot moduli (300). Aparatūras ierīces, kas piemērotas izmantošanai par URI izveides moduli un marķiera izveides moduli transakcijas serverī, iekļauj brīvpieejas atmiņu (RAM). Šādi aparatūras komponenti var tikt iegulti URI ģenerēšanas modulī vai marķieru ģenerēšanas modulī vai augšupielādēti. Tiek veidotas programmatūras funkcijas, lai veidotu procesu, kur mediastraumei derīgs URI un lietotājs tiek izvēlēti.

Ilustrētās darbības

Attēlā 4 klients izpilda ielādi (400) un klients tiek ielādēts ar URI un marķieri (410). Klients veic dubultklikšķi uz klienta ikonas (nē) vai tiek palaists ar vides serveri (jā). Ja klientu palaida vides

serveris, klienta komandrindas parametros tiek pieprasīts URI un marķieris. Aplūkojot logu (420) var redzet visas iegādātās (un pašreizējās) datu straumes, kas pieejams aplūkošanai vai cita veida darbībām. Lietotājām būs iespēja izvēlēties datu straumi piekļūvei, veicot dubultklikšķi uz straumes nosaukuma. Ekrāns gaida lietotāja (430) ievadi un lietotājs izvēlās datu straumi vai citu sakopšanas opciju (440). Ja tiek atlasīta sakopšanas opcija, tiek izpildīts lietotāja pieprasījums (450) un atgriežas atpakaļ pie video straumju raidīšanu ar moduli (420).

Ja lietotājs palaiž datu straumi (izvēlas „jā" pozicijā 410), URI un marķieris tiek saglabāts iegādes straumju sarakstā tā, lai tos varētu skatīt atkārtoti vēlāk (460). Tiek atvērts savienojums ar straumēšanas serveri un URI, marķieris un lietotāja informācija tiek nosūtīti uz straumēšanas serveri (470). Straumēšanas serveris apstiprina URI un marķiera kombinācijas derīgumu (vai nederīgumu) (480). Ja marķieris nav derīgs vai tam beidzies termiņš, serveris aizvērs savienojumu un klients būs atgriezts atpakaļ un varēs apskatīt visu skatīšanai pieejamo datu straumju sarakstu. Ja serveris apstiprina URI un marķiera kombinācijas derīgumu, klients sāks saņemt datus no straumēšanas servera un varēs tos aplūkot (490).

Ja datu straume tiek beigta vai lietotājs atlasa citu pieejamu straumēšanas opciju, piemēram, pauzi, stop, iedarbināt vai restartēt (500), straume tiek apturēta un gaida turpmāko lietotāja ievadi. Ja straumēšanas atskaņošana ir beigusies (straumēšana tika pabeigta(510)), process tiek atgrizts pie pieejamo straumju (420) saraksta vai turpina rādīt tekošo datu straumi (490), turpinot lietotāja pieprasījuma (520) izpildi un pēc tam atgriežoties pie straumju rādīšanas (490).

Attēlā 5 un procesā, kas tiek palaists ar straumēšanas serveri, pirmais ir savienojums ar lietotāja datu kontroles moduli (200 un 600), lai atļautu lietotājam izveidot savienojumu ar straumēšanas serveri. Klients nodrošinas URI, marķieri un lietotāja informāciju (610) no lietotāja (470). Straumēšanas serveris nosaka, vai marķieris un URI ir derīgi (620). Ja marķieris nav derīgs vai tam beidzies termiņš, savienojums ar klientu tiks aizvērts (630) ar atbilstošo kļūdas ziņojumu. Ja marķieris ir derīgs, ar klientu tiks saskaņota unikālu šifrēto atslēgu kopa (640). URI tiks atverts un straumēšanas dati tiks nolasīti buferī (650).

Klienta plūsmas vadības modulis (230) nodrošina klientam un straumēšanas serverim plūsmas vadības savienojumu, kas izveidots, lai nodrošinātu, ka datu straume pamet straumēšanas serveri ar tādu pašu ātrumu, kā tā tiek saņemta klienta pusē (660). Tas attiecas uz joslas platuma jautājumiem, kā arī nodrošina, ka klienta atskaņošanas buferis netiek pārkopēts. Tāpēc klienta plūsmas kontroles mehānisms (660) izmanto klienta plūsmas vadības moduli (230), lai iegūtu atgriezenisko saiti no klienta datu bufera (710) un kontrolētu datu straumēšanas ātrumu, lai uzturētu klienta buferi pēc iespējas pilnīgāku. Ja klients šajā brīdī nevar akceptēt vairāk datu, ir jāatgriežas plūsmas vadības modulī kā norāda (670), lai palēninātu vai uz laiku apstatītu datu straumēšanu. Ja klients var pieņemt vairāk datu (680), klienta plūsmas kontrole vispirms noteiks, vai ir vēl straumēšanai paredzētie dati (680). Ja nav straumēšanai paredzēto datu, datu straume var tikt pabeigta un klienta savienojums tiek aiztaisīts ciet (690). Ja ir vēl dati sūtīšanai, dati, kas gaida sūtīšanas buferī tiks šifrēti (700) un jau šifrētie dati tiek nosūtīti klientam (710).

Attēlā 6 ir transakcijas servera scenārijs, kur klients pirmām kārtam savienojas (800) ar transakcijas serveri, piemēram, izmantojot Web lapu. Vienā salikumā transakcijas serveris tiek ieviests ar ASP skriptiem. Taču izgudrojums nav ierobežots tik lielā mērā un būtībā var izmantot jebkuru mehānismu, neietekmējot izgudrojuma aizsardzības apjomu vai būtību. Klients nosūta pieprasījuma URI un lietotāja informāciju (810) izmantojot ASP komandrindas mainīgos, un transakcijas servera lietotāja verifikācijas modulis (310) nosaka pieejamo marķieru laika ierobežojumus un parāda tos lietotājam atlasei. Transakcijas serveris meklē lietotāja informāciju (820) lietotāju verifikācijas moduļa (310) datu bāzē. Lietotāja informācijas meklēšanas piemēri ir, noskaidrot ir vai nav lietotājam autorizācija (piemēram, autorizācijas eksistē saskaņā ar transakcijas serveri) (830). Ja lietotājam nav autorizācijas (840), transakcija tiks atvērta, lai

izveidotu jaunu autorizācijas lapu un iegūtu informāciju no lietotāja (840). Papildus transakcijas servera lietotāja verifikācijas modulis (310) noteiks, vai pieprasītais URI ir bezmaksas (850). Ja par URI ir jāmaksā nauda (860), transakcijas servera lietotāju verifikācijas modulis (310) atskaita naudu no kredītkartes, dati par kuru ir lietotāja datu bāzē. Šis process transakcijas servera URI izveides modulī (320) izveido URI.

Tiklīdz URI tiek nodrošināts, kā arī apmaksāts vai sniegts bezmaksas, marķieru izveides modulī (330) tiek izveidots marķieris (870). Tikko izveidotais marķieris tiks sasaistīts ar URI un attiecīgais laika ierobežojums tiks izvēlēts (880). Visbeidzot klienta ierīcē tiks startēts skatītājs un nosūtīts atpakaļ klienta kopā ar URI un izveidoto marķieri.

Lietotāja komponenti ilustratīvā virtuālajā viedkartē

Klienta komponenti, kas iepriekš aprakstīti saistībā ar 1. attēlu, var tikt izmantoti dažādās klientu sistēmās. Šādas klientu sistēmas var iekļaut ierīces, kas parasti savieno, izmantojot vadu komunikācijas vidi, tādu kā personālo datoru, multiapstrādes sistēmas, mikroprocesora vai programmējamu patērētāja elektroniku, televizora pierīces, interaktīvās televīzijas ierīces, izvēršanas interfeisus un moduļus, tīkla datorus utt. Šādas ierīces var arī iekļaut ierīces, kas parasti savieno, izmantojot bezvadu komunikācijas vidi, piemēram, mobilos telefonus, augstu tehnoloģiju telefonus (smartphones), peidžerus, mazus pārnēsājamus radioaparātus, radio frekvences (RF) ierīces, infrasarkanās ierīces, CB, integrētas ierīces, kas apvieno vienu vai vairākas iepriekš uzskaitītās ierīces, vai faktiski jebkuru mobilu ierīci utt. Līdzīgi, klienta sistēmas, kas var izmantot 1. attēlā paradītus klienta komponentus, var būt jebkura ierīce, kas spēj savienot, izmantojot tādu vadu vai bezvadu komunikācijas vidi, kā plaukstdators (PDA), kabatas personālais dators, portatīvais dators vai jebkura cita ierīce, kas ir aprīkota, lai komunicētu vadu un/vai bezvadu komunikācijas vidē.

Šādas klienta sistēmas var būt konfigurētas tā, lai izmantotu straumētos datus dažādiem nolūkiem, ieskaitot filmu un audio klipu utt. baudīšanai. Vienā salikumā straumētos datos var būt iekļauta vismaz daļiņa datu, kas saistīta ar interaktīvās televīzijas pakalpojumu. Straumētie dati var būt saistīti ar banku aktivitātēm, e-komercijas aktivitātēm utt.

Papildus, 1.attēlā redzamie klienta komponenti var tikt sakārtoti dažādās konfigurācijās un būt saistīti ar dažādo uzbūvju kombinācijām. Piemēram, vienā salikumā klienta komponenti no 1. attēlā var būt sakārtoti klienta sistēmā, kurā ir virtuālā viedkarte (VSC). Papildus klienta komponentus var izmantot saistībā ar interaktīvās televīzijas vidi, izmantojot VSC.

Attēlā 7 ir parādīts tāds VSC izkārtojuma klienta ierīcē viens salikums, kas ir konfigurēts, lai mijiedarbotos ar transakcijas serveri līdzīgā veidā, kā tas tika aprakstīts iepriekš saistībā ar 2. - 6. attēliem. Attēlā 7 paradīta klienta sistēma 7000 var iekļaut daudz vairākus komponentus nekā attēlots. Tomēr parādītie komponenti ir pietiekami, lai parādītu izgudrojuma izmantošanas ilustratīvu salikumu un komponentu sakārtojuma un tipu variācijas var būt izmantoti, neietekmējot izgudrojuma apjomu vai būtību.

Aprakstītas VSC izmantošana iedarbina privātumu (konfidencialitāti), integritāti, laicīgumu, piekļuves kontroli (autorizāciju) un autentifikāciju (identifikāciju), kā arī ātru atjaunošanu, krossaišu kopēšanas aizsardzību vai digitālo tiesību pārvaldību un lielāku ietilpību, pielāgojamību un spēju saistīt ar ierīci, lai nodrošinātu palielinātu drošību.

Kā parādīts attēlā, klientu sistēma 7000 iekļauj klienta ierīci 7002. Klienta ierīce 7002 iekļauj VSC 7004, bojājumu noteikšanu 7006, datu straumes saņemšanas moduli 7170, rādīšanas moduli 7140, lokālās raidīšanas kontroles moduli 7130 un lietotāja interfeisu 7110. VSC 7004 iekļauj komunikācijas un plūsmas kontroles moduļus 7010, drošības ziņojumu vadības ierīci 7012, bojājumu aizsardzību 7014, klienta ievades buferi 7150, marķiera vadības ierīci 7016,

kriptogrāfiskos moduļus 7060, marķieru glabāšanas moduli 7100, atslēgu ģeneratoru 7018 un saistīšanas moduli 7020.

Lietotāja interfeiss 7110 darbojas principiāli līdzīgi lietotāja interfeisam 110, kas ir 1. attēlā. Lietotāja interfeiss 7110 var iekļaut dažādas klienta ievades ierīces, ieskaitot peli, tastatūru, mikrofonu, skārienekrānu, tālvadības ierīci utt., kas ir konfigurēti, lai nodrošinātu spēju atlasīt izvēlēties datu straumi, kā arī sniegt informāciju.

Lokālās raidīšanas kontroles modulis 7130 darbojas principiāli līdzīgi lokālās raidīšanas vadības modulim 130, kas ir 1. attēlā, Lokālās raidīšanas vadības modulis 7130 var būt faktiski jebkura ierīce, programmatūra, programmatūras un aparatūras kombinācija utt., kas ļauj kontrolēt datu rādīšanu un kuram ir iespēja pauzēt, apturēt, iesākt un atsākt datu straumi.

Raidīšanas modulis 7140 darbojas principiāli līdzīgi kā raidīšanas modulis 140, kas ir 1. attēlā. Raidīšanas modulis 7140 uzsāk datu straumes prezentāciju klientam, ieskaitot video datus, audio datus utt. Piemēram, raidīšanas modulis 7140, var iedarbināt interaktīvās televīzijas datu straumes prezentāciju.

Datu straumes saņemšanas modulis 7170 darbojas principiāli līdzīgi datu straumes saņemšanas modulim 170, kas ir 1. attēlā. Datu straumes saņemšanas modulis 7170 ir konfigurēts, lai vadītu datu paketes, kas saistītas ar servera sūtīto datu straumi, saņemšanu. Datu straumes saņemšanas modulis 7170 var papildus būt konfigurēts tā, lai nodrošinātu saņemto datu paketes komunikācijas un plūsmas kontroles modulim 7010.

Marķieru glabāšanas modulis 7100 ir konfigurēts tā, lai darbotos principiāli līdzīgi marķieru glabāšanas modulim 100, kas ir 1. attēlā. Marķieru glabāšanas modulis 7100 ir konfigurēts tā, lai nodrošinātu drošu URI, ar URI saistīto marķieru un marķieru beigu termiņa datu utt. glabāšanu. Pie tam, marķieru glabāšanas modulis 7100 ir papildus konfigurēts tā, lai nodrošinātu drošu lokālu glabāšanu, kas ir cieši saistīta ar klienta ierīci 7002. Marķieru glabāšanas modulis 7100 var tikt ieviests kā fails, mape, datu bāze utt. Saistīšana ar klienta sistēmu var tikt veikta, izmantojot saistīšanas moduli 7020. Lokālā drošība var tikt nodrošināta, izmantojot vairāku veidu šifrēšanu, jaukšanu un arī izmantojot dažādus tīkla resursus.

Saistīšanas modulis 7020 ir konfigurēts tā, lai viennozīmīgi identificētu klienta ierīci 7002, servera sistēmu utt. Vienā salikumā tas tiek panākts, izmantojot pirkstu nospiedumus. Pirkstu nospiedumi var tik izveidoti no katram pirkstu nospiedumam specifiskā elementu kopuma. Šādiem elementiem šeit tiek izmantots termins kores. Katra kore iekļauj pirkstu nospieduma elementu, kas nodrošina informāciju pirkstu nospiedumam, padarot to unikālu salīdzinājumā ar pārējiem. Daži koru paraugi iekļauj aparatūras sērijas numuru, operētājsistēmas versijas numuru, Interneta protokola adresi, fiziskās atmiņas apjomu utt. Katra pirkstu nospiedumā iekļautā kore detalizē sistēmas identitāti, lai to varētu viennozīmīgi identificēt sistēmā. Visu pirkstu nospiedumu kombinācijas var veidot rokas nospiedumu vai sistēmas pirkstu nospiedumu, kas viennozīmīgi identificē personālo datoru, serveri, klienta ierīci, televizora pierīci vai līdzīgu ierīci sistēmā. Katras pirkstu nospiedumu grupas un atsevišķu koru kārtība var ietekmēt sistēmas pirkstu nospiedumu vai plaukstas nospieduma rezultātu. Tas ir, katrs saistīšanas moduļa 7020 lietotājs var ģenerēt unikālu serdeņpirkstu nospiedumu un attiecīgu plaukstas nospiedumu, lai gan izmantotā kores informācija ir vienāda.

Ģenerēta pirkstu nospieduma izmantošana saista VSC 7004 ar specifisku ierīci, tādu kā klienta ierīce 7002, tā, ka tā nedarbosies pareizi, ja tas tiks klonēts vai to mēģinās palaist citā ierīcē. Šī pieeja faktiski ierobežo ierasto hakeru pieeju saistībā ar fiziskās viedkartes pirātismu.

Vienā salikumā VSC 7004 var būt kombinēts ar citu ierīci, tādu kā fiziskā viedkarte, lai papildus palielinātu fiziskās viedkartes drošības identitātes parametrus attiecībā uz pirkstu nospieduma

ierīci, uzturot VSC 7004 pielāgojamību un jaudu. To var īstenot, piemēram, sistēmā, kurā ierīces identitāte ir sākotnēji vāja, kur cena un/vai fiziskās kartes vai citas ierīces ērtums var nebūt tik svarīgi.

Komunikācijas un plūsmas vadības modulis 7010 ir konfigurēts tā, lai iedarbinātu komunikāciju un datu plūsmas kontroli starp VSC 7004 un transakcijas un straumēšanas serveriem. Komunikācijas un plūsmas vadības modulis 7010 kā tāds, var veikt darbības līdzīgas dažām uz 1. attēla redzama straumes kontroles protokola moduļa (120) darbībām. Tas ir, komunikācijas un plūsmas kontroles modulis 7010 var iedarbināt sākotnējo savienojumu ar serveri un iedarbinot pieprasītā URI, marķiera un lietotāja informācijas nodošanu.

Komunikācijas un plūsmas kontroles modulis 7010 var arī iedarbināt datu plūsmas no servera kontroli, lai nodrošinātu, ka plūsmas ātrums uztur pilnu klienta buferi (piemēram, klienta ievades buferi 7150) principiāli līdzīgi straumēšanas kontroles protokola modulim 120, kas ir 1. attēlā Komunikācijas un plūsmas kontroles modulis 7010 to var darboties arī tā, ka, piemēram, pārraudzīt dažādus parametrus, kā datu saņemšanas ātrumu, tīkla statistiku, ievades bufera statistiku utt. Komunikācijas un plūsmas vadības modulis 7010 kā tāds var iedarbināt ievades bufera 7150 pieprasījumu ar nolūku noteikt procentus, piemēroto ātrumu, bufera atlikušā apjoma procentuālo radītāju utt. Komunikācijas un plūsmas kontroles modulis 7010 pēc tam var nodrošināt serveri ar plūsmas vadības metriku, balstoties uz pārraudzītajiem raksturlielumiem šifrētā vai nešifrētā veidā. Ja informācija ir nodrošināta šifrēta veidā, komunikācijas un plūsmas kontroles modulis 7010 var izmantot drošības ziņojumu pārvaldnieku 7012, lai nodrošinātu, ka informācija ir droša.

Drošības ziņojumu pārvaldnieks 7012 ir konfigurēts tā, lai nodrošinātu drošu ziņapmaiņas vidi. Lai gan tas nav ilustrēts, drošības ziņojumu pārvaldnieks 7012 mijiedarbojas ar vairākiem citiem VSC 7004 pieprasītiem komponentiem, lai nodrošinātu pušu savstarpējas autentifikācijas izpildi un ziņojumu konfidencialitāte uzturēšanu.

Marķieru vadības ierīce 7016 ir konfigurēta, lai vadītu marķieru un līdzīgu objektu saņemšanu, glabāšanu, sūtīšanu un interpretāciju. Marķieru vadības ierīce 7016 ka tāda var veikt dažādas darbības, kas ir saistītas ar straumēes kontroles protokola moduli 120, kas ir 1. attēlā. Piemēram, marķieru vadības ierīce 7016 var nodot serverim pieprasīto URI, marķieri un lietotāja informāciju. Marķieru vadības ierīce 7016 var arī ģenerēt ar serveri šifrētu atslēgu kopu, izmantojot kriptogrāfisko moduli 7060 un/vai atslēgu ģeneratoru 7018. Pie tam marķieru vadības ierīce 7016 var izmantot drošības ziņojumu pārvaldnieku 7012, lai iedarbinātu drošu komunikāciju starp serveri un klienta ierīci 7002.

Marķieri ir īsi aprakstīti iepriekš. Vienā salikumā tomēr marķieris var iekļaut ciparu sertifikātu, kurā var būt iekļauta identifikācijas informācija, šifrēšanas atslēgas utt., saistītas ar tādiem kā sertificēšanas speciālistu. VSC 7004 izmantojama marķiera struktūra nodrošina unikālu pilnvaru ķēdes koncepciju, kura var paplašināt biznesa modeli ārpus tam, kas parasti tiek atbalstītās ar tradicionālo sertifikācijas speciālista modeli. Taču izgudrojums nav tik ierobežots un marķiera struktūra var izmantot faktiski jebkuru struktūru, kas ir konfigurēta tā, lai saistītu lietotāja atļaujas ar konkrētu datu straumi.

Kriptogrāfijas modulis 7060 ir paredzēts, lai nodrošinātu kriptogrāfijas mehānismu šifrēšanas, atšifrēšanas, ciparu parakstu, atslēgu ģenerēšanas utt. veikšanai. Piemēram, kriptogrāfijas modulis 7060 var iekļaut asimetrisku kriptogrāfijas mehānismus, kas konfigurēti, lai nodrošinātu kriptogrāfijas darbības, kas balstītas uz publisku/privātu atslēgu. Publiskas/privātas kriptogrāfijas darbības ietver atslēgas ģenerēšanu, ciparu parakstus, šifrēšanu, atšifrēšanu un integritātes pārbaudi. Kriptogrāfijas modulis 7060 iedarbina arī drošu šifrēšanas atslēgu apmaiņu, izmantojot marķieru vadības ierīci 7016 un drošības ziņojumu vadības ierīci 7012.

Kriptogrāfijas modulis 7060 papildus spēj saņemt drošu saturu no komunikāciju un plūsmas vadības moduļa 7010, atšifrēt drošu saturu un sūtīt atšifrēto saturu lietotāja ievades buferim 7150.

Lietotāja ievades buferis 7150 darbojas principiāli līdzīgi lietotāja ievades buferim 150, kas ir 1. attēlā. Lietotāja ievades buferis 7150 ir konfigurēts, lai iekļautu straumēšanas buferi. Ir svarīgi atzīmēt, ka, lai gan lietotāja ievades buferis 7150 ir attēlots kopā ar VSC 7004, izgudrojums nav tik ļoti ierobežots. Piemēram, lietotāja ievades buferis 7150 var atrasties lietotāja ierīcē 7002 un ārpus VSC 7004.

Kriptogrāfijas modulis 7060 ir konfigurēts tā, lai nodrošinātu kriptogrāfijas atslēgu dažādību, tai skaitā simetriskas vai privātas atslēgas, asimetriskas vai publiskas atslēgas utt. Lai gan kriptogrāfijass modulis 7060 var izmantot faktiski jebkuru kriptogrāfijas mehānismu, vienā salikumā, kriptogrāfijas modulis 7060 simetriskai kriptogrāfijai izmanto AES. Citā salikumā kriptogrāfijas modulis 7060 asimetriskām kriptogrāfijas darbībām izmanto RSA.

Atslēgu ģenerators 7018 ir konfigurēts kriptogrāfiskā moduļa 7060 izmantošanai, lai iedarbinātu kriptogrāfijas atslēgu ģenerēšanu. Šādu ģenerēšanu var izmantot, piemēram, ātrs atjaunošanas mehānisms, pie kam jaunu atslēgu ģenerēšana tiek veikta īsā laika periodā, salīdzinājumā ar parasto fiziskās viedkartes atslēgas aizvietošanas mehānismu. Vienā salikumā atslēgu ģenerators 7018 var iedarbināt jaunu atslēgu ģenerēšanu dažu stundu laikā dažu dienu, nedēļu vai pat mēnešu vietā. Vienā salikumā, lai papildus noslēptu iespējamo uzbrukuma vietu, tiek izmantota dinamiskā ātrā atjaunošana, kur atslēgu utt. ģenerēšanu veic pēc nejaušības principa, lai izveidotu neparedzamu vidi. Citā salikumā šādu dinamisko ātro atjaunošanu var izmantot, lai aizvietotu vairākus programmatūras komponentus, kas var turpmāk minimizēt uzbrukumus. Šādas ātrās atjaunošanas izmantošana iedarbinā VSC 7004 izmantošanu dažādās situācijās, ieskaitot banku operācijās, uzņēmuma drošību, e-komerciju un programmu izplatīšanas studijas..

Ielaušanas fakta atklāšanu 7006 un aizsardzību pret ielaušanos 7014 var dažādi izmantot lietotāja sistēmā 7000, lai nodrošinātu augstu infrastruktūras drošību. Parasti noteikta līmeņa aizsardzība pret ielaušanos vai pretspēks var būt nodrošināti kā VSC 7004 programmatūras un/vai aparatūras daļa. Kā attēlots, VSC 7004 ietver aizsardzību pret ielaušanos 7014, lai nodrošinātu pretspēku vai aizsardzību pret ielaušanos un pret līdzīgām hakeru darbībām. Šī aizsardzība var papildus iekļaut aģentus, kas ir konfigurēti vairāku darbību veikšanai, ieskaitot iekšshēmas emulatora noteikšanu, atkļūdotāja noteikšanu, atkļūdotāja pretspēku, atmiņas vietas laušanas noteikšanu un aizsardzību, kā arī līdzīgā līmeņa pirātisko darbību noteikšanu un aizsardzību.

Ielaušanas noteikšana 7006 ir konfigurēta tā, lai identificētu ielaušanos no citām sistēmām, tādām kā klienta ierīcē 7002 un līdzīgām. Piemēram, interaktīvās televīzijas vidē ir iespējams izvietot ielaušanās noteikšanu tīklā, lai kontrolētu virtuālās viedkartes un/vai tās dažādu komponentu dublēšanas mēģinājumus. Ielaušanas noteikšana 7006 var papildus nodrošināt drošu laika avotu, tādējādi novēršot atkārtotas atskaņošanas uzbrukumus.

Operatīvi VSC 7004 var darboties līdzīgi kā aprakstīts 4. attēlā. Piemēram, kā tika aprakstīts 4. attēlā, klients tiek ielādēts ar URI un marķieri (skat. bloku 400 4. attēlā). Šī darbība var parādīties 7. attēlā, mijiedarbojoties ar komunikāciju un plūsmas kontroles moduli 7010, kā arī lietotāja interfeisu 7110, rādīšanas moduli 7140 utt.

Ja lietotājs palaiž datu straumi lemējblokā 410 saskaņā ar 4. attēlu, process virzīsies uz bloku 460, kur URI un marķieris tiek saglabāti, izmantojot marķieru vadības ierīci 7016 un marķieru glabāšanas moduli 7100. Pārvietojoties blakus blokam 470, komunikāciju un plūsmas kontroles modulis 7010 savienojumā ar marķieru vadības ierīci 7016 nosūta URI, marķiera un lietotāja informāciju straumēšanas serverim.

Ja lemējblokā 480 serveris apstiprina derīgu URI un marķiera kombināciju, process turpinās ar bloku 490 saskaņā ar 4. attēlu, kur dati tiek straumēti no straumēšanas servera. Šādu datu straumējumu var saņemt datu straumes saņemšanas modulis 7170 un nosūtīt uz komunikāciju un plūsmas kontroles moduli 7010, kur saņemtās straumēšanas atšifrēšana var notikt, izmantojot kriptogrāfiskos moduļus 7060. Atšifrētā datu straume pēc tam var tik ievietota lietotāja ievades buferī 7150 ar tādu ātrumu, kura nepieciešama, lai klienta buferis tiktu uzturēts pilns. Komunikācijas un plūsmas kontroles modulis 7010 sūta plūsmas kontroles informāciju datu straumēšanas procesā, lai nodrošinātu klienta buferi pilnu.

Iepriekš izklāstīta izgudrojuma specifikācija, piemēri un dati nodrošina pilnīgu izgudrojuma īstenošanas un izmantošanas variantu aprakstu. Tā kā izgudrojumam ir iespējami dažādi realizācijas varianti, kas neietekmē izgudrojuma būtību un spējas, no izgudrojuma izrietošās tiesības ir formulētas šādas zemāk uzskaitītas pretenzijās..

PRETENZIJAS

1. Sistēma datu straumes komunicēšanai tīklā, kas ietver:
   - lietotāja ierīci, kas konfigurēta darbību veikšanai, iekļaujot:
     - datu straumes pieprasījuma veikšanu;
   - virtuālās viedkartes, kas saistītas ar lietotāja ierīci, pie kam virtuālā viedkarte, kas konfigurēta darbību veikšanai, iekļauj:
     - ar pieprasīto datu straumi saistīta marķiera nosūtīšanu;
     - pieprasītās datu straumes saņemšanu, kur pieprasītā straume ir šifrēta, un
     - plūsmas vadības metrikas, kas saistīta ar datu straumi, nodrošināšanu un
   - straumes serveri, kas konfigurēts darbību veikšanai, iekļaujot:
     - pieprasītās datu straumes marķiera apstiprināšanu un, ja pieprasītās datu straumes marķieris ir derīgs,
       - šifrēto datu straumes pārsūtīšanu uz virtuālo viedkarti un
       - plūsmas vadības metrikas no virtuālās viedkartes izmantošanu, tostarp, lai vadītu šifrētās datu straumes plūsmu pa tīklu, uzturot pilno ar virtuālo viedkarti saistīto buferi.

2. Sistēma saskaņā ar 1. pretenziju, kur virtuālā viedkarte papildus ietver marķiera vadības ierīci, kas konfigurēta, lai ar straumēšanas serveri saskaņotu marķieri.

3. Sistēma saskaņā ar 1. pretenziju, kur pieprasītās datu straumes marķiera apstiprināšana papildus ietver marķiera identifikatora apstiprināšanu, kas saistīts ar datu straumes atrašanās vietu, kurai piemīt piešķirtais identifikators.

4. Sistēma saskaņā ar 1. pretenziju, kur virtuālā viedkarte papildus ietver plūsmas vadības moduli, kas konfigurēts, lai pārraudzītu vismaz vienu tīkla statistiku un bufera raksturlielumu, lai noteiktu plūsmas vadības metriku.

5. Sistēma saskaņā ar 1. pretenziju, kur virtuālā viedkarte papildus iekļauj saistīšanas moduli, kas konfigurēts, lai unikāli saistītu virtuālo viedkarti ar lietotāja ierīci.

6. Sistēma saskaņā ar 1. pretenziju, kur straumes serveris ir konfigurēts, lai veiktu papildus darbības, iekļaujot šifrēšanas atslēgu saskaņošanu ar virtuālo viedkarti un to izmantotu pieprasītās datu straumes šifrēšanai.

7. Sistēma saskaņā ar 6. pretenziju, kur virtuālā viedkarte papildus iekļauj marķiera vadības ierīci, kas ir konfigurēta, lai mijiedarbotos ar straumes serveri šifrēšanas atslēgu saskaņošanaas nolūkā.

8. Sistēma saskaņā ar 7. pretenziju, kur virtuālā viedkarte papildus iekļauj marķieru glabāšanas moduli, kas ir konfigurēts, lai glabātu vismaz vienu lietotāja informāciju, URI un šifrēšanas atslēgas.

9. Sistēma saskaņā ar 1. pretenziju, kur marķieris papildus ietver ciparu sertifikātu.

10. Sistēma saskaņā ar 1. pretenziju, kur lietotāja ierīcei datu straume tiek piegādāta tā, ka tā ir skatāma iepriekš noteiktu skaitu reižu.

11. Modulēts datu signāls datu straumes pārvaldībai tīklā, pie kam modulētais datu signāls ietver:
    - datu straumes pieprasīšanu no lietotāja, kuram ir virtuālā viedkarte;
    - marķiera, kas saistīts ar pieprasīto datu straumi, nodrošināšanu ar virtuālo viedkarti;
    - pieprasītās datu straumes marķiera derīguma novērtēšanu, pie tam, ja pieprasītās datu straumes marķieris ir derīgs, modulētais signāls ietver:
        - šifrēšanas atslēgas saskaņošanu ar virtuālo viedkarti;
        - datu plūsmas šifrēšanu, tiklīdz datu straume tiek sūtīta lietotājam, pie kam datu straume tiek šifrēta, izmantojot saskaņoto šifrēšanas atslēgu;
        - plūsmas metriskas vadību, kas saistīta ar šifrēto datu straumes nodrošināšanu, izmantojot virtuālo viedkarti, un
        - lietotājām pa līklu sūtītās šifrēto datu straumes plūsmas ātruma vadību, izmantojot serveri, pie kam serveris izmanto plūsmas kontroles metriku, tostarp, lai vadītu šifrēto datu straumes plūsmas ātrumu un lai uzturētu lietotāja buferi būtībā pilnu.

12. Modulēts datu signāls saskaņā ar 11. pretenziju, kur datu straume ir konfigurēta vienreizējai skatīšanai.

13. Modulēts datu signāls saskaņā ar 11. pretenziju, kur plūsmas ātruma vadība papildus iekļauj šifrēto datu straumes pārsūtīšanu lietotājam ar tādu pašu ātrumu, kā šifrēto datu straumi saņem lietotājs.

14. Modulēts datu signāls saskaņā ar 11. pretenziju, kur plūsmas vadības metrikas nodrošināšana papildus ietver vismaz vienas tīkla statistikas un lietotāja bufera raksturlieluma pārraudzīšanu.

15. Lietotāja ierīce datu straumes saņemšanai pa tīklu, kas iekļauj:
    - lietotāja interfeisu, kas ir konfigurēts darbību veikšanai, ieskaitot datu straumes pieprasījuma veikšanu, un
    - virtuālo viedkarti, kas saistīta ar lietotāja interfeisu un ir konfigurēta, lai veiktu darbības, ieskaitot:
        - marķiera, kas saistīts ar pieprasīto datu straumi, saskaņošanu;
        - marķiera izmantošanu, lai veiktu datu straumes pieprasījuma apstiprināšanu un, ja pieprasījums ir apstiprināts, datu straumes saņemšanu no servera, kas konfigurēts, lai piegādātu datu straumi ar tādu plūsmas ātrumu, kas lietotāja ierīcē uztur būtībā pilnu lietotāja buferi, un
        - metrikas nodrošināšanu serverim, kas serverim ir jāizmanto, lai datu straumes plūsmas ātrumu vadītu tā, ka lietotāja buferis būtībā tiek uzturēts pilns.
16. Lietotāja ierīce saskaņā ar 15. pretenziju, kur lietotāja interfeiss ir konfigurēts tā, lai veiktu papildus darbības, ieskaitot lietotāja izvēlētā laika limita ievērošanu datu straumes piekļuvei, lai to piegādātu serverim, pie kam lietotāja izvēlētais laika limits ir saistīts ar apstiprināto marķieri tā, ka piekļuve datu straumei tiekt liegta pēc laika limita beigām.
17. Lietotāja ierīce saskaņā ar 15. pretenziju, kur marķieris iekļauj lietotāja atļaujas pieprasītajai datu straumei.
18. Lietotāja ierīce saskaņā ar 17. pretenziju, kur lietotāja informācija iekļauj informāciju par lietotāja reģistrāciju.
19. Lietotāja ierīce saskaņā ar 15. pretenziju, kur marķieris iekļauj lietotāja izvēlēto laika limitu piekļūšanai pie datu straumes, pie kam piekļuve pie datu straumes tiek liegta pēc lietotāja izvēlētā laika limita beigām.
20. Lietotāja ierīce saskaņā ar 15. pretenziju, kur saņemtā datu straume ir šifrēta, izmantojot vismaz vienu no DES, Triple-DES un AES šifrēšanas iespējām.
21. Lietotāja ierīce saskaņā ar 15. pretenziju, kur virtuālā viedkarte ir saistīta tikai ar lietotāja ierīci.

22. Lietotāja ierīce saskaņā ar 15. pretenziju, kur virtuālā viedkarte papildus iekļauj aizsardzības moduli pret noziedzīgo izmantošanu, kas ir konfigurēts, lai noteiktu virtuālās viedkartes noziedzīgu izmantošanu un aizsargātu no tās.
23. Lietotāja ierīce saskaņā ar 15. pretenziju, kur virtuālā viedkarte iekļauj lietotāja buferi.
24. Metode datu straumes komunikācijai pa tīklu, kas iekļauj:
    - datu straumes pieprasīšanu;
    - virtuālās viedkartes izmantošanu, kas ir saistīta ar lietotāja ierīci, lai saskaņotu marķieri, kas saistīts ar pieprasīto datu straumi;
    - saskaņotā marķiera izmantošanu, lai veiktu datu straumes pieprasījuma apstiprināšanu;
    - ja pieprasījums ir derīgs, datu straumes saņemšanu no servera, kas ir konfigurēts datu straumes piegādei ar tādu plūsmas ātrumu, kas uztur lietotāja buferi būtībā pilnu, un
    - metrikas nodrošināšanu, izmantojot virtuālo viedkarti, lai to varētu izmantot serveris, tostarp, lai vadītu datu straumes plūsmas ātrumu tā, ka lietotāja buferis būtībā tiek uzturēts pilns.
25. Metode saskaņā ar 24. pretenziju, kas papildus iekļauj marķiera vadības ierīces izmantošanu, kas savienota ar virtuālo viedkarti, lai mijiedarbotos ar serveri šifrēšanas atslēgu saskaņošanai, kas pielietojamas datu straumes šifrēšanai, tiklīdz datu straume tiek sūtīta uz lietotāja ierīci.
26. Metode saskaņā ar 24. pretenziju, kur virtuālā viedkarte papildus iekļauj marķieru glabāšanas moduli, kas ir konfigurēts, lai glabātu vismaz vienu lietotāja informāciju, marķieri, URI un šifrēšanas atslēgas.
27. Iekārta datu straumes saņemšanai pa tīklu, kas ietver:
    - datu straumes pieprasīšanas ierīci;
    - marķieri, kas savienots ar pieprasītās datu straumes saskaņošanas ierīcēm, pie kam marķieris tiek izmantots, lai veiktu pieprasījuma apstiprināšanu un pieņemtu datu straumi;
    - pieprasītās datu straumes saņemšanas ierīci, ja pieprasījums ir derīgs, pie kam pieprasītā straume ir šifrēta;
    - ierīci, kas nodrošina plūsmas kontroles metriku, saistītu ar saņemto datu straumi,
    - šifrēto datu straumes saņemšanas ierīci no servera vadītas plūsmas veidā, pie kam serveris ir konfigurēts tā, lai izmantotu plūsmas vadības metriku, tostarp, lai vadītu šifrēto datu plūsmas nosūtīšanu pa tīklu un lai iekārtā būtībā uzturētu pilnu buferi.

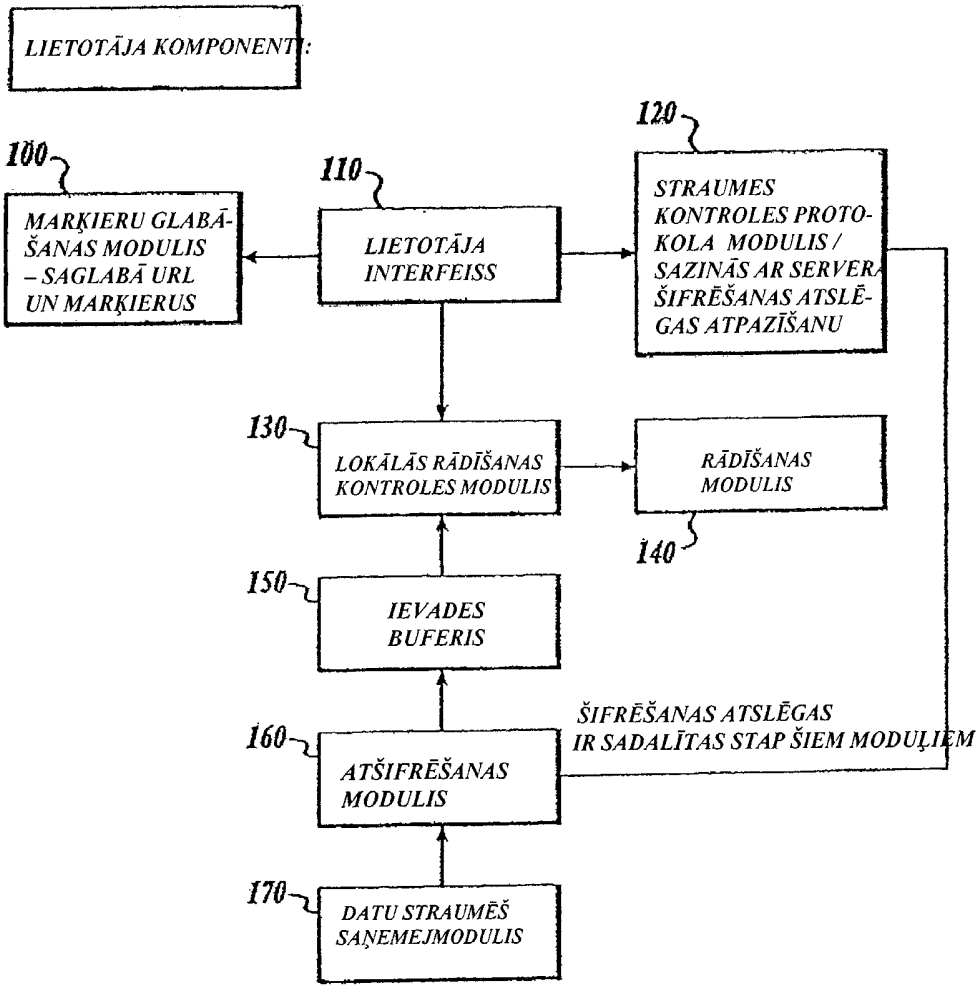
LIETOTĀJA KOMPONENTI:
100
MARĶIERU GLABĀŠANAS MODULIS – SAGLABĀ URL UN MARĶIERUS
110
LIETOTĀJA INTERFEISS
120
STRAUMES KONTROLES PROTOKOLA MODULIS / SAZINĀS AR SERVERA ŠIFRĒŠANAS ATSLĒGAS ATPAZĪŠANU
130
LOKĀLĀS RĀDĪŠANAS KONTROLES MODULIS
RĀDĪŠANAS MODULIS
140
150
IEVADES BUFERIS
160
ATŠIFRĒŠANAS MODULIS
ŠIFRĒŠANAS ATSLĒGAS IR SADALĪTAS STAP ŠIEM MODUĻIEM
170
DATU STRAUMĒŠ SAŅEMEJMODULIS

FIG. 1

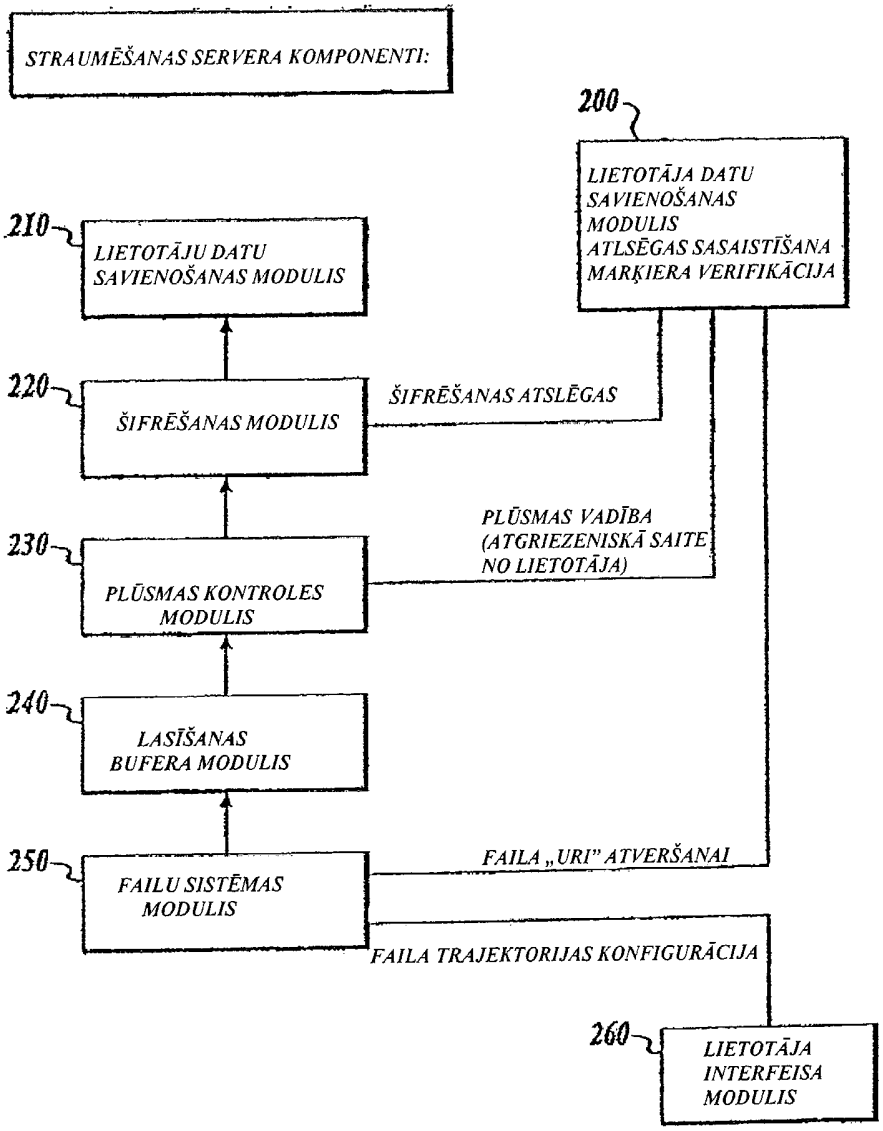
STRAUMĒŠANAS SERVERA KOMPONENTI:
200
LIETOTĀJA DATU SAVIENOŠANAS MODULIS ATLSĒGAS SASAISTĪŠANA MARĶIERA VERIFIKĀCIJA
210
LIETOTĀJU DATU SAVIENOŠANAS MODULIS
220
ŠIFRĒŠANAS MODULIS
ŠIFRĒŠANAS ATSLĒGAS
230
PLŪSMAS KONTROLES MODULIS
PLŪSMAS VADĪBA (ATGRIEZENISKĀ SAITE NO LIETOTĀJA)
240
LASĪŠANAS BUFERA MODULIS
250
FAILU SISTĒMAS MODULIS
FAILA „URI" ATVERŠANAI
FAILA TRAJEKTORIJAS KONFIGURĀCIJA
260
LIETOTĀJA INTERFEISA MODULIS

FIG. 2

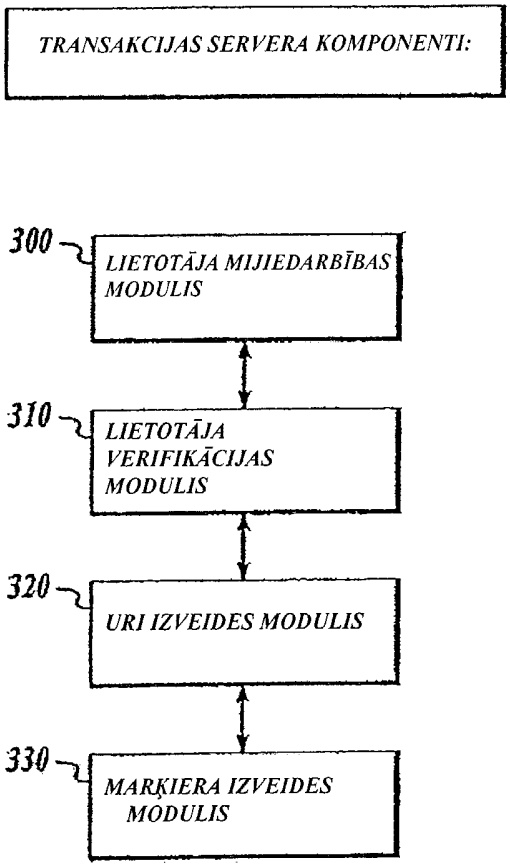
TRANSAKCIJAS SERVERA KOMPONENTI:
300
LIETOTĀJA MIJIEDARBĪBAS MODULIS
310
LIETOTĀJA VERIFIKĀCIJAS MODULIS
320
URI IZVEIDES MODULIS
330
MARĶIERA IZVEIDES MODULIS

FIG. 3

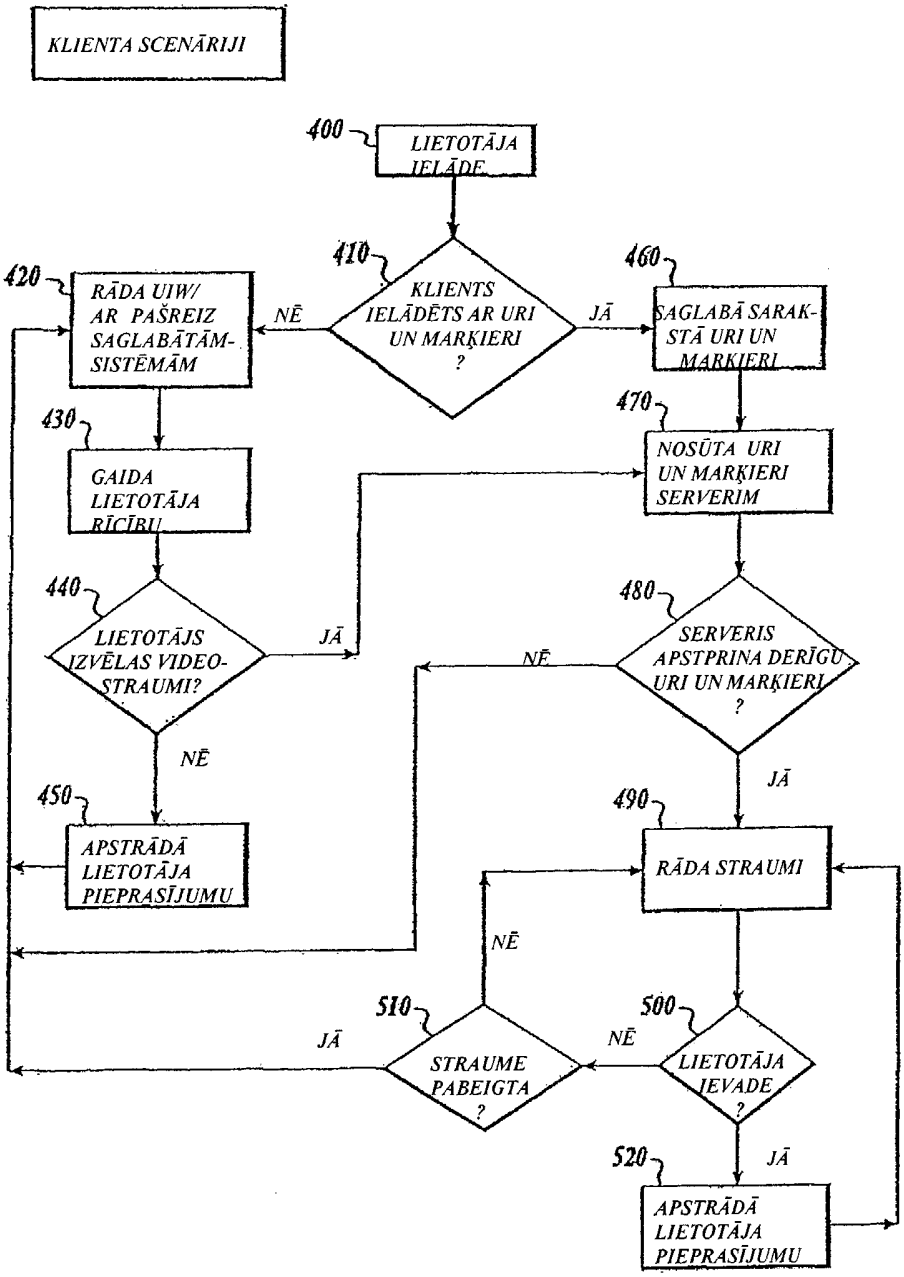
KLIENTA SCENĀRIJI
400
LIETOTĀJA IELĀDE
410
KLIENTS IELĀDĒTS AR URI UN MARĶIERI ?
NĒ
JĀ
420
RĀDA UIW/ AR PAŠREIZ SAGLABĀTĀM-SISTĒMĀM
460
SAGLABĀ SARAKSTĀ URI UN MARĶIERI
430
GAIDA LIETOTĀJA RĪCĪBU
470
NOSŪTA URI UN MARĶIERI SERVERIM
440
LIETOTĀJS IZVĒLAS VIDEO-STRAUMI?
JĀ
NĒ
480
SERVERIS APSTPRINA DERĪGU URI UN MARĶIERI ?
NĒ
JĀ
450
APSTRĀDĀ LIETOTĀJA PIEPRASĪJUMU
490
RĀDA STRAUMI
NĒ
510
STRAUME PABEIGTA ?
JĀ
500
LIETOTĀJA IEVADE ?
NĒ
JĀ
520
APSTRĀDĀ LIETOTĀJA PIEPRASĪJUMU

FIG. 4

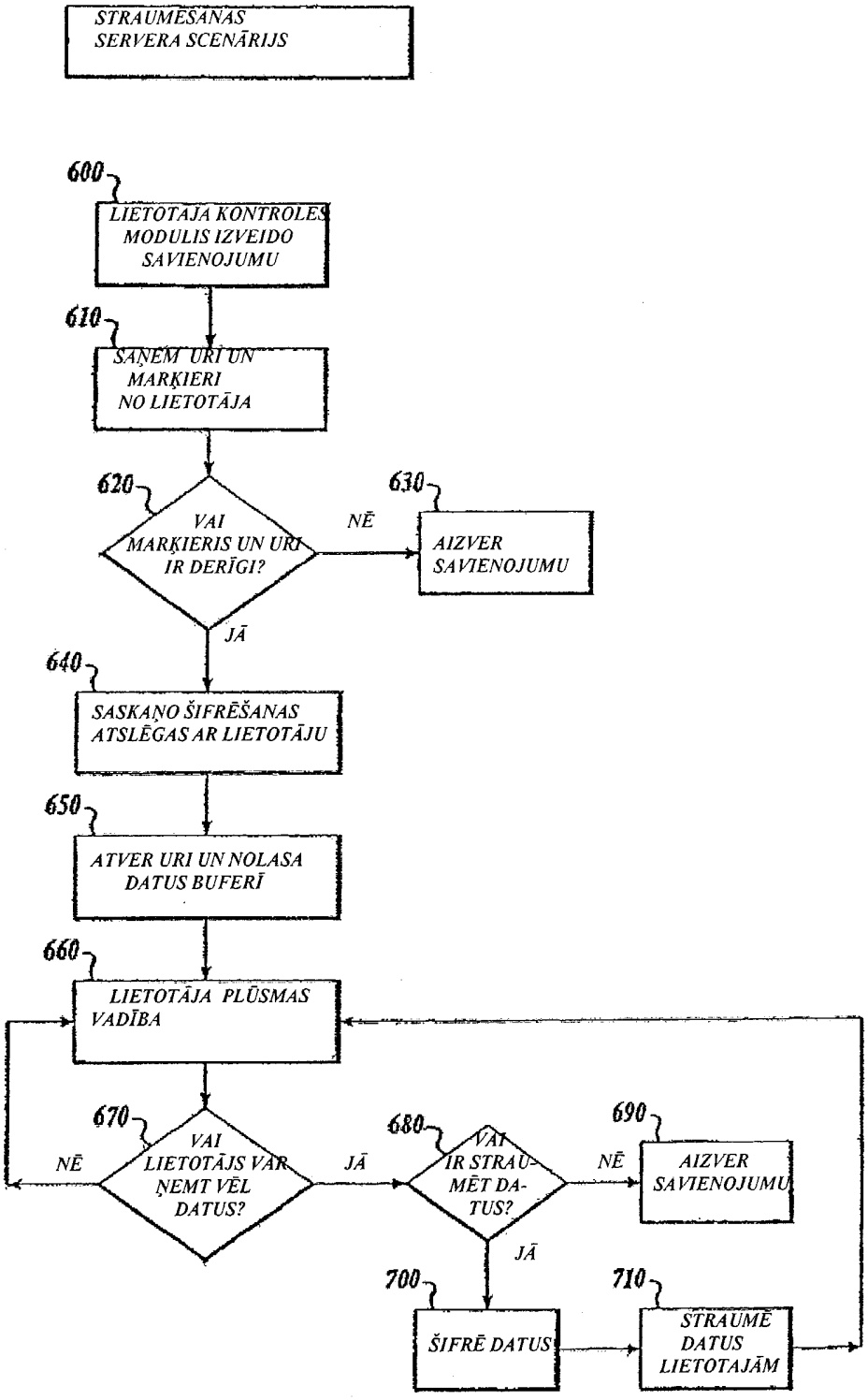
STRAUMĒŠANAS SERVERA SCENĀRIJS
600
LIETOTĀJA KONTROLES MODULIS IZVEIDO SAVIENOJUMU
610
SAŅEM URI UN MARĶIERI NO LIETOTĀJA
620
VAI MARĶIERIS UN URI IR DERĪGI?
NĒ
630
AIZVER SAVIENOJUMU
JĀ
640
SASKAŅO ŠIFRĒŠANAS ATSLĒGAS AR LIETOTĀJU
650
ATVER URI UN NOLASA DATUS BUFERĪ
660
LIETOTĀJA PLŪSMAS VADĪBA
670
VAI LIETOTĀJS VAR ŅEMT VĒL DATUS?
NĒ
JĀ
680
VAI IR STRAUMĒT DATUS?
NĒ
690
AIZVER SAVIENOJUMU
JĀ
700
ŠIFRĒ DATUS
710
STRAUMĒ DATUS LIETOTAJĀM

FIG. 5

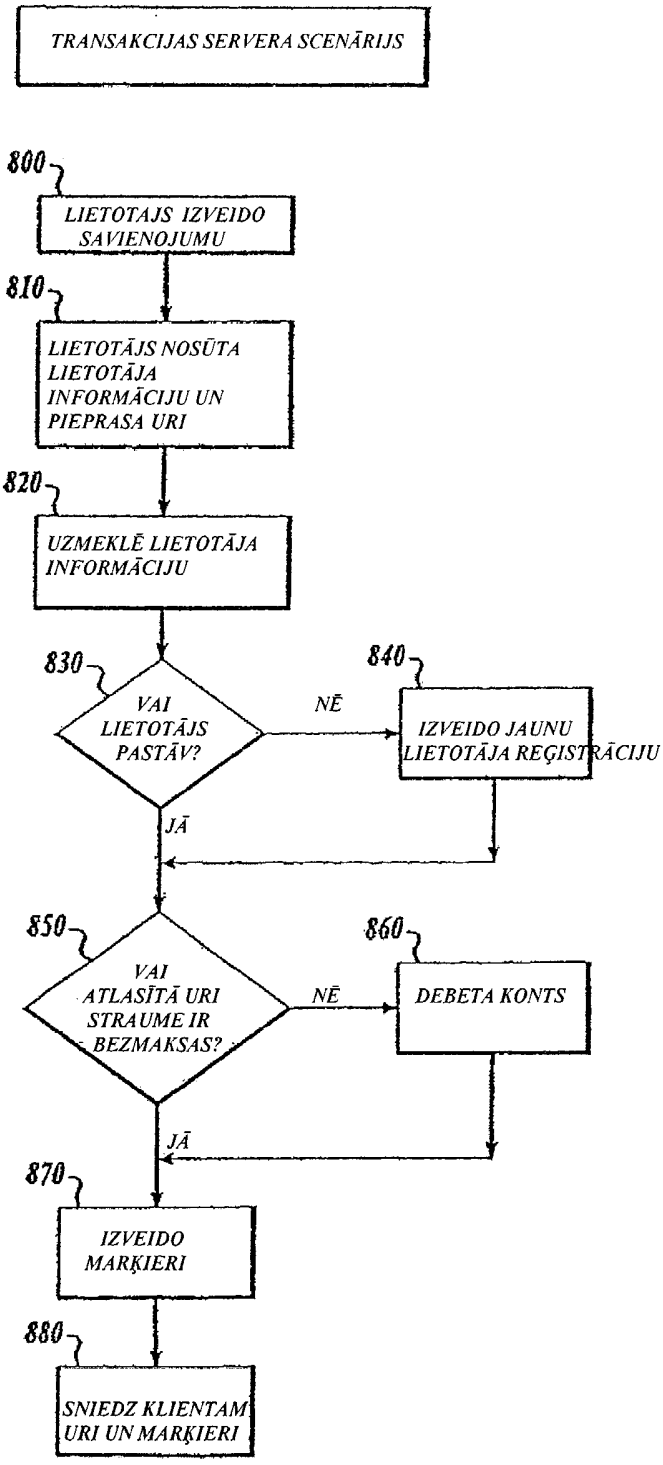
TRANSAKCIJAS SERVERA SCENĀRIJS
800
LIETOTAJS IZVEIDO SAVIENOJUMU
810
LIETOTĀJS NOSŪTA LIETOTĀJA INFORMĀCIJU UN PIEPRASA URI
820
UZMEKLĒ LIETOTĀJA INFORMĀCIJU
830
VAI LIETOTĀJS PASTĀV?
NĒ
840
IZVEIDO JAUNU LIETOTĀJA REĢISTRĀCIJU
JĀ
850
VAI ATLASĪTĀ URI STRAUME IR BEZMAKSAS?
NĒ
860
DEBETA KONTS
JĀ
870
IZVEIDO MARĶIERI
880
SNIEDZ KLIENTAM URI UN MARĶIERI

FIG. 6

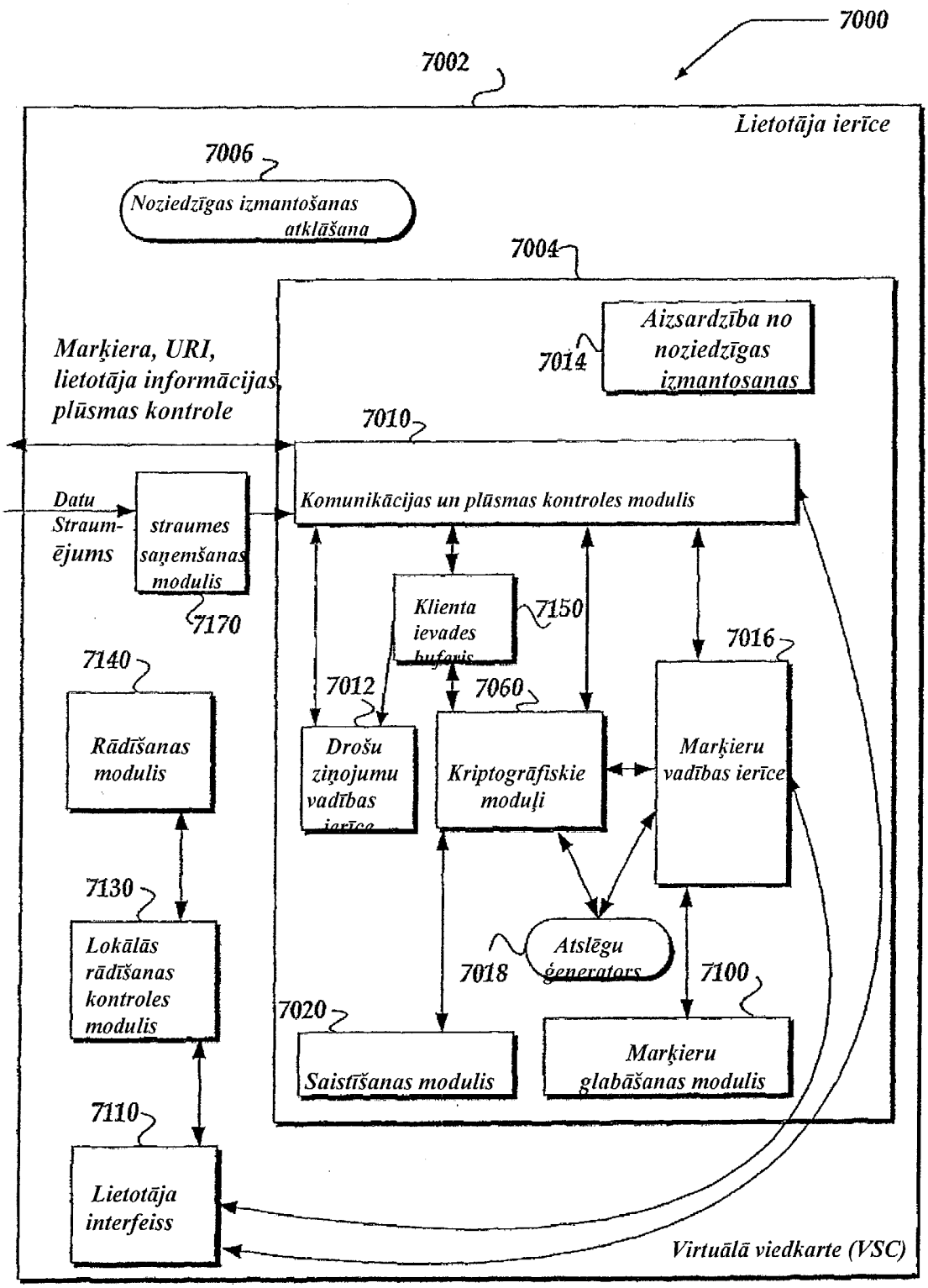
7000
7002
Lietotāja ierīce
7006
Noziedzīgas izmantošanas atklāšana
7004
Aizsardzība no noziedzīgas izmantošanas
7014
Marķiera, URI, lietotāja informācijas, plūsmas kontrole
7010
Komunikācijas un plūsmas kontroles modulis
Datu Straumējums
straumes saņemšanas modulis
7170
Klienta ievades buferis
7150
7016
7140
7012
7060
Rādīšanas modulis
Drošu ziņojumu vadības ierīce
Kriptogrāfiskie moduļi
Marķieru vadības ierīce
7130
Lokālās rādīšanas kontroles modulis
Atslēgu ģenerators
7018
7100
7020
Saistīšanas modulis
Marķieru glabāšanas modulis
7110
Lietotāja interfeiss
Virtuālā viedkarte (VSC)

FIG. 7