

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Erik-Martin Feldberg 213462IACB

Veebibrauserite turvalisus ja AI

Bakalaureusetöö

Juhendaja: Vladimir Viies

Doktorikraad

Tallinn 2024

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Erik-Martin Feldberg

05.05.2024



BAKALAUREUSETÖÖ ÜLESANDEPÜSTITUS

Kuupäev: 01.02.2024

Üliõpilase ees- ja perekonnanimi: Erik-Martin Feldberg

Üliõpilaskood: 213462IACB

Lõputöö teema: Veebibrauserite turvalisus ja AI

Juhendaja: Vladimir Viies

Kaasjuhendaja:

Lahendatavad küsimused ning lähtetingimused:

- Veebibrauserid ja nende turvalisus
 - Töökäigus saadud tulemuste ja AI soovitude võrdlus
- Turvaliseima brauseri soovitamine vastavalt kasutusele

Lõpetaja allkiri
(*digitaalselt allkirjastatud*)

Annotatsioon

Antud töö eesmärk on koostada metoodika turvaliseima brauseri valikuks eri kasutusvaldkondade jaoks Internetis. Töös koostatud metoodikat on kasutatud näitena kolme kasutusvaldkonna jaoks brauseri valimisel.

Iga kasutusvaldkonna jaoks turvaliseima veebibrauseri välja selgitamiseks võrreldakse viite eri brauserit. Turvalisuse hindamiseks kontrollitakse iga brauseri seadete olemasolu, jooksutatakse teste ning võrreldakse tulemusi. Vastavalt turvalisus- ja privaatsusseadete olemasolule ning testimistulemustele pakutakse välja sobivaim brauser. Saadud testimistulemusi võrreldakse tehisintellekti poolt antud soovitustega.

Töö lõpus selgub, et kasutusvaldkondade jaoks turvalisim brauser on sama, kuid erineb tehisintellekti soovitustest.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 28 leheküljel, 3 peatükki, 14 joonist, 9 tabelit.

Abstract

The Safety of Web Browsers and AI

The purpose of this work is to develop a methodology for selecting the safest browser for different areas of use on the Internet. The methodology compiled in this work has been used as an example for selecting a browser for three areas of use.

To find out the safest web browser for each area of use, five different browsers are compared. For the assessment of security, the existence of each browser's settings are checked, tests are run, and the results are compared. Based on the availability of security and privacy settings and test results, the most suitable browser is suggested. The test results obtained are compared with the recommendations given by Artificial Intelligence.

At the end of the work, it turns out that the safest browser for the areas of use is the same, but it differs from the recommendations of Artificial Intelligence.

The thesis is in estonian and contains 28 pages of text, 3 chapters, 14 figures, 9 tables.

Lühendite ja mõistete sõnastik

AI	<i>Artificial Intelligence</i> , tehisintellekt
<i>Autofill</i>	Veebivormi väljale automaatne info sisestamine
<i>Bookmarks toolbar</i>	Järjehoidja tööriba, hoiustab salvestatud veebilehti
<i>Dataset</i>	Andmestik
DNT	<i>Do Not Track</i> , seade info kogumise piiramiseks
<i>Extension</i>	Brauseris lisafunktsionaalsust pakkuv programm
<i>Fingerprint</i>	Digitaalne jälg, mis kujuneb brauseri kasutusel
HTTP	<i>Hypertext Transfer Protocol</i> , hüpertexti edastusprotokoll
HTTPS	Turvaline hüpertexti edastusprotokoll
IP-aadress	Seadme aadress arvutivõrgus
LLM	<i>Large Language Model</i> , suur keelemudel
<i>Multiprocess memory use</i>	Muutmälu jagamine parajasti kõigi toimuvate protsesside vahel
NLP	<i>Natural Language Processing</i> , loomuliku keele töötlus
<i>Onion routing</i>	Kolmekihiline võrguliikluse krüpteerimine
<i>Plug-in</i>	Pistikprogramm
RAM	<i>Random Access Memory</i> , muutmälu
RLHF	<i>Reinforced Learning Human Feedback</i> , inimtagasisidega stiimulõpe
<i>Tab</i>	Vaheleht brauseris
<i>Tabbed browsing</i>	Brausimine kasutades vahelehti
<i>Themes</i>	Värvikujundus brauseris
XSS/Data injection	<i>Cross Site Scripting</i> rünnak, mille korral sisestatakse pahavaralikud skriptid veebilehekülje väljadesse

Sisukord

Sissejuhatus	11
1 Veebibrauserid ja nende põhiomadused	12
1.1 Google Chrome.....	12
1.2 Brave.....	14
1.3 Microsoft Edge	15
1.4 Mozilla Firefox	16
1.5 Tor Browser	16
1.6 Brauserite võrdlus.....	18
2 Veebibrauserite turvalisuse tagamise vahendid.....	20
2.1 BrowserAudit.....	21
2.2 Turvalisus- ja privaatsusseaded brauseris.....	22
2.2.1 Hüpikaknad; veebisaidi kirjavigadevastane kaitse	22
2.2.2 Tugeva parooli genereerimine; <i>HTTPS mode</i> ; ohtlikud allalaadimised.....	23
2.2.3 Sirvimisandmed, <i>fingerprinti</i> blokeerimine	24
2.2.4 Kolmanda osapoole küpsised, <i>Do Not Track</i> , privaatsusrežiim.....	24
2.3 Panopticlick/Cover Your Tracks	25
2.4 Microsoft Copilot	25
3 Turvaliseima veebibrauseri leidmine vastavalt kasutusvaldkonnale.....	27
3.1 Testimismetoodikad.....	27
3.2 Testimistulemused	27
3.2.1 Brauseri ehitus	27
3.2.2 Brauseri <i>fingerprint</i>	29
3.3 Brauseritele hinnangu andmise meetoodika.....	30
3.3.1 Hinnangute andmine.....	30
3.4 Brauseri hinnangu andmise tulemused	32
3.5 Võrdlus MS Copilot'i poolt antud soovitusetega	36
Kokkuvõte	36
Kasutatud allikad	39
Lisa 1 – Lingid brauserite testimistulemustele	43

Lisa 2 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks 44

Jooniste loetelu

Joonis 1. Google Chrome brauseri logo.	12
Joonis 2. Populaarseimate brauserite turg 2023. aastal [1].....	13
Joonis 3. Tõlke tulemus otsingusoovitustes.	13
Joonis 4. Brave brauseri logo.	14
Joonis 5. Microsoft Edge'i logo.	15
Joonis 6. Mozilla Firefox brauseri logo.....	16
Joonis 7. Tor Browser'i logo.....	17
Joonis 8. <i>Onion routing</i> tööpõhimõte [17].	17
Joonis 9. Veebibrauseri turvalisust mõjutavad tegurid.....	20
Joonis 10. BrowserAudit'i testikategooriad.....	21
Joonis 11. Veebisaidi kirjavigadevastane kaitse.....	23
Joonis 12. Turvalisem brauser sotsiaalmeedia jaoks MS Copilot'i soovitustel.	36
Joonis 13. Turvaliseima brauser panganduseks MS Copilot'i soovitustel.	36
Joonis 14. Turvalisem brauser uurimistöö kirjutamiseks MS Copilot'i soovitustel. ...	37

Tabelite loetelu

Tabel 1. Brauserite põhiomaduste võrdlus.	18
Tabel 2. BrowserAudit'i testimistulemused.....	28
Tabel 3. Turvalisus- ja privaatsusseaded brauserites.	28
Tabel 4. Panopticlick'i testimistulemused.	29
Tabel 5. Kaalukoefitsendid seadetele ja testimistulemustele.	31
Tabel 6. Hinnangud brauseritele.....	33
Tabel 7. Hinnangu tulemused sotsiaalmeedias kasutamise jaoks.....	33
Tabel 8. Hinnangu tulemused pangandusvaldkonna jaoks.....	34
Tabel 9. Hinnangu andmise tulemused uurimistöo kirjutamise jaoks.....	35

Sissejuhatus

Tänapäeva tehisintellektiga arenevas digimaailmas on aina olulisemaks muutumas veebibrauseri kasutaja turvalisus ja privaatsus. Igapäevaselt jätab veebibrauseri kasutaja endast maha andmeid, veebilehti kasutatakse kasutaja tegevuse jälgimise ning kuritegevuslikel eesmärkidel. Seetõttu on oluline valida brauser, mille turvalisuse ja privaatsuse üle on kasutajal suurem kontroll. Viimaste aastate tehisintellekti valdkonna kiire arenguga on tekkinud uued võimalused saamaks infot kasutaja turvalisuse tõstmisega seotud küsimustes.

Käesoleva bakalaureusetöö eesmärk on anda metoodika, kuidas valida brauserite hulgast turvalisem. Näitena on välja selgitatud turvalisem brauser järgmiste valdkondade jaoks: sotsiaalmeedia, pangandus ning uurimistöö kirjutamine.

Iga kasutusvaldkonna jaoks turvalisema brauseri välja selgitamiseks valitakse esmalt välja viis populaarseimat turvalisuse suunitlusega brauserit, mille turvalisus- ja privaatsusseadete olemasolu kontrollitakse ning mida testitakse veebipõhiste tööriistadega. Tulemuste põhjal pakutakse iga kasutusvaldkonna jaoks välja turvalisem brauser.

Töö on jaotatud kolmeks peatükiks. Esimeses peatükis kirjeldatakse veebibrausereid ja nende põhiomadusi. Teises peatükis tehakse ülevaade töös kasutatavatest brauserite turvalisuse tagamise vahenditest: brauserite turvalisuse- ja privaatsusseadetest, veebipõhistest tööriistadest ja tehisintellektist. Kolmandas peatükis kirjeldatakse testide ülesehitust ja tulemusi, mida võrreldakse tehisintellekti poolt antud soovitusetega. Töö tulemusena antakse vastavalt kasutusvaldkonnale soovitusel turvalisema brauseri valikuks.

1 Veebibrauserid ja nende põhiomadused

Brauserite valik sai tehtud eesmärgiga testida erinevaid levinuimaid ning turvalisuse suunitlusega brausereid. Valiku tegemisel peeti silmas asjaolu, et mitmed levinuimad brauserid (Google Chrome, Brave, Microsoft Edge) on loodud Chromium'i koodibaasil. Testitavate brauserite valiku mitmekesistamiseks valiti ka kaks brauserit, mis olid loodud kasutades Mozilla Foundation'i Gecko Rendering Engine'it (Mozilla Firefox, Tor Browser).

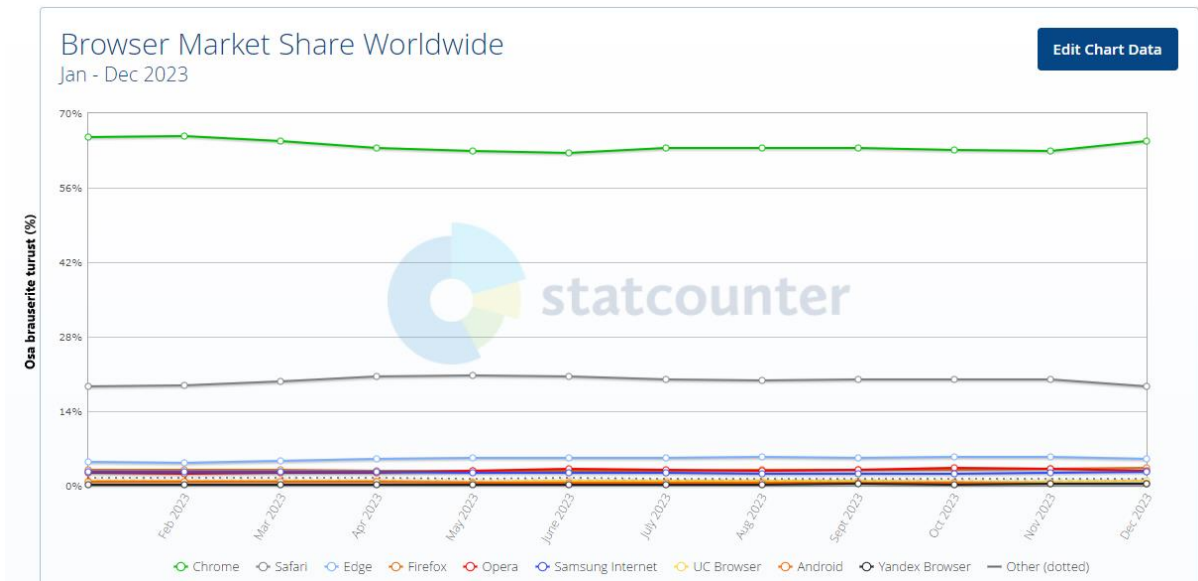
Järgnevalt tehakse ülevaade viie erineva brauseri kohta ning tuuakse brauserite põhiomaduste võrdlus.

1.1 Google Chrome

Jätakuvalt on maailma populaarseimaks brauseriks Google Chrome (logo näha Joonisel 1), hõlmates 2023. aasta seisuga ligi 67% turuosast (Joonis 2) [1]. Tänu oma mugavale kasutajaliidesele ja eri seadmetevahelisele sünkroniseerimisvõimalusele, on veebibrauser moodustanud suurima osa brauserite turust juba aastaid [2].

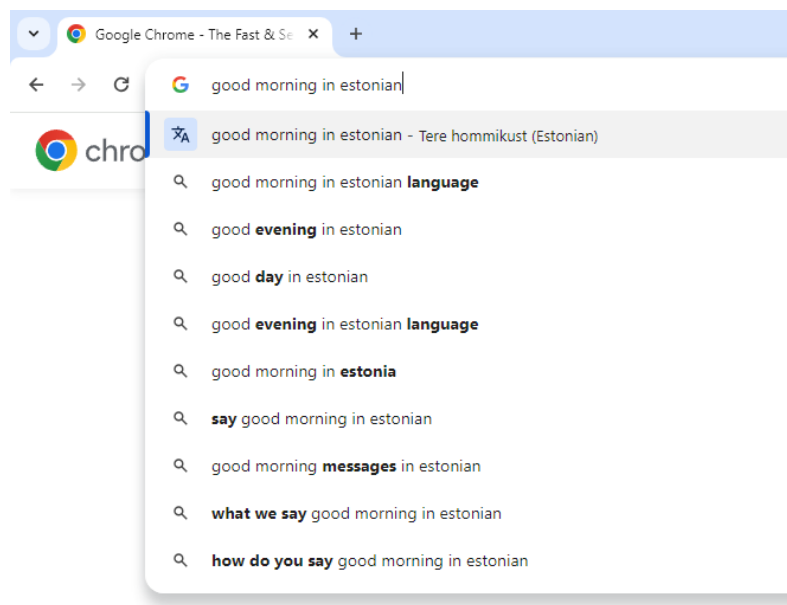


Joonis 1. Google Chrome brauseri logo.



Joonis 2. Populaarseimate brauserite turg 2023. aastal [1].

Google'i poolt loodud brauser pakub multifunktsionaalset otsinguriba, mis töötab peale Interneti otsingu teostamise ka valuuta teisendajana, kalkulaatorina, tõlkijana (Joonis 3) ja ilmteadete näitajana, kuvades sealjuures vastust kohe otsingusoovitustes [3].



Joonis 3. Tõlke tulemus otsingusoovitustes.

Antud brauser loodi selleks, et pakkuda paremat platvormi uutele Google'i pilvepõhistele veebiprogrammidele nagu tekstiredaktor Google Docs, ajaplaneerimisprogramm Google Calendar ja failihaldusprogramm Google Drive [4].

Google Chrome'i on sisseehitatud andmetekogumise mehhanismid, mis aeglustavad mõnikord brauseri tööd, kasutades suurt osa arvuti mälu mahust [5]. Osad mehhanismidest on valikulised, teised aga kohustuslikud. Andmete kogumine toimub eesmärgiga luua kasutaja kohta profiil, et näidata/soovitada brauseri kasutajale veebilehtedel artikleid, blogisid ja sisu üle veebi, mis oleks tema eelistustele vastavad. Kogutud andmeid müüakse teinekord edasi ka kolmandale osapoolele (reklaamettevõtted).

1.2 Brave

Brave erineb teistest brauseritest, kuna sellesse sisseehitatud turvamehhanismid krüpteerivad kasutaja veebisirvimise tagajärjel tekkivad andmed. Sellega välistatakse võimalus kasutaja kontot tema tegevuse järgi „jälitada“. Brauserit on võimalik seadistada sulgemisel automaatselt andmeid kustutama [5].

Tegemist on uuemat tüüpi brauseriga, mis loodi 2016. aastal Brave Software'i poolt (logo näha Joonisel 4). Nagu Mozilla Firefox, on ka see brauser vabavaraline. Brave on ehitatud Chromium'i koodibaasi peal. Brauseri ehitus võimaldab kasutajal ise reguleerida mitmeid erinevaid privaatsusseadeid [6].



Joonis 4. Brave brauseri logo.

Brave'i kasutajaskond on aastatega kasvanud, kuid jääb siiski suurettevõtete brauseritele nagu Google Chrome ja Mozilla Firefox alla: iga päev kasutab Brave'i 50,2 miljonit kasutajat, samas kui Google Chrome'i näitajad ulatuvad miljarditesse [7].

1.3 Microsoft Edge

Windows'i poolt soovitatud ametlik brauser on ehitatud Chromiumi koodibaasil ja Blink veebimootoril (logo näha Joonisel 7). Brauseri tekkis 2015. aastal eesmärgiga asendada kunagine maailma populaarseim brauser Internet Explorer, mille tehnilise toe Microsoft peatas 2016. aastal brauseri kasutuskonna ulatusliku languse tõttu [8]. Olenemata mitmetest funktsionaalsustest ja uuendustest, moodustub Microsoft Edge (edaspidi MS Edge) tänapäeval alla 6% [1].



Joonis 5. Microsoft Edge'i logo.

Sarnaselt Google Chrome'ile pakub MS Edge andmete sünkroniseerimisvõimalust mitmete eri seadmete vahel. Peale Windows'i on MS Edge'i võimalik kasutada erinevatel operatsioonisüsteemidel: MacOS'il, iOS'il ja Androidi põhistel seadmetel [9]. Brauserisse on sisseehitatud mitmed kasulikud funktsioonid: süvaluger võimaldab brauserisiseselt teha tekstidokumendile märkmeid, joonistusi, tõlkida teksti, ning küsida esiletõstetud teksti kohta Microsoft Copilot AI-lt infot; artiklite lugemisel, kui veebileht toetab, saab kasutada Immersive Reader'it, mis muudab veebilehe formaadi mugavaks nii, et see meenutab virtuaalset raamatut või ajakirja artiklit; võimalik on kasutada tekst-kõneks funktsionaalsust ehk lugemisel on võimalik lasta tekst endale ette lugeda [10].

Veebi anonüümsemaks brausimiseks on brauserisse sisseehitatud InPrivate mode. InPrivate brauseriaknas on blokeeritud küpsised ja veebilehtede poolt tegevuse jälgimine. Peale InPrivate akna sulgemist kogu brausimisajalugu ja allalaaditud failide ajalugu kustutatakse (sealhulgas ka vahemälus olevad salasõnad, pildid ja *autofill* andmed) [9].

1.4 Mozilla Firefox

Mozilla Firefox (logo näha Joonisel 3) on kasutaja privaatsuse tagamisele keskendunud brauser, mis loodi ettevõtte Netscape Communications Corporation'i poolt. Brauser sisaldab mitmeid sisseehitatud funktsioone, et kaitsta kasutajat andmelekete ning tema veebitegevuse jälgimise eest.



Joonis 6. Mozilla Firefox brauseri logo.

Sarnaselt Chrome'ile, on ka Mozilla Firefox'is võimalik isikupärastada brauserit erinevate brauseri laiendustega, *plug-in*'idega (pistikprogrammidega) ja *themes*'ide (kasutajaliidese värvide) kujundamisega [11]. Mozilla Firefox'i teke pakkus brauserite maailma uusi funktsionaalsusi nagu *Bookmarks toolbar* (järjehoidja tööriba), võimaldades salvestada veebilehti kaustadesse; *tabbed browsing* (vahelehtedega brausimine), mis võimaldas mitut erinevat veebilehte hoida avatuna ühes brauseriaknas. Mtime *tab*'i (vahelehe) lahtiolekul kasutab brauser *Multiprocess memory use* tehnoloogiat (muutmälu jagamine parajasti kõigi toimuvate protsesside vahel), mis võimaldab brauseril kasutada vähem mälu [12].

Brauserist on erinevaid versioone, alustades standardversioonist, mis on mõeldud ainuüksi Interneti otsingute jaoks ja lõpetades Firefox Enterprise Support Release' iga, mis võimaldab organisatsioonidel rakendada brauserit laiemal skaalal. Mozilla Firefox on vabavaraline brauser – see võimaldab nii tarkvaraarendajatel kui ka tavakasutajatel oma vastavas versioonis testida brauseri uusi omadusi [13].

1.5 Tor Browser

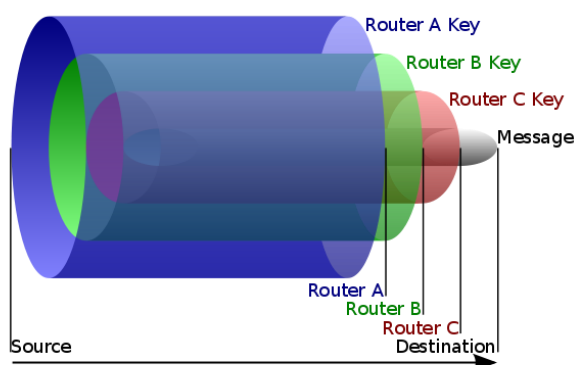
Tor Browser'it (logo näha Joonisel 6) hakati arendama 2008. aastal, kuid brauseri alustalana töötav *Onion routing* tehnoloogia arendati välja juba 1990. aastate keskel [14]. *Onion routing* suunab võrguliiklust läbi mitme serveri ja krüpteerib seda igal sammul

[15]. Tor'i võrgu esmakordse kasutuselevõtuga 2002. aastal avaldati selle kood vabataarkvara litsentsi alusel. Vajadus eraldi brauseri järele tekkis Interneti tavakasutajate, vähem tehnilise taustaga inimeste huvist kasutada *Onion routing* (kolmekihiline võrguliikluse krüpteerimine) tehnoloogiat.



Joonis 7. Tor Browser'i logo.

Onion routing tehnoloogia tagab brauseri kasutamisel kasutaja anonüümsuse. Võrguliikluse krüpteerimist ja suunamist teostatakse läbi kolme rahvusvahelistest võrgusõlmedest koosneva võrgukihi (Joonis 7). Esimene sisendsõlmedest koosnev krüpteerimiskiht loob ühenduse Tor'i võrguga. Teine keskmistest sõlmedest koosnev kiht krüpteerib võrguliikluse, et tagada anonüümsus. Välisõlmedest koosnev kiht krüpteerib veelkord andmed enne lõppserverisse jõudmist. Avalikud IP-aadressid ja brausimisajalugu on maskeeritud [16].



Joonis 8. *Onion routing* tööpõhimõte [17].

Brauserit kasutatakse tihti, et saada ligipääs .onion domeenilaiendiga veebilehtedele, millele teiste brauseritega (näiteks Google Chrome, Mozilla Firefox) ei ole võimalik ligi saada. Tavaline veebibrausimine võib osutuda ajamahukaks. Tor Browser'iga veebilehtedele minek on aeglane, sest andmed suunatakse ja krüpteeritakse läbi kolme võrgukihi.

1.6 Brauserite võrdlus

Järgnevalt võrreldakse viite eelnevalt käsitletud brauseri põhiomadust. Tabelis 1 on välja toodud neli omadust, mis brausereid kirjeldavad ning ülevaade brauserite poolt toetatavatest operatsioonisüsteemidest.

Tabel 1. Brauserite põhiomaduste võrdlus.

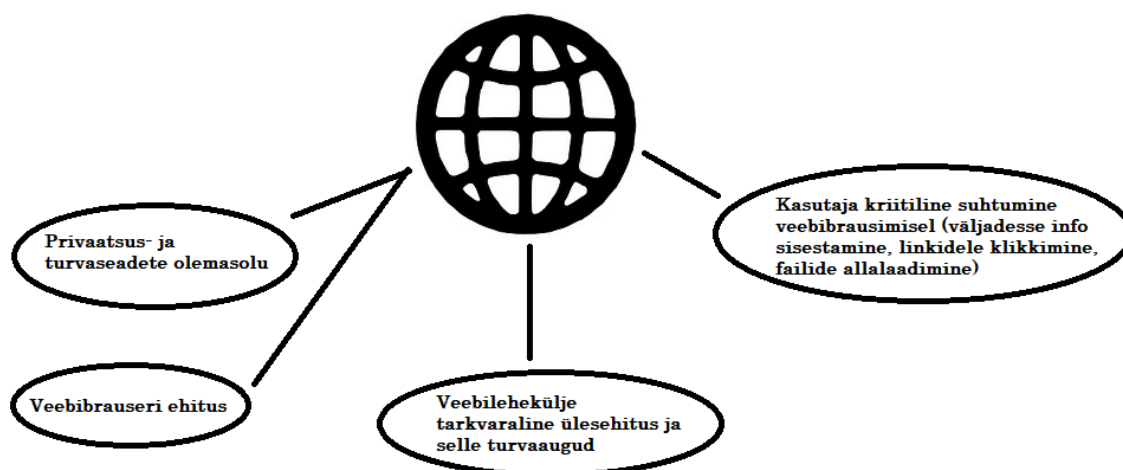
Brauser	Koodibaas	Sünkroniseerimine seadmete vahel	Themes'id	AI-assistent	RAM-i kasutus (10 tab'i lahti)
Google Chrome	Chromium	+	+	-	950 MB
Mozilla Firefox	Gecko Rendering Engine	+	+	-	990 MB
Brave	Chromium	+	+	Leo AI	920 MB
MS Edge	Chromium	+	+	Microsoft Copilot	790 MB
Tor Browser	Gecko Rendering Engine	+	+	-	Andmed puuduvad
Brauser	Operatsioonisüsteemi tugi				
	Windows	MacOS	Linux	Android	iOS
Google Chrome	+	+	+	+	+
Mozilla Firefox	+	+	+	+	+
Brave	+	+	+	+	+
MS Edge	+	+	+	+	+
Tor Browser	+	+	+	+	-

Toodud võrdlusest on näha, et kõik brauserid pakuvad seadmetevahelist sünkroniseerimisvõimalust ja brauseri stiili kujundamist. Sisseehitatud AI-põhist assistenti omavad vaid kaks brauserit – Brave ja MS Edge. RAM-i (*Random Access Memory*, muutmälu) kasutuses tulid esikohale Google Chrome ja Mozilla Firefox. Pea

kõik maailma populaarseimad operatsioonisüsteemid on iga viie brauseri poolt toetatud. Ainsaks erandiks on Tor Browser, mis ei toeta iOS-i [18]. Selle operatsioonisüsteemi kasutajatele on alternatiivina võimalik kasutada Onion Browser'it, mis võimaldab samuti ühenduda Tor'i võrguga [19].

2 Veebibrauserite turvalisuse tagamise vahendid

Turvaline veebibrauser hõlmab endast mitut komponenti. Vajalik on, et brausimisel jääks kasutajast maha võimalikult vähe andmeid ning kasutaja tuvastamine tema veebitegevuse järgi oleks võimalikult raske. Joonis 9 näitab, et peale erinevate muudatusi teha võimaldavate privaatsus- ja turvaseadete sõltub brauseri turvalisus suuresti iga veebilehekülje enda tarkvaralisest ülesehitusest ning selle võimalikest turvaaukudest, aga ka kasutaja veebibrausimise harjumustest ning kriitilisest suhtumisest info sisestamisel väljadesse. Käesolevas töös hinnatakse veebibrauseri turvalisust privaatsus- ja turvaseadete olemasolu ning turvalisust hindavate tööriistade tulemuste järgi.



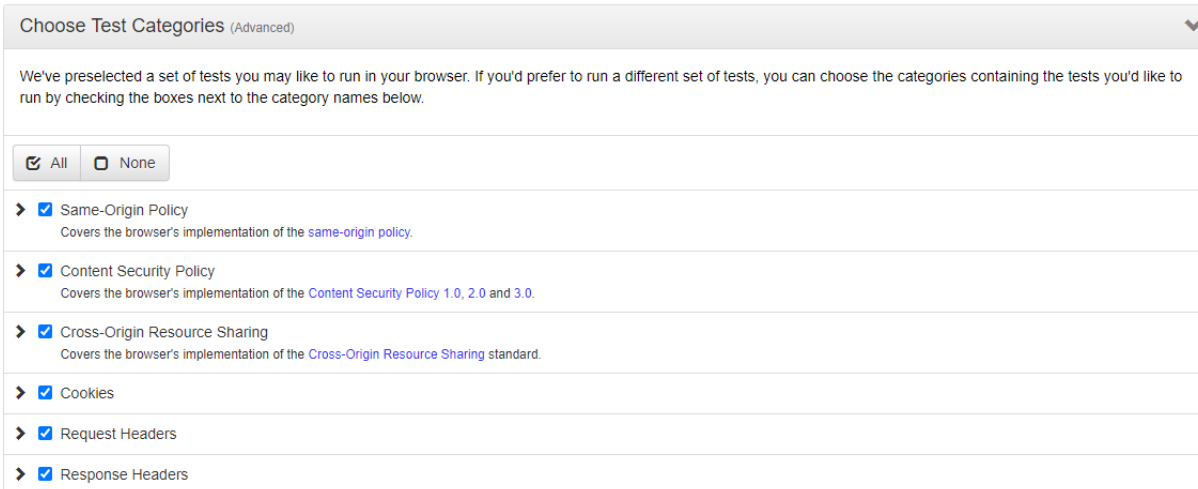
Joonis 9. Veebibrauseri turvalisust mõjutavad tegurid.

Brauserite turvalisuse tagamise vahenditena käsitletakse veebipõhiseid tööriistu Panopticlick, BrowserAudit ning brauserite turvalisuse- ja privaatsusseadeid. *Fingerprinti* ja brauseri turvastandardite ning mehhanismide testimiseks valiti tööriistadeks vastavalt välja Panopticlick ja BrowserAudit, lähtudes veebiartikli „11 tools to test browser security in 2024“ soovitudest [20]. Seaded, mille olemasolu brauseris kontrollida, valiti välja Thu-Hanna Leinbergi bakalaureusetöö „Veebibrauserite valik nutiseadmete kasutajale“ põhjal, kus hinnati nutiseadmetes brauserite turvalisust ja privaatsust viie kriteeriumi järgi [21] ning Tartu Ülikooli infoturbealase veebiartikli põhjal, kus tehti ülevaade veebibrauserite turvalisusest [22]. Seaded „Veebisaidi kirjavigadevastane kaitse“, „Tugeva parooli genereerimine“ ja „Ohtlike allalaadimiste blokeerimine“ võeti hindamisele brauserite seadete täiendava uurimise käigus.

Järgnevalt käsitletakse testimiseks kasutatavaid veebipõhiseid tööriistu ning testimiseks välja valitud turvalisuse seadeid brauserites.

2.1 BrowserAudit

Antud veebipõhine tööriist testib brauseri ehitust: levinuimate turvastandardite ning omaduste õigesti rakendumist brauseris. Selleks jookustatakse brauseris üle 400 testi, mis jagunevad kuute kategooriasse (Joonis 10).



Choose Test Categories (Advanced) ▼

We've preselected a set of tests you may like to run in your browser. If you'd prefer to run a different set of tests, you can choose the categories containing the tests you'd like to run by checking the boxes next to the category names below.

All None

- Same-Origin Policy
Covers the browser's implementation of the [same-origin policy](#).
- Content Security Policy
Covers the browser's implementation of the [Content Security Policy 1.0, 2.0 and 3.0](#).
- Cross-Origin Resource Sharing
Covers the browser's implementation of the [Cross-Origin Resource Sharing](#) standard.
- Cookies
- Request Headers
- Response Headers

Joonis 10. BrowserAudit'i testikategooriad.

Same-Origin Policy on brauseri turvamehhanism, mis reguleerib, kuidas ühest lähtekohast (domeenist, protokollist, pordist) [23] laetud dokument või skript saab suhelda teisest lähtekohast pärit ressursiga. See takistab pahatahtlikku veebilehte brauseris JavaScript'i jooksumisest, et kolmandalt osapoolelt andmeid lugeda ja ründajale edastada [24]. *Content Security Policy* turvamehhanism aitab tuvastada ja leevendada erinevaid rünnakuid nagu XSS ja *data injection*, mida kasutatakse andmete varastamiseks ja pahavara levitamiseks [25]. Tänu *Cross-Origin Resource Sharingule* saavad kliendipoolsed veebirakendused, mis laaditakse ühelt domeenilt, suhelda ressursidega teiselt domeenilt [26]. *Cookies* kategoorias testitakse küpsiste *HttpOnly* ja *Secure* atribuutide käitumist [27]. Request ja Response Headers kategooriates testitakse HTTP-vastuste päistega seotud brauseri turvafunktsioone, mida teistes kategooriates ei testitud [27].

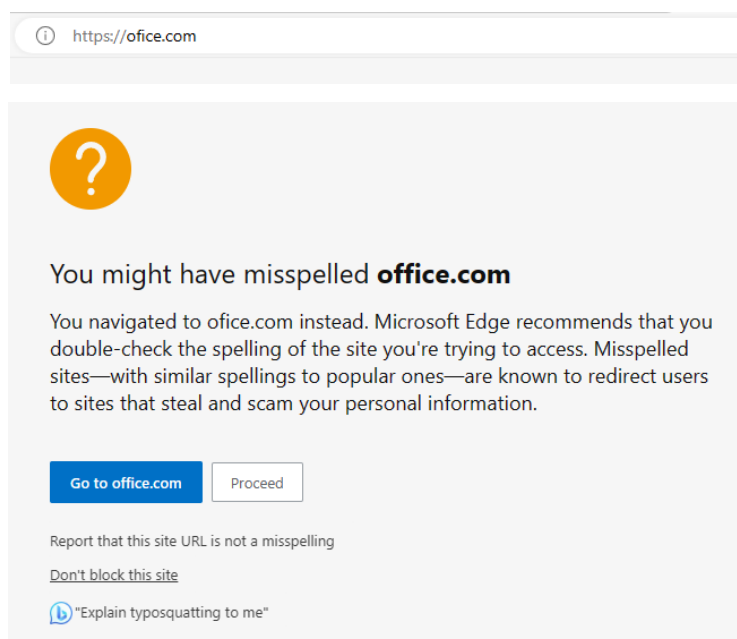
2.2 Turvalisus- ja privaatsusseaded brauseris

Igal brauseril on olemas seaded, mida kasutaja saab ise oma privaatsuse tõstmiseks kohaldada. Sõltuvalt brauseritest võib seadete ülesehitus erineda, kuid reeglina on olenemata brauserist põhilised privaatsusseaded, mis reguleerivad andmete kasutust, allalaadimisi ja veebisirvimisandmete säilitamist.

2.2.1 Hüpikaknad; veebisaidi kirjavigadevastane kaitse

Hüpikaknad on bännerid või brauseriaknad, mis ilmuvad veebilehe esiplaanile, kui kasutaja brausib veebilehte [28]. Nende akende eesmärgiks on veebilehe külastaja tähelepanu püüdmine mingi sisu reklaamimiseks või kasutaja andmete päringuks. Hüpikaknad võivad ilmuda mitmel eri viisil: peale kindlat aega, mis kasutaja on veebilehel veetnud; veebilehe allakerimisel; kui kasutaja hakkab veebilehelt lahkuma; kui kasutaja on veebilehel teatud aja mitteaktiivne olnud [28]. Kuigi hüpikaknaid kasutatakse laialdaselt turunduslikel eesmärkidel ettevõtete poolt, kasutatakse neid ka pahatahtlikel eesmärkidel andmepüügiks ja pahavara levitamiseks. Sellisel juhul tuleb brauseris kasuks hüpikakende blokeerimise seade, millega brauser automaatselt blokeerib mingi kindla veebilehe või mistahes veebilehe poolt kuvada soovitavad hüpikaknad, ilma et kasutaja neid näeks.

Otsinguribale veebilehe aadressi kirjutades on oluline sisestada täpne aadress. Kasutaja tähelepanematust täpse aadressi sisestamisel kasutatakse ära ründajate poolt. Sisestades aadressi valesti, näiteks „office.com“ asemel „ofice.com“, võib kasutaja sattuda andmepüügi või muu kasutajat kahjustava sisuga leheküljele. Kasutajat hoiatatakse, vältimaks soovimatule veebileheküljele sisenemist (Joonis 11) [29].



Joonis 11. Veebisaidi kirjavigadevastane kaitse.

Veebisaidi kirjavigadevastane kaitse on spetsiaalne seadistus, mis annab teada, kui soovitud veebilehe aadress on sisestatud valesti ning võib suunata pahatahtlikule veebilehele [30].

2.2.2 Tugeva parooli genereerimine; *HTTPS mode*; ohtlikud allalaadimised

Veebikeskkonda uue kasutajakonto loomisel peab kasutaja looma endale salasõna. Mida pikem ning erinevatest tähe- ja numbrimärkidest koosneva salasõna kasutusele võetakse, seda keerulisem on ründajal murda sisse kasutaja kontosse. Mitmed brauserid pakuvad konto loomisel funktsionaalsust, mille korral genereeritakse piisava pikkuse ja keerukusega tugev parool.

HTTPS (turvaline hüpertexti edastusprotokoll) on rakenduskihi protokoll. See on turvalisem versioon kui HTTP (hüpertexti edastusprotokoll), sest edastab andmeid üle võrgu krüpteeritult. Seega kui kasutusel on HTTPS, ei pea kartma andmete lekke pärast [31].

Brauserid kasutavad sisseehitatud viiruste tuvastussüsteemi, mille rakendumisel takistatakse kasutajat pahavaralist faili allalaadimast. Seeläbi välditakse erinevaid

kasutaja andmetega seotud probleeme, mis võivad pahavaralise faili allalaadimise ja kasutamise kaasneda.

2.2.3 Sirvimisandmed, *fingerprinti* blokeerimine

Veebibrausimisel salvestab brauser infot otsinguajaloo ja külastatud veebilehtede kohta. Brausimisandmed võimaldavad veebilehtedel kasutaja mugavuse huvides automaatselt täita küsitlusvormi väljad ja jätta kasutaja sisselogitaks veebilehtedele pärast brauseriakna sulgemist. See loob aga privaatsusriski, misjuhul kolmandal osapoolel on ligipääs kasutaja isiklikele andmetele [32]. Laialtlevinud brauseri seadeks on seetõttu kujunenud „Sirvimisandmete kustutamine“, mis on tänavu sisseehitatud pea igasse brauserisse. Antud seadet kasutades saab kustutada valitud ajavahemikus brausimis- ja otsinguajaloo, kuid ka küpsised ja brauseri vahemälu.

Fingerprinti (digitaalne jälg, mis kujuneb brauseri kasutusel) blokeerimine raskendab kolmandatel osapooltel kasutaja identifitseerimist veebibrausimisel [33]. Seade on alternatiiv kolmanda osapoole küpsistele – kui kolmanda osapoole küpsised on brauseris keelatud, on võimalik saada infot kasutaja arvuti riistvara ja tarkvara kohta ka *fingerprintimise* kaudu [34].

2.2.4 Kolmanda osapoole küpsised, *Do Not Track*, privaatsusrežiim

Ühe veebilehe elemente laetakse mitmelt eri domeenilt, mis saavad kasutada just kolmanda osapoole küpsiseid [22]. Need jälgivad kasutaja ajalugu ja tegevust (huvid, brausimistavad, eelistused). Kolmanda osapoole küpsiseid kasutatakse digiturunduslikel eesmärkidel, soovimaks veebilehe külastajale näidata tema huvidele vastavaid reklaame [35]. Küpsised omandavad suures koguses isikuandmeid, mida hiljem (kasutaja teadmata, luba küsimata) müüakse digitaalreklaami turunduse tööstuses edasi. Andmed, mida kogutakse on tundlikud: kasutaja IP-aadress, seadme info, otsingu- ja brausimisajalugu, isiklik info inimese tervise, perekonna, poliitiliste veendumuste ja muude omaduste kohta. Kogutud andmete põhjal koostatakse kasutajast digitaalprofiil, mida omakorda kasutatakse turunduslikel eesmärkidel [36]. Selleks, et kaitsta oma kasutajaid soovimatu isikuandmete laialtleviku eest, on osades brauserites olemas spetsiaalne seadistus, mis võimaldab kolmanda osapoole küpsiste seadmele salvestamist keelata.

Do Not Track (edaspidi DNT) on üks teine seadistus, millega võib ära hoida küpsiste teel info kogumise. Kasutaja ei keela sellega kolmanda osapoole küpsiseid, kuid kui seadistus

on aktiivne, siis saadab brauser veebilehele *Do not track* signaali. Signaal annab veebilehele märku, et selle küpsiseid ei soovita seadmesse salvestada [37].

Privaatsusrežiim on brausimisviis, mille korral veebibrauser ei salvesta kasutaja brausimistegevust. See võimaldab Interneti brausida veebilehtedelt küpsiseid salvestamata. Kuigi privaatsusrežiim hoiab lokaalse brausimise privaatsena, ei takista see näiteks võrguühenduse teenusepakkujat nägemast, mis veebilehtedel on kasutaja käinud [38]. Google Chrome'is täidab privaatsusrežiimi funktsionaalsusi *Incognito mode*, Mozilla Firefox'is *Private window*, MS Edge'is *InPrivate browsing* ning Brave brauseris *Private window with Tor*, mis kasutab Tor'i võrku [39]. Tor browser'is spetsiaalne režiim puudub – kasutaja brausimistegevus ja veebilehtedelt salvestatud küpsised kustutatakse brauseriakna sulgemisel.

2.3 Panoptick/Cover Your Tracks

Igal brauseril on oma *fingerprint* (digitaalne jälg), mis kujuneb kasutaja brauseri kasutusel. Identifitseerimiseks kasutatakse kohalikke (ühes brauseris) ja ülebrauserilisi (mitmes brauseris) tuvastusmeetodeid [40]. Veebilehed kasutavad digitaalset jälge kasutaja tuvastamiseks. Külastamisel saadab brauser veebilehele infot arvuti tarkvara (näiteks operatsioonisüsteemi versioon, brauseri versioonid, kasutuskeel) ja riistvara (näiteks protsessori klass, puutetundlikuse tugi) kohta [34], [41]. *Fingerprinti* alusel luuakse kasutajast profiil. Mida vähem unikaalsem *fingerprint*, seda raskem on kasutajat veebilehtedel tuvastada.

Panoptick on veebipõhine tööriist, millega on võimalik testida, kui unikaalse *fingerprinti* on kasutaja endast brauserit kasutades Internetis maha jätnud. Tulemust võrreldakse anonüümsetest kasutajaprofiilidest koosnevate sõrmejälgede andmebaasiga, andes iga identifitseerimismeetodiga hinnangu digitaalse jälje unikaalsusele.

2.4 Microsoft Copilot

Microsofti poolt loodud Microsoft Copilot (edaspidi MS Copilot) on treenitud OpenAI GPT-4 LLM-i (suur keelemudel) baasil, mis kasutab RLHF (inimtagasisidega stiimulõpe) meetodit [42]. Tehisintellekt kasutab suures koguses andmestikku, et treenida närvivõrku genereerimaks NLP (loomuliku keele töötlus) põhist teksti. *Dataset* (andmestik) koosneb

suurtest andmekogumitest: raamatutest, artiklitest ja veebilehtedest [43]. MS Copilot suhtleb kasutajaga dialoogi vormis, pakkudes lahendusi laias spektris probleemidele, sealhulgas kasutaja privaatsuse ja turvalisusega seotud küsimustele.

3 Turvaliseima veebibrauseri leidmine vastavalt kasutusvaldkonnale

3.1 Testimismetoodikad

Kõik testimised viidi läbi Windows 10 operatsioonisüsteemi peal. Testimised jaotati kaheks osaks: brauseri ehitus ja brauseri *fingerprint*.

Brauseri ehituse testimiseks võeti aluseks 2. peatükis käsitletud seaded ning turvastandardite ja ehituse õigesti rakendumist testiv tööriist BrowserAudit. Igas brauseris kontrolliti seadete olemasolu ning jooksutati BrowserAudit'i teste, et kontrollida brauserite turvastandardite ja omaduste rakendumist.

Fingerprinti testimiseks tuli enne testimist luua ühtsed eeltingimused. Eeltingimuste loomisel eeldati, et tavakasutaja brauseri vaikeseadeid ei muuda - iga brauseri seati esialgsetele seadetele. Brausimisajalugu kustutati, igat brauserit uuendati uusima versioonini ning veenduti, et ühtegi brauseri *extension*'it (brauseris lisafunktsionaalsust pakkuv programm) ei oleks kasutusel ning kõigist veebilehtede kontodest oleks välja logitud. Selleks, et testida, kuidas brauseri digitaaljalje kujunemine sõltub brauseri valikust, külastati iga brauseriga kolme eri valdkonna raames veebilehti. Esiteks külastati iga brauseriga kolme Eesti uudisteteemalist veebilehte [44], [45], [46]. Igal uudistelehel avati üks kindel artikkel. Teiseks külastati iga brauseriga kolme Eesti panganduseteemalist veebilehte [47], [48], [49]. Kolmandaks külastati iga brauseriga kolme Eesti ülikooli veebilehte [50], [51], [52]. Tor Browser'iga ilmnas, et leheküljed aripaev.ee ja panganduslehekülg luminor.ee olid Tor brauseri kasutamise tõttu veebilehele ligipääsu keelanud. Seetõttu jäid antud brauseri puhul kaks veebilehte külastamata.

3.2 Testimistulemused

3.2.1 Brauseri ehitus

Allolevas tabelis 2 on toodud välja BrowserAudit'i testide tulemused (Lisa 1). BrowserAudit'i testid kontrollisid brauseris levinuimate turvastandardite ning omaduste

õigesti rakendumist. Numbrid veergudes näitavad testide arvu vastavalt tulemustele (näiteks Google Chrome läbis edukalt 401 testi).

Tabel 2. BrowserAudit'i testimistulemused.

Test	Brauseri nimetus				
	Google Chrome	Brave	MS Edge	Mozilla Firefox	Tor Browser
<i>Passed</i> (läbitud)	401	402	401	402	393
<i>Warning</i> (hoiatus)	30	29	30	29	35
<i>Critical</i> (kriitiline)	0	0	0	0	0
<i>Skipped</i> (vahele jäetud)	0	0	0	0	3

Kõige rohkem teste läbisid edukalt Mozilla Firefox ja Brave, mis läbisid võrdse arvu teste. Kõige vähem teste läbis Tor Browser. Kriitilist tulemust ei saanud ükski brauser. Tabel 3 testimistulemused näitavad, millised turvalisus- ja privaatsusseaded millises brauseris esindatud on. Testimisel kontrolliti iga turvalisus- või privaatsusseade olemasolu brauserites.

Tabel 3. Turvalisus- ja privaatsusseaded brauserites.

Turvalisusseade	Brauseri nimetus				
	Google Chrome	Brave	MS Edge	Mozilla Firefox	Tor Browser
Hüpikakende blokeerimine	+	+	+	+	+
Veebisaidi kirjavigadevastane kaitse	-	-	+	-	-
Tugeva parooli genereerimine	+	+	+	+	-
<i>HTTPS mode</i>	+	+	-	+	+
Ohtlike allalaadimiste blokeerimine	+	+	+	+	+
Privaatsusseade	Brauseri nimetus				
	Google Chrome	Brave	MS Edge	Mozilla Firefox	Tor Browser
Sirvimisandmete kustutamine	+	+	+	+	+
<i>Fingerprinti</i> blokeerimine	-	+	+	+	-

Privaatsusseade	Brauseri nimetus				
	Google Chrome	Brave	MS Edge	Mozilla Firefox	Tor Browser
3.osapoole küpsiste keelamine	+	+	+	+	-
DNT	+	+	+	+	-
Privaatsusrežiim	Incognito mode	Private window with Tor	InPrivate Window	Private window	Private browsing mode

Seadete testimistulemustest võib järeldada, et pea kõik vajalikud turvalisus- ja privaatsusseaded on olemas igas viies brauseris, väiksemate erisustega. Kolmanda osapoole küpsiste blokeerimise seade Tor Browser'is eraldi puudub, kuid brauser kustutab automaatselt kõik küpsised brauseriakna sulgemisel. Hüpikakende blokeerimine, *HTTPS mode*, ohtlike allalaadimiste blokeerimine ning sirvimisandmete kustutamine on esindatud kõigis viies brauseris. Privaatsusrežiim on omane kõigile viiele brauserile. Erinevalt teistest brauseritest, kus privaatsusrežiimi avamiseks tuleb avada eraldi brauseriakna, on Tor Browser'i privaatsusrežiimi funktsionaalsus juba brauseri allalaadimisel seadetes määratud (lehekülje andmed ja küpsised kustutatakse brauseri sulgemisel). Tor Browser'il puuduvad eraldi DNT ja *fingerprinti* blokeerimise seaded. *Fingerprinti* blokeerimine toimub vaikimisi. Veebisaidi kirjavigadevastane kaitse on omane vaid ühele brauserile – MS Edge'ile.

3.2.2 Brauseri *fingerprint*

Tabelis 4 on väljatoodud Panopticlick'iga läbitud peamised testimistulemused (Lisa 1). Hinnati brauseri *fingerprinti* unikaalsust, jälgijate blokeerimise võimet ning kaitstust 3.osapoole jälgimise eest.

Tabel 4. Panopticlick'i testimistulemused.

Brauseri nimetus	<i>Fingerprinti</i> unikaalsus	Jälgijate blokeerimine	Kaitse 3. osapoole jälgimise eest
Google Chrome	Peaaegu unikaalne	-	Puudub kaitse
Brave	Randomiseeritud	+	Tugev kaitse
MS Edge	Unikaalne	-	Puudub kaitse
Mozilla Firefox	Unikaalne	+/-	Osaline kaitse
Tor Browser	Mitte-unikaalne	+	Tugev kaitse

Unikaalse *fingerprinti* tulemuse said kaks brauserit – MS Edge ja Mozilla Firefox. „Tugeva kaitse“ hinnangu said Tor Browser ja Brave, mis said ühtlasi hakkama jälgijate blokeerimisega ja omandasid kõige mitte-unikaalsema hinnangu *fingerprintile*. See oli oodatav tulemus, arvestades nende brauserite erilist suunitlust turvalisuse ja privaatsuse saavutamisel. Mozilla Firefox blokeeris osa jälgijatest, kuid MS Edge ja Google Chrome jälgijate blokeerimise osas kaitset ei pakkunud. Google Chrome, MS Edge ja Mozilla Firefox said kõik peaaegu või täiesti unikaalse *fingerprinti* hinnangu, millest järeldub, et nende brauserite kasutamine vaikimisi seadetal annab kolmandatele osapooltele hea võimaluse andmete kogumiseks ja kasutaja tuvastamiseks.

3.3 Brauseritele hinnangu andmise meetodika

Iga kasutusvaldkonna jaoks turvaliseima brauseri välja pakkumiseks võeti iga kasutusvaldkonna jaoks aluseks peatükis 3.2 käsitletud seaded ning Panopticlick'i ja BrowserAudit'i testide tulemused.

Soovituste tegemiseks määrati kasutusvaldkonniti igale seadele ning Panopticlick'i ja BrowserAudit'i testitulemusele kaalukoefitsent ja anti brauseritele hinnang (punktid). Seejärel rakendati iga kasutusvaldkonna punktide jaoks valemit (1) ning anti soovitused brauseri valikuks sotsiaalmeedias ja panganduses kasutamiseks ning uurimistöö kirjutamiseks.

Iga kasutusvaldkonna jaoks turvaliseima brauseri välja valimiseks kasutati valemit 1, kus k_i on kaalukoefitsent ja a_i on hinnang:

$$f(x) = \sum_{i=1}^n k_i a_i \quad (1)$$

Kaalukoefitsente anti skaalal 1-3, kusjuures 1 oli antud kasutusvaldkonna jaoks minimaalse tähtsusega ning 3 suure tähtsusega. Testimistulemuste eest või seadete olemasolu eest anti hinnanguid skaalal 0-4.

3.3.1 Hinnangute andmine

BrowserAuditi testide läbimise arvud ei erinenud üksteisest märgatavalt, mistõttu toimus ka punktide andmine seda arvestades. Brauserid, mis läbisid 402 või 401 testi, omandasid 4 punkti ning 393 testi läbinud brauser (Tor Browser) omandas 3 punkti. Iga turvalisus-

või privaatsusseade olemasolu andis brauserile 1 punkti. Iga seade puudumine andis brauserile 0 punkti. Peaaegu unikaalne või unikaalne *fingerprinti* testimistulemus andis brauserile juurde 0 punkti. Randomiseeritud või mitte-unikaalne testimistulemus andis brauserile juurde 1 punkti. Kõigi jälgijate blokeerimise eest omandas brauser 2 punkti (+). Osalise jälgijate blokeerimise eest (+/-) 1 punkti ja mitte-blokeerimise eest (-) 0 punkti. Kaitsele 3. osapoole jälgimise eest anti punkte järgnevalt: kaitse puudumise eest 0 punkti; osalise kaitse eest 1 punkt; tugeva kaitse eest 2 punkti.

Tabel 5 kirjeldab seadete kaalukoefitsentide suurusi vastavalt kasutusvaldkonnale. Väljatoodud kaalukoefitsendid on määratud brauseri seadetele ning Panopticklick'i ja BrowserAudit'i testide tulemustele. BrowserAuditi ja Panopticklick'i testimistulemused on võrdse kaaluga 3, sest need on olulised olenemata valdkonnast.

Tabel 5. Kaalukoefitsendid seadetele ja testimistulemustele.

Seade/Testitulemus	Kasutusvaldkond		
	Sotsiaalmeedia	Pangandus	Uurimistöö kirjutamine
BrowserAudit'i testid	3	3	3
Hüüpikakende blokeerimine	2	1	3
Veebisaidi kirjavigadevastane kaitse	1	2	3
Tugeva parooli genereerimine	2	3	1
<i>HTTPS mode</i>	2	3	3
Ohtlike allalaadimiste blokeerimine	1	1	3
Sirvimisandmete kustutamine	3	2	2
<i>Fingerprinti</i> blokeerimine	3	2	2
3.osapoole küpsiste keelamine	3	2	3
DNT	3	1	3

Seade/Testitulemus	Kasutusvaldkond		
Privaatsusrežiim	3	1	3
<i>Fingerprinti</i> unikaalsus	3	3	3
Jälgijate blokeerimine	3	3	3
Kaitse 3. osapoole jälgimise eest	3	3	3

Levinuimate sotsiaalmeedia platvormide kasutamisega on oluline, et kasutajal oleks võimalik kaitsta oma andmeid ning brausida veebi võimalikult anonüümselt. Seetõttu on antud kasutusvaldkonna jaoks oluline brauseriseaded 3. osapoole küpsiste keelamine, DNT, sirvimisandmete kustutamine, *fingerprinti* blokeerimine ja privaatsusrežiim.

Pangandusvaldkonnas sisestab kasutaja oma andmeid ja parooli. Sealjuures on mugav, aga samas ka turvalisuse lähtepunktist oluline, et paroolid luuakse tugevad. Oluline on ka turvaline krüpteeritud ühendus. Pangalahekülje aadressi sisestamisel on oluline tuvastada ära vigane veebipangalehe aadress.

Uurimistöö kirjutamine hõlmab endast mitmete veebilehtede külastamist, mistõttu on oluline, et kasutajal oleks turvaline krüpteeritud ühendus, samuti ka kaitse andmete kogumise eest, mis enamikele veebilehtedele on omane. Internetis võib otsingute käigus sattuda kohtadesse, kus klikitavad väljad võivad avada hüplikaknaid, mis võivad omakorda kasutajat suunata pahavara juurde või andmepüügi eesmärgil toimivatele lehekülgedele.

3.4 Brauseri hinnangu andmise tulemused

Tabel 6 näitab ära brauserite hinnangud enne valem 1 rakendamist. Üldise parima skoori saavutas enne valem 1 rakendamist Brave. Esimese ja teise parima skoori vahel oli 3 punkti ning madalaima skooriga brauser erines kõrgeima skooriga brauserist 6 punkti võrra.

Tabel 6. Hinnangud brauseritele.

Seade/Testitulemus	Brauseri nimetus				
	Google Chrome	Brave	MS Edge	Mozilla Firefox	Tor Browser
BrowserAudit'i testid	4	4	4	4	3
Hüplikakende blokeerimine	1	1	1	1	1
Veebisaidi kirjavigadevastane kaitse	0	0	1	0	0
Tugeva parooli genereerimine	1	1	1	1	0
<i>HTTPS mode</i>	1	1	0	1	1
Ohtlike allalaadimiste blokeerimine	1	1	1	1	1
Sirvimisandmete kustutamine	1	1	1	1	1
<i>Fingerprinti</i> blokeerimine	0	1	1	1	0
3.osapoole küpsiste keelamine	1	1	1	1	0
DNT	1	1	1	1	0
Privaatsusrežiim	1	1	1	1	1
<i>Fingerprinti</i> unikaalsus	0	1	0	0	1
Jälgijate blokeerimine	0	2	0	1	2
Kaitse 3.osapoole jälgimise eest	0	2	0	1	2
Summa	12	18	13	15	13

Järgnevalt tuuakse välja tulemused pärast valem 1 rakendamist ja antakse soovitusel turvaliseima brauseri valikuks. Tabel 7 näitab brauseritele hinnangu andmise tulemusi sotsiaalmeedias kasutamise jaoks.

Tabel 7. Hinnangu tulemused sotsiaalmeedias kasutamise jaoks.

Seade/Testitulemus	Brauseri nimetus				
	Google Chrome	Brave	MS Edge	Mozilla Firefox	Tor Browser
BrowserAudit'i testid	12	12	12	12	9
Hüplikakende blokeerimine	2	2	2	2	2
Veebisaidi kirjavigadevastane kaitse	0	0	1	0	0
Tugeva parooli genereerimine	2	2	2	2	0
<i>HTTPS mode</i>	2	2	0	2	2
Ohtlike allalaadimiste blokeerimine	1	1	1	1	1

Seade/Testitulemus	Brauseri nimetus				
	Google Chrome	Brave	MS Edge	Mozilla Firefox	Tor Browser
Sirvimisandmete kustutamine	3	3	3	3	3
<i>Fingerprinti</i> blokeerimine	0	3	3	3	0
3.osapoole küpsiste keelamine	3	3	3	3	0
DNT	3	3	3	3	0
Privaatsusrežiim	3	3	3	3	3
<i>Fingerprinti</i> unikaalsus	0	3	0	0	3
Jälgijate blokeerimine	0	6	0	3	6
Kaitse 3.osapoole jälgimise eest	0	6	0	3	6
Summa	31	49	33	40	35

Turvalisem veebibrauser sotsiaalmeedias kasutamise jaoks on Brave. Tabel 8 näitab hinnangu andmise tulemusi sotsiaalmeedias kasutamise jaoks.

Tabel 8. Hinnangu tulemused pangandusvaldkonna jaoks.

Seade/Testitulemus	Brauseri nimetus				
	Google Chrome	Brave	MS Edge	Mozilla Firefox	Tor Browser
BrowserAudit'i testid	12	12	12	12	9
Hüplikakende blokeerimine	1	1	1	1	1
Veebisaidi kirjavigadevastane kaitse	0	0	2	0	0
Tugeva parooli genereerimine	3	3	3	3	0
<i>HTTPS mode</i>	3	3	0	3	3
Ohtlike allalaadimiste blokeerimine	1	1	1	1	1
Sirvimisandmete kustutamine	2	2	2	2	2
<i>Fingerprinti</i> blokeerimine	0	2	2	2	0
3.osapoole küpsiste keelamine	2	2	2	2	0
DNT	1	1	1	1	0
Privaatsusrežiim	1	1	1	1	1
<i>Fingerprinti</i> unikaalsus	0	3	0	0	3
Jälgijate blokeerimine	0	6	0	3	6
Kaitse 3.osapoole jälgimise eest	0	6	0	3	6
Summa	35	50	37	41	41

Turvaliseim veebibrauser pangandusvaldkonna jaoks on Brave. Võrdse punktiskoori saavutasid Mozilla Firefox ja Tor Browser.

Tor Browser pole siiski pangandusvaldkonna jaoks sobilik, arvestades peatükis 3.1 selgunud asjaolu, et osasid pangandus- või uudisteteemalisi veebilehti pole võimalik Tor Browser'i kasutamise tõttu külastada. Tabel 9 näitab hinnangu andmise tulemusi uurimistöõ kirjutamise jaoks.

Tabel 9. Hinnangu andmise tulemused uurimistöõ kirjutamise jaoks.

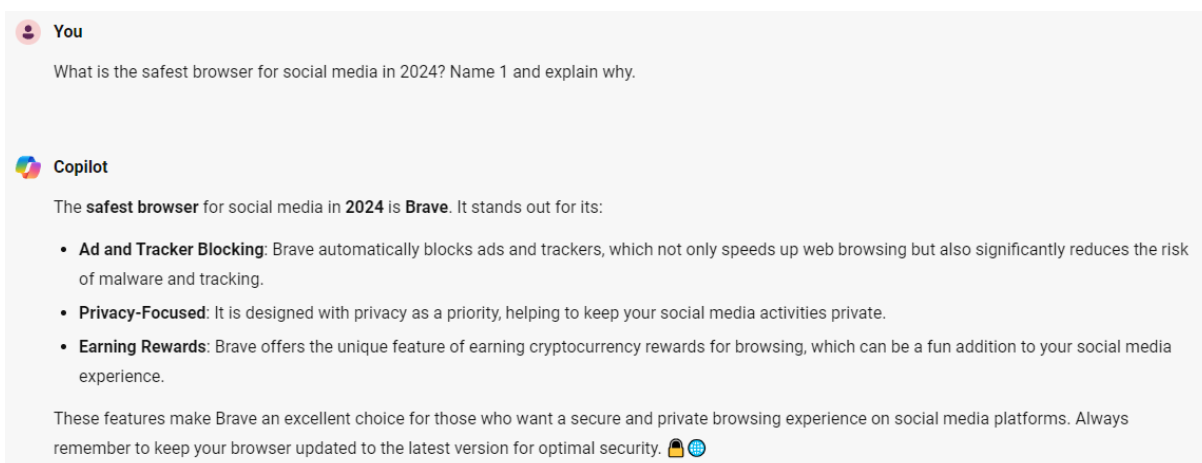
Seade/Testitulemus	Brauseri nimetus				
	Google Chrome	Brave	MS Edge	Mozilla Firefox	Tor Browser
BrowserAudit'i testid	12	12	12	12	9
Hüplikakende blokeerimine	3	3	3	3	3
Veebisaidi kirjavigadevastane kaitse	0	0	6	0	0
Tugeva parooli genereerimine	3	3	3	3	0
<i>HTTPS mode</i>	9	9	0	9	9
Ohtlike allalaadimiste blokeerimine	3	3	3	3	3
Sirvimisandmete kustutamine	4	4	4	4	4
<i>Fingerprinti</i> blokeerimine	0	4	4	4	0
3.osapoole küpsiste keelamine	6	6	6	6	0
DNT	3	3	3	3	0
Privaatsusrežiim	3	3	3	3	3
<i>Fingerprinti</i> unikaalsus	0	3	0	0	3
Jälgijate blokeerimine	0	6	0	3	6
Kaitse 3.osapoole jälgimise eest	0	6	0	3	6
Summa	46	65	47	51	46

Turvaliseim veebibrauser uurimistöõ kirjutamiseks on Brave.

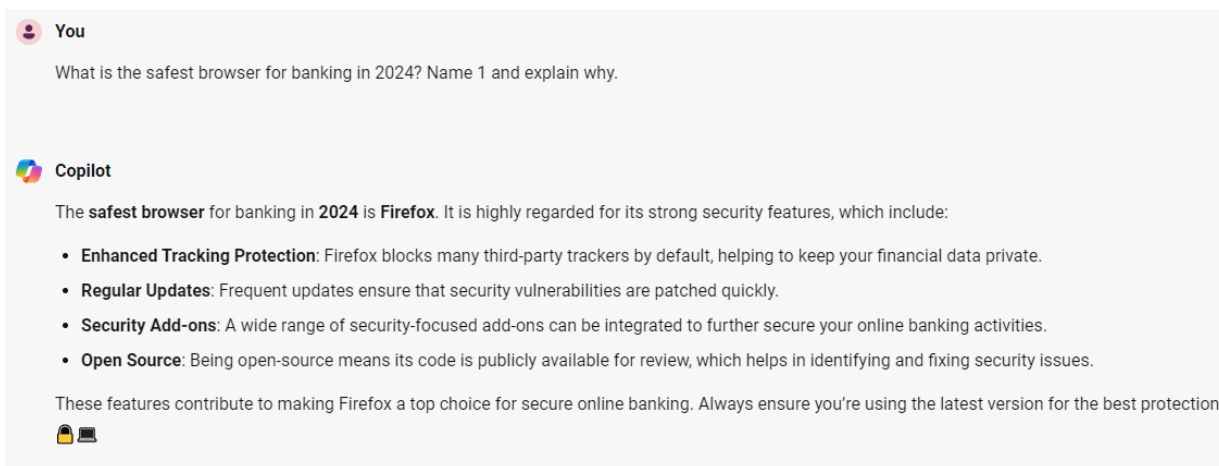
Testimistulemuste põhjal võib väita, et iga kasutusvaldkonna (sotsiaalmeedia, pangandus, uurimistöõ kirjutamine) jaoks sobib kasutada Brave'i brauserit. Olenemata veebisaidi kirjavigadevastase kaitse puudumisest, kaalub teiste seadete olemasolu üle MS Edge'i valiku. Mitmete turvalisus- ja privaatusseadete olemasolu ja kõrged tulemused BrowserAuditi ja Panopticklick'i testides teevad Brave'ist turvalise brauseri.

3.5 Võrdlus MS Copilot'i poolt antud soovitustega


Tehisintellektile esitatud küsimused formuleeriti ühtse struktuuri järgi, arvestades asjakohasust (2024. aasta) ja kasutusvaldkonda (sotsiaalmeedia; pangandus; uurimistöö kirjutamine). MS Copilot'il paluti nimetada üksainus turvalisem brauser ja anda ka seletus. Joonised 12-14 esitavad MS Copilot'i brauserite soovitused iga kasutusvaldkonna jaoks. Tehisintellekti soovitusi võrreldakse peatükis 3.4 välja toodud brauserite hinnangutega.




Joonis 12. Turvalisem brauser sotsiaalmeedia jaoks MS Copilot'i soovitustel [53].



Joonis 13. Turvalisema brauser panganduseks MS Copilot'i soovitustel [53].

 **You**

What is the safest browser for writing a research paper in 2024? Name 1 and explain why.

 **Copilot**

The **safest browser** for writing a research paper in **2024** is **Mozilla Firefox**. It is highly recommended for its:

- **Security and Privacy:** Firefox offers strong protection against tracking, ensuring your research activities remain private.
- **Customizability:** You can tailor the browser with various add-ons and extensions, which can be particularly useful for research purposes.
- **Reliability:** Regular updates and an open-source nature mean that any security vulnerabilities are quickly addressed.

These features make Firefox a secure and reliable choice for conducting research and writing papers online. Always ensure you're using the latest version for the best protection. 🛡️📄

Joonis 14. Turvalisem brauser uurimistöö kirjutamiseks MS Copilot'i soovitusel [53].

Nii nagu töö tulemustes, oli ka MS Copilot'i soovitus kasutada sotsiaalmeedias Brave'i. Panganduses ja uurimistöö kirjutamisel erinesid MS Copilot'i soovitusel brauserite hinnangu andmise tulemustest. Brauseri seadete olemasolu kirjeldavas tabelis 3 on näha, et Brave'i kasutamine võimaldab peaaegu kõigi turvalisus- ja privaatsusseadete reguleerimist. Firefox on hea alternatiiv Brave'ile, kuid seda ei saa antud töö raames soovitada unikaalse *fingerprinti* ja vaid osalise jälgijate blokeerimise tulemuste tõttu (Tabel 4).

Kokkuvõte

Antud töö eesmärgiks oli anda metoodika, kuidas konkreetse kasutusvaldkonna jaoks valida brauserite hulgast välja turvalisem. Näitena selgitati välja turvalisem brauser järgmiste valdkondade jaoks: sotsiaalmeedia, pangandus ning uurimistöö kirjutamine. Loodud metoodika kasutamine kolme valdkonna peal toimis ning leidis osalist kinnitust tehisintellektilt.

Töös vaadeldi viite erinevat veebibrauserit ja võrreldi nende põhiomadusi, kontrolliti brauserite turvalisus- ja privaatsusseadete olemasolu ning viidi läbi brauseri *fingerprinti* ja ehituse testid, mille põhjal anti igale brauserile vastavalt kasutusvaldkonnale hinnang, kasutades lõputöös käsitletud metoodikat. Hinnangu andmise tulemusi võrreldi AI soovitusetega.

Töö tulemusena selgus, et kõigi kolme kasutusvaldkonna (sotsiaalmeedia, pangandus, uurimistöö kirjutamine) jaoks turvalisem brauser on Brave. Tehisintellekti soovitusete põhjal on sotsiaalmeedia jaoks turvalisem brauser Brave, panganduses ja uurimistöö kirjutamiseks Mozilla Firefox.

Töö raames brauseritest tehtud ülevaated, seadete analüüs ja testimimetoodika on lugejale abiks brauserite turvalisuse hindamisel. Töös rakendatud metoodika abil on võimalik valida eri kasutusvaldkonna jaoks turvalisem brauser. Tehisintellekti soovitused näitavad, et turvalisemad brauserid on sõltuvalt kasutusvaldkonnast erinevad.

Kasutatud allikad

- [1] GlobalStats, „Browser Market Share Worldwide,“ [Võrgumaterjal]. Available: <https://gs.statcounter.com/browser-market-share#monthly-202301-202312>. [Kasutatud 09. 03. 2024].
- [2] I. T. Ketan, „Google’s Chrome is the Leading Web Browser in 2023,“ [Võrgumaterjal]. Available: <https://www.marketresearchfuture.com/news/google-s-chrome-is-the-leading-web-browser-in-2023>. [Kasutatud 10. 03. 2024].
- [3] Google, „Google Search bar,“ [Võrgumaterjal]. Available: <https://www.google.com/chrome/browser-features/#google-search-bar>. [Kasutatud 10. 03. 2024].
- [4] W. L. Hosch, „Chrome Internet browser,“ [Võrgumaterjal]. Available: <https://www.britannica.com/technology/Chrome>. [Kasutatud 10. 03. 2024].
- [5] McAfee, „What is a safe browser?,“ [Võrgumaterjal]. Available: <https://www.mcafee.com/en-us/safe-browser.html>. [Kasutatud 11. 03. 2024].
- [6] D. Athow, „Brave browser review,“ [Võrgumaterjal]. Available: <https://www.techradar.com/reviews/brave-web-browser>. [Kasutatud 10. 03. 2024].
- [7] R. Shewale, „35+ Chrome Statistics for 2024 (Users, Data & Facts),“ [Võrgumaterjal]. Available: <https://www.demandsage.com/chrome-statistics/>. [Kasutatud 11. 03. 2024].
- [8] A. Powell, „The Fall of Internet Explorer: Where It Lost Out to Rivals,“ [Võrgumaterjal]. Available: <https://tinyurl.com/2x8xyz4m>. [Kasutatud 11. 03. 2024].
- [9] K. Yasar, „What is Microsoft Edge? A Definition from TechTarget.com,“ [Võrgumaterjal]. Available: <https://tinyurl.com/yv8akym3>. [Kasutatud 11. 03. 2024].
- [10] L. Whitney, „Better Than Chrome: 21 Hidden Tricks Inside Microsoft's Edge Browser,“ [Võrgumaterjal]. Available: <https://www.pcmag.com/how-to/microsoft-edge-browser-tips-tricks>. [Kasutatud 11. 03. 2024].
- [11] mdn web docs, „MDN Web Docs Glossary: Mozilla Firefox,“ [Võrgumaterjal]. Available: https://developer.mozilla.org/en-US/docs/Glossary/Mozilla_Firefox. [Kasutatud 12. 03. 2024].
- [12] N. Barney, „What is Firefox? | Definition from TechTarget,“ [Võrgumaterjal]. Available: <https://www.techtarget.com/whatis/definition/Firefox>. [Kasutatud 12. 03. 2024].
- [13] J. Keeley, „What Are the Different Versions of Firefox (And Which One Is Best for You)?,“ [Võrgumaterjal]. Available: <https://www.makeuseof.com/tag/different-versions-firefox/>. [Kasutatud 12. 03. 2024].

- [14] The Final Hop, „The History of the Tor Project: A Journey Towards Internet Freedom,“ [Võrgumaterjal]. Available: <https://www.thefinalhop.com/the-history-of-the-tor-project-a-journey-towards-internet-freedom/>. [Kasutatud 13. 03. 2024].
- [15] The Tor Project, „Tor Project | History,“ [Võrgumaterjal]. Available: <https://www.torproject.org/about/history/>. [Kasutatud 14. 03. 2024].
- [16] Kaspersky, „Tor Browser: What is it and is it safe?,“ [Võrgumaterjal]. Available: <https://www.kaspersky.com/resource-center/definitions/what-is-the-tor-browser>. [Kasutatud 14. 03. 2024].
- [17] D. Jayasekara, „Deep Dive Into TOR (The Onion Router),“ [Võrgumaterjal]. Available: <https://blog.insiderattack.net/deep-dive-into-tor-the-onion-router-6de4c25beba7>. [Kasutatud 18. 04. 2024].
- [18] The Tor Project, „Which platforms is Tor Browser available for?,“ [Võrgumaterjal]. Available: <https://support.torproject.org/tbb/tbb-31/>. [Kasutatud 15. 03. 2024].
- [19] mtigas, „Tor at the Heart: Onion Browser (and more iOS Tor),“ [Võrgumaterjal]. Available: <https://blog.torproject.org/tor-heart-onion-browser-and-more-ios-tor/>. [Kasutatud 15. 03. 2024].
- [20] A. Rimeikis, „11 tools to test browser security in 2024,“ [Võrgumaterjal]. Available: <https://surfshark.com/blog/browser-security-test>. [Kasutatud 29. 03. 2024].
- [21] T.-H. Leinberg, „Veebibrauseri valik nutiseadmete kasutajatele,“ [Võrgumaterjal]. Available: <https://digikogu.taltech.ee/et/Item/aff26f8b-3003-4f35-8305-bd022848a51f>. [Kasutatud 02. 01. 2024].
- [22] Tartu Ülikooli arvutiteaduse instituut, „Veebibrauserid,“ [Võrgumaterjal]. Available: <https://courses.cs.ut.ee/t/infoturvekoolis/Main/Veebibrauserid>. [Kasutatud 30. 03. 2024].
- [23] mdn web docs, „Origin,“ [Võrgumaterjal]. Available: <https://developer.mozilla.org/en-US/docs/Glossary/Origin>. [Kasutatud 19. 03. 2024].
- [24] M. Kosaka, „Same-origin policy,“ [Võrgumaterjal]. Available: <https://tinyurl.com/3kta385c>. [Kasutatud 19. 03. 2024].
- [25] mdn web docs, [Võrgumaterjal]. Available: <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>. [Kasutatud 19. 03. 2024].
- [26] Amazon Web Services, „What is Cross-Origin Resource Sharing?,“ [Võrgumaterjal]. Available: <https://tinyurl.com/mp6w9e6y>. [Kasutatud 19. 03. 2024].
- [27] BrowserAudit, „Choose Test Categories,“ [Võrgumaterjal]. Available: <https://browseraudit.com/>. [Kasutatud 20. 03. 2024].
- [28] A. Durzyńska, „What are pop-ups? Definition, types, and examples,“ [Võrgumaterjal]. Available: <https://www.getresponse.com/blog/what-are-popups#:~:R1i>. [Kasutatud 24. 03. 2024].
- [29] S. P, „Enable Disable Website Typo Protection in Edge Browser,“ [Võrgumaterjal]. Available: <https://tinyurl.com/2w7h5zzv>. [Kasutatud 26. 03. 2024].
- [30] Microsoft, „What is typosquatting?,“ [Võrgumaterjal]. Available: <https://tinyurl.com/4y9rnhh6>. [Kasutatud 26. 03. 2024].

- [31] Amazon Web Services, „What’s the Difference Between HTTP and HTTPS?“, [Võrgumaterjal]. Available: <https://tinyurl.com/ywfyws4>. [Kasutatud 03. 05. 2024].
- [32] CCleaner, „What is browsing data?“, [Võrgumaterjal]. Available: https://support.ccleaner.com/s/article/what-is-browsing-data?language=en_US. [Kasutatud 20. 03. 2024].
- [33] Brave Privacy Team, „Brave browser simplifies its fingerprinting protections“, [Võrgumaterjal]. Available: <https://tinyurl.com/3sczs8as>. [Kasutatud 20. 03. 2024].
- [34] Brave, „Privacy Glossary Fingerprinting“, [Võrgumaterjal]. Available: <https://brave.com/glossary/fingerprinting/>. [Kasutatud 18. 04. 2024].
- [35] K. Yasar, „What is a Third-Party Cookie | Definition from TechTarget“, [Võrgumaterjal]. Available: <https://www.techtarget.com/whatis/definition/third-party-cookie>. [Kasutatud 26. 03. 2024].
- [36] Cookiebot, „No more cookies? Google ending third-party cookies in Chrome“, [Võrgumaterjal]. Available: <https://www.cookiebot.com/en/google-third-party-cookies/>. [Kasutatud 26. 03. 2024].
- [37] Cookieyes, „What is Do Not Track? (DNT)“, [Võrgumaterjal]. Available: <https://www.cookieyes.com/knowledge-base/cookies-101/what-is-do-not-track/>. [Kasutatud 26. 03. 2024].
- [38] Mozilla Corporation, „Incognito browser: What it really means“, [Võrgumaterjal]. Available: <https://tinyurl.com/4kvhwe59>. [Kasutatud 25. 03. 2024].
- [39] iom2222, „Is a Brave Private Window with Tor Connectivity as good as the TOR browser?“, [Võrgumaterjal]. Available: <https://tinyurl.com/yc4yk85x>. [Kasutatud 25. 03. 2024].
- [40] K. Kikkas, „Interneti kasutaja anonüümse tuvastuse meetodite kasutamine kaubanduslikel eesmärkidel“, [Võrgumaterjal]. Available: <https://tinyurl.com/vtwfbh5v>. [Kasutatud 10. 03. 2024].
- [41] T. Kadar, „What Is Browser Fingerprinting & How Does It Work?“, [Võrgumaterjal]. Available: <https://tinyurl.com/2vawburu>. [Kasutatud 09. 03. 2024].
- [42] OpenAI, „Introducing ChatGPT“, [Võrgumaterjal]. Available: <https://openai.com/blog/chatgpt>. [Kasutatud 22. 02. 2024].
- [43] E. G. Dsouza, „How ChatGPT Works: Training Model of ChatGPT“, [Võrgumaterjal]. Available: <https://www.edureka.co/blog/how-chatgpt-works-training-model-of-chatgpt/>. [Kasutatud 22. 02. 2024].
- [44] ERR, „uudised | ERR“, [Võrgumaterjal]. Available: <https://www.err.ee/>. [Kasutatud 21. 04. 2024].
- [45] Delfi, „Delfi“, [Võrgumaterjal]. Available: <https://www.delfi.ee/>. [Kasutatud 21. 04. 2024].
- [46] Äripäev, „Majandus- ja äriuudised Eestist ja välismaalt“, [Võrgumaterjal]. Available: <https://www.aripaev.ee/>. [Kasutatud 21. 04. 2024].
- [47] LHV, „LHV“, [Võrgumaterjal]. Available: <https://www.lhv.ee/>. [Kasutatud 21. 04. 2024].
- [48] SEB, „Koduleht | SEB“, [Võrgumaterjal]. Available: <https://www.seb.ee/>. [Kasutatud 21. 04. 2024].

- [49] Luminor, „Luminor - paindlik ja tulevikku vaatav pank,“ [Võrgumaterjal]. Available: <https://luminor.ee/>. [Kasutatud 21. 04. 2024].
- [50] Tallinna Ülikool, „| Tallinna Ülikool,“ [Võrgumaterjal]. Available: <https://www.tlu.ee/>. [Kasutatud 21. 04. 2024].
- [51] Tartu Ülikool, „Avaleht | Tartu Ülikool,“ [Võrgumaterjal]. Available: <https://ut.ee/et/avaleht>. [Kasutatud 21. 04. 2024].
- [52] TalTech, „Ülikool | TalTech on Eesti uuendusmeelseim ülikool,“ [Võrgumaterjal]. Available: <https://taltech.ee/>. [Kasutatud 21. 04. 2024].
- [53] Microsoft, „Copilot,“ [Võrgumaterjal]. Available: <https://copilot.microsoft.com/>. [Kasutatud 30. 04. 2024].
- [54] Brave, „Brave Browser icon,“ [Võrgumaterjal]. Available: <https://uxwing.com/brave-browser-icon/>. [Kasutatud 09. 03. 2024].
- [55] WikimediaImages, „Google Chrome Logo,“ [Võrgumaterjal]. Available: <https://tinyurl.com/3pkud9jd>. [Kasutatud 09. 03. 2024].
- [56] The Tor Project, „Tor Browser icon (New).png,“ [Võrgumaterjal]. Available: https://en.m.wikipedia.org/wiki/File:Tor_Browser_icon_%28New%29.png. [Kasutatud 09. 03. 2024].
- [57] M. Corporation, „Microsoft Edge logo (2019).png,“ [Võrgumaterjal]. Available: <https://tinyurl.com/mupaszfy>. [Kasutatud 09. 03. 2024].
- [58] Mozilla Corporation, „firefox-logo,“ [Võrgumaterjal]. Available: <https://blog.mozilla.org/opendesign/evolving-the-firefox-brand/firefox-logo/>. [Kasutatud 09. 03. 2024].

Lisa 1 – Lingid brauserite testimistulemustele

Lingid brauserite BrowserAudit'i testimistulemustele:

Google Chrome

<https://browseraudit.com/results/203341/0247eec47ce7ead6eb620c0013f27a8b3cb05596>

Mozilla Firefox

<https://browseraudit.com/results/203344/205a5169c1a0faf030976b8b74282fb15a5aea1c>

Brave

<https://browseraudit.com/results/203345/b46d8c57ec315068eefd5faa57ab57677582cac1>

Tor Browser

<https://browseraudit.com/results/203352/b66cffad408423f7866a32c99cbe49ce3847e041>

MS Edge

<https://browseraudit.com/results/203346/831c41fb723fd255eb41c442063a2397de56a14f>

Link Google Drive'i Panopticlick'i testimistulemuste kaustale:

Google Chrome, Mozilla Firefox, Brave, Tor Browser, MS Edge

<https://tinyurl.com/mry4t8xe>

Lisa 2 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks¹

Mina, Erik-Martin Feldberg

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Veebibrauserite turvalisus ja AI“, mille juhendaja on Vladimir Viies
 - 1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
 - 1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

07.05.2024

¹ Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingu tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.