GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 11, Issue 04, April (2023)

COMBINED APPLICATION OF FILTERING ALGORITHMS IN ENSURING TRAFFIC SECURITY

Alisher Samandarovich Matyakubov
Sanjar Kadirugli Esonmurodov
National University of Uzbekistan named after Mirzo Ulugbek

ABSTRACT

The article talks about the joint use of filtering algorithms in ensuring traffic safety.

Keywords: traffic, filtering, algorithms, use of filtering algorithms.

TRAFIK XAVFSIZLIGINI TA'MINLASHDA FILTRLASH ALGORITMLARINI BIRGALIKDA QO'LLASH

Matyakubov Alisher Samandarovich
Esonmurodov Sanjar Qodir o`g`li
Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti

ANNOTATSIYA

maqolada trafik xavfsizligini ta'minlashda filtrlash algoritmlarini birgalikda qo'llash haqida gap brogan.

Kalit so'zlar: trafik, filtrlash, lgoritmlar, filtrlash algoritmlaridan foydalanish.

Hozirgi kunda internet, axborot texnologiyalari degan tuhsunchalar har bir xonadonga kirib olgani sir emas. Bugungi kunning asosiy muommolari bo'lib qolayotgan tushunchalar "Trafik", "ma'lumot xavfsizligi", "yoshlarni turli oqimlardan saqlash", "diniy ekstremizm" va shunga o'xshash nafaqat yoshlar balki barchani birdek sergak turishimizga chorlayotgan tushunchalardir. Bu muammoni hal qilishda biz taklif qilayotgan usul – birgalikda qo'llangan filtrlash algoritmlaridan foydalanishdir [1-4].

Asosan filtrlash algoritmlari quyidagilardan iborat:

- Signature-based filtering: bu algoritm oldindan bizga berilgan maxsus imzo va kalit so'zlar orqali kelayotgan ma'lumotni bizga xavfli tomoni bor yoki yo'qligini aniqlab beradi, bu usul asosan oldin ko'rilgan xavflardan xulosa qilib uni topsihda yordam beradi, ammo no'malum tahdidlarda foydasi tegmaydi.
- Behavior-based filtering: bu asosan ma'lumotlarni uzatish va qabul qilsihda shubhali va noodatiy yo'llardan foydalanishda ishlatiladi.
- Machine learning-based filter: bu turdagi fitrlar asosan katta hajmdagi ma'lumotni tahlil qilish va tahdid mavjudligini ko'rsatishda yordam beradi. Mashina o'rganishga asoslangan filtrlar yangi yoki noma'lum tahdidlarni aniqlashda samarali bo'lishi mumkin, ammo ular katta hajmdagi o'quv ma'lumotlarini talab qiladi, aniq va maqsadli hujumlarni aniqlashda samarasiz bo'lishi mumkin.

• Content-based filter: ushbu turdagi filtrlash ruxsat etilgan yoki bloklanganligini aniqlash uchun ma'lumotlarning haqiqiy mazmunini tahlil qiladi. Masalan, kontentga asoslangan filtrlar muayyan kalit so‘zlar yoki kontent turlarini o‘z ichiga olgan trafikni bloklashi mumkin.

• Reputation-based filtering: ushbu turdagi filrlash malumot kelayotgan Ip va domen ga asoslanadi.

• Protocol-based filtering:Ushbu turdagi filtrlash ruxsat etilgan yoki bloklanganligini aniqlash uchun ma'lumotlarni uzatish uchun ishlatiladigan maxsus protokollarni ko‘rib chiqadi. Masalan, protokolga asoslangan filtrlar zararli faoliyat bilan bog'liq bo‘lgan ma'lum turdagi protokollardan foydalanadigan trafikni bloklashi mumkin.

• Url filter: bu filtr to‘ri asosan url manzillar va oldindan ma’lum bo‘lgan saytlarni bloklashda aniq ma’lumotga qarab bizga xabar beradi.

Shunga o‘xshash yana ba’zi algoritmlarni misol keltirish mumkin.

Biz taklif qilayotgan usul asosan 4 ta algoritmni birgalikda quyidagi ketma-ketlikda umumiy qo‘llashga mo‘ljallgan. Bular: Signature-based, Machine learning-based, Content-based va Url based algoritmlari. Bu algoritmlar bazadagi ma’ulumotlar ko‘payishi bilan samaradorligi ham oshib boradi, masalan signature-based filtrni ko‘rsak:

```
public static boolean isBad(String input) {
String[] patterns = {
"';(?:--[^-]*)?\\n|\\b(?:drop|select|truncate|alter)\\b",
"<script>(.*?)</script>",
";ls",
"\\.\\./\\.\\.",
"\\.exe|\\.dll|\\.js|\\.vbs|\\.hta"
};

for (String pattern : patterns) {
Pattern regex = Pattern.compile(pattern, Pattern.CASE_INSENSITIVE);
Matcher matcher = regex.matcher(input);
if (matcher.find()) {
return true;
}
}
return false;
}
```

Bu algoritm ko‘rinib turibdiki patterns(baza) dagi malumotlar ko‘paygani bilan samaradorligi oshib boradi.

Biz shu algorimlarni birga qo‘llashni ko‘rib chiqaylik:

Avvalambor har bir kelgan ma’lumot har bir bosqich bo‘yicha tekshiriladi va bizda “qora ro‘yhat” shakllanib boradi. **java** dasturlash tilida foydalanayotganimiz sababli tezlik jihatdan bizga yordam beradigan xesh funksiyalaridan foydalanamiz:

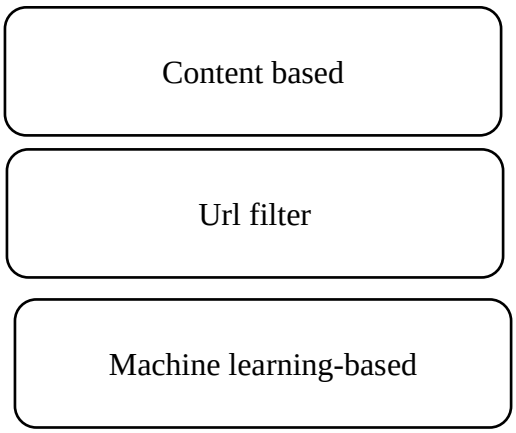
```
EnumMap<FilterType, Function<String, Boolean>> checkFilters;
```

buning uchun ularni enummap tipidagi va har bir filtr turi bo‘yicha yurib chiqamiz, hashmap imizga qo‘shib olamiz:

```
checkFilters.put(FilterType.SIGNATURE_BASED, this::checkSignature);
```

```
checkFilters.put(FilterType.MACHINE_LEARNING, this::checkMachine);
checkFilters.put(FilterType.URL_FILTERING, this::checkUrlFilter);
checkFilters.put(FilterType.CONTENT_FILTERING, this::checkContentFilter);
```

Davomida har bir Filtr turi bo‘yicha tekshirganimizda ma’lumotlar bazamizni boyitib boramiz va bu bizda ma’um vaqtdan so‘ng filtrlarimizning samaradorligini oshirib beradi.



Yana shuni aytib o‘tish kerakki, hozirgi kunda tashkilotlarda ba’zi bir cheklovlar tufayli trafik to‘liq bartaraf etilmagan va bu ko‘plab muammolarni keltirib chiqaradi masalan:

- Signature based-filter ga haddan tashqari ishonish. Bu filtrlar ma'lum tahdidlarni aniqlashda samarali bo‘lishi mumkin, ammo ular yangi yoki noma'lum tahdidlarni aniqlashda unchalik samarali emas. Bu filtrlarga haddan tashqari ishonish noto‘g'ri xavfsizlik tuyg'usiga olib kelishi va tashkilotlarni yangi va paydo bo‘layotgan tahdidlarga qarshi himoyasiz qoldirishi mumkin.
- Machine learning-based yomon: Mashina o‘rganishga asoslangan filtrlar samarali bo‘lishi uchun katta hajmdagi o‘quv ma'lumotlarini talab qiladi. Agar tashkilot yetarlicha ta'lim ma'lumotlariga kirish imkoniga ega bo‘lmasa yoki ma'lumotlar tashkilot duch kelishi mumkin bo‘lgan tahdidlar turlarini aks ettirmasa, filtr tahdidlarni aniqlashda samarasiz bo‘lishi mumkin.

• Maqsadli hujumlarni aniqlash va blok qilishda qiyinchilik: Ba'zi hujum turlari, masalan, “spear phishing” yoki “social engineering attacks” hujumlari juda maqsadli bo‘lib, boshqa tahdid turlari bilan bir xil kalit yoki xatti-harakatlarni namoyish etmasligi mumkin. Ushbu turdagi hujumlarni aniqlash va blok qilish an'anaviy filtrlash algoritmlari yordamida qiyin bo‘lishi mumkin.

• Noto‘g'ri pozitivlar: Filtrlash algoritmlari ba'zan noto‘g'ri ravishda yaxshi trafikni zararli deb aniqlashi va uni bloklashi mumkin, natijada noto‘g'ri ijobiy natijaga olib keladi. Noto‘g'ri pozitivlar biznes operatsiyalarini buzishi va filtrlash tizimiga ishonchni yo‘qotishi mumkin.

Ushbu qiyinchiliklar va cheklovlarga qaramay, filtrlash algoritmlari harakat xavfsizligini ta'minlashning muhim vositasi bo‘lib qolmoqda. Filtrlarni sinchkovlik bilan tanlash va sozlash, shuningdek, turli xil filtrlar kombinatsiyasidan foydalangan holda, tashkilotlar veb-ga asoslangan tahdidlarga qarshi yanada samarali himoya yaratishi mumkin shu bilan birga Eng so‘nggi tahdidlarga qarshi samarali bo‘lishini ta'minlash uchun filtrlar to‘g'ri sozlangan va muntazam ravishda yangilanganligiga ishonch hosil qiling.

Hozirgi kunda ko‘plab davlat korxonalari quyidagi control tizimlaridan foydalanib keladi va bu tizimlarning o‘ziga yarasha bir nechta kamchiliklari bor, Masalan:

• Faqat bitta algoritm: Bu dasturlarning noqulayliklari shunda ular asosan Signature based algoritmiga asoslangan va bazadagi bor ma’lumotlar bilan juda yaxshi ishlaydi ammo yangi cheklov quyilmagan malumotlarda deyarli ishlamaydi.

• Set bilan sozlangan: agar set bilan cheklov olib qo‘yilsa demak bunda foydalanuvchi uzi xohlagan malumotni olib kurishi mumkin bo‘ladi.

Biz ilgari so‘rayotgan yechimda 1-muammo ko‘p miqdorda hal qilinadi, sonlarda ko‘rsak(ma’lumot loglar yoziladigan file yasalib, random generatsiya so‘z qilindi va tekshiriildi):

-> Oddiy usulda faqat bitta algoritm ishlaganda xavfsizlik darajasi: 23%

-> Birgalikda qO‘llangan algoritmda : 79%

Bu algoritmlarni birgalikda qo‘llash va ma’lumotni yagona bazada olib kelish bizga juda katta samara berish extimoli bilan birga agar ma’lumot noto‘g’ri yozilib quyiladigan bulsa bizga zarali bullishi ham mumkin. Buni aniq tekshirish va yozilayotgan dastur to‘g’ri ishlashiga amin bo‘lgach qo‘llash tavsiya qilinadi. Yuqorida ko‘rganimizdek bu bizga yetarlicha samara beradi.

Foydalanilgan adabiyotlar

1. Matyakubov A.S., Tadjiyev R.N. Esonmurodov S.Q. The role of information technology in modern medicine. Web of Scientist: International Scientific Research Journal (WoS), Vol. 3, No. 7, (2022).
2. Tadjiev R.N., & Esonmurodov S.Q. (2022). Network traffic analysis and ip packet processing monitoring in Linux OS. European Journal of Interdisciplinary Research and Development, 5, 41–47.
3. Matyakubov A.S., Tadjiyev R.N., Komilov R.K. Kiruvchi va chiquvchi tarmoq trafigini tekshirish va boshqarishning ilg’or usullari. Халқаро илмий-амалий анжуман материаллари, Бухоро давлат университети, 2022.
4. Matyakubov A.S., Tadjiyev R.N., Komilov R.K. Kiruvchi va chiquvchi tarmoq trafigini *deep packet inspection* (dpi) yordamida kiruvchi va chiquvchi trafiklarni teran tahlil qilish. Urganch, 29-30 aprel 2022-y, Xalqaro ilmiy-amaliy anjuman, 2022, 89-91 б.