

**Kauno technologijos universitetas**

Informatikos fakultetas

Programų inžinerijos katedra

**Programų sistemų inžinerija**

**p175B015**

**Application Layer (L7) Firewall component**

**HRPI analyzer**

Atliko ELITNET1:

Robertas Strazdauskas, IFF-6/7

Kazimieras Buškus, IFF-6/9

Šarūnas Andrijauskas, IFF-6/7

Tomaš Jurevič, IFF-6/1

Priėmė:

Andrej Ušaniov

# Bendra informacija

* Tvarkaraštis:

Semestro projektas: antradienis 15:30

Programų sistemų inžinerija: nelyg. sav. trečiadienis 11:00

* Programos *wiki:* https://github.com/sarand2/ELITNET1/wiki/
* Komandos narių pareigos:

Robertas Strazdauskas: GUI kūrimas ir duomenų bazė

Kazimieras Buškus: HRPI logika ir multiproceso įgyvendinimas

Šarūnas Andrijauskas: DDoS atakų generavimas ir multiproceso įgyvendinimas

Tomas Jurevič: paketų iš tinklo plokštės rinkimas

[1]. Tongguang Ni, Xiaoqing Gu, Hongyuan Wang, and Yu Li, “Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis,” Journal of Control Science and Engineering, vol. 2013, Article ID 821315, 6 pages, 2013. doi:10.1155/2013/821315

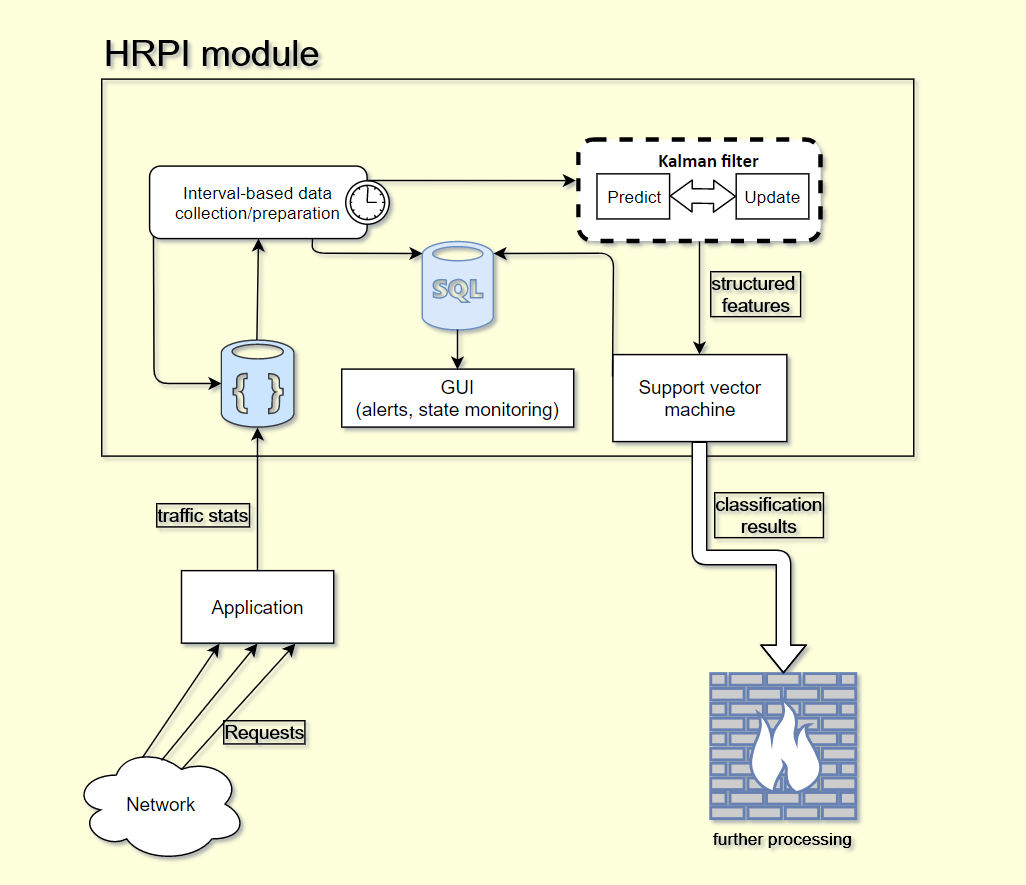
# Įvadas

# Programos idėjos aprašas

HRPI analizatorius, kuriamas pagal pateiktą matematinį modelį [1], leidžia realiu laiku aptikti aplikacijos sluoksnio DDoS atakas ir iš esmės veikia kaip vienas iš L7 ugniasienės modulių, skirtų HTTP protokolu paremtoms atakoms aptikti.

Šio komponento tikslas – pateikti efektyvią, realiu laiku galinčią veikti sistemos struktūrą bei sąveikaujančias apdorojimo funkcijas, klasifikuojančias programos lygio DDoS atakas. Analizatorius taip pat pateikia sistemos administratoriams paprastą naudoti grafinę sąsają tinklo srauto stebėjimui.

Pagrindinės funkcijos:

* Programų lygio DDoS atakų aptikimas. Šis sprendimas turi aptikti tinklo pralaidumą ir serverio resursus švaistančias HTTP GET užklausų atakas, remdamasis tam tikromis statistinėmis atakų savybėmis.
* Būsenos stebėjimas. Analizatorius teikia intuityvias tinklo srauto stebėjimo galimybes, atakos įspėjimo sistemą, ankstesnių būsenų grafikus ir manipuliacijas su istoriniais duomenimis.

pav. 1 Abstrakti sistemos architektūra