Reviews

3 ICC 2020 Symposiums

Review 1 (Reviewer A)

|  |  |  |  |
| --- | --- | --- | --- |
| Relevance and timeliness | Technical content and scientific rigour | Novelty and originality | Quality of presentation |
| Excellent (5) | Valid work but limited contribution. (3) | Some interesting ideas and results on a subject well investigated. (3) | Excellent. (5) |

**Strong aspects (Comments to the author: what are the strong aspects of the paper)**

The submitted manuscript shows a solution for designing a high performance ETA, starting from the baseline Cisco Joy ETA, compliant with x86 processors picked by a network edge. The introduction of machine learning techniques is the added value proposed for the identification of encrypted malware network flows. The most appreciable contribution of teh paper is the proposed archietecture. The paper is clear and well written.

**Weak aspects (Comments to the author: what are the weak aspects of the paper?)**

The implementation presented in the paper is based on well-known Python libraries. Although the implementation effort produced is appreciable, as well as the performance evaluation results are promising, for the novel architecture to be considered in operation in high-end system dealing very large traffic volumes some latency issues are still expected. From the point of view of ML algorithms, the paper does not include any novelties.

**Recommended changes (Please indicate any changes that should be made to the paper if accepted.)**

The paper is well structured as it is. However, it would be nice to see the achievable performance by using better equipped machines, in particular with larger RAM.

**Submission Policy (Does the paper list the same author(s), title and abstract (minor wording differences in the abstract are okay) in its PDF file and EDAS registration? (yes/no))**

Yes, it does.

Review 2 (Reviewer B)

|  |  |  |  |
| --- | --- | --- | --- |
| Relevance and timeliness | Technical content and scientific rigour | Novelty and originality | Quality of presentation |
| Good (4) | Valid work but limited contribution. (3) | Some interesting ideas and results on a subject well investigated. (3) | Well written. (4) |

**Strong aspects (Comments to the author: what are the strong aspects of the paper)**

The paper investigates the identification of network threats on encrypted traffic flows using machine learning techniques. Motivated by the usage of x86 platforms at the edge and advancements on next-generation processors, the authors propose a modification on the Cisco open-sourced ETA software Joy to multithreading processing. Also, they extend the software with three new machine-learning models.

**Weak aspects (Comments to the author: what are the weak aspects of the paper?)**

- Section 1 could be renamed introduction and motivation and Section 2 could focus on explaining Joy and how it works. Therefore, in section 3, the authors could focus on the changes and extensions made in the software. - As the paper contribution is the modification of existing software to improve performance and run in multithread processors, the authors could open the software source code to the academia for further advancements in the area, otherwise, I don't see how the readers can avail from this work. - Algorithms 1 and 2 could be represented as pipelines figures as they present sequential steps and do not have complex logical steps

**Recommended changes (Please indicate any changes that should be made to the paper if accepted.)**

The recommended changes are presented in the Weak aspects

**Submission Policy (Does the paper list the same author(s), title and abstract (minor wording differences in the abstract are okay) in its PDF file and EDAS registration? (yes/no))**

Yes

Review 3 (Reviewer C)

|  |  |  |  |
| --- | --- | --- | --- |
| Relevance and timeliness | Technical content and scientific rigour | Novelty and originality | Quality of presentation |
| Excellent (5) | Solid work of notable importance. (4) | Significant original work and novel results. (4) | Well written. (4) |

**Strong aspects (Comments to the author: what are the strong aspects of the paper)**

The paper studies the problem of encrypted traffic analytics based on machine learning, and designs a corresponding software system. The system is an improvement of Cisco's encrypted traffic analytics software Joy. The main novelties are: the system exploits multithreading and two Intel machine learning software packages, and implemented three new types of learning algorithms compared to Joy.

**Weak aspects (Comments to the author: what are the weak aspects of the paper?)**

It is mentioned that the open-sourced version of Joy only has logistic regression as the learning algorithm. Does Joy have other learning algorithms that are not open-sourced? Is the software of this paper open-sourced? In the abstract, it is said that "we are able to boost the performance by a maximum order of 32x and 46x respectively." Does performance mean running time? Do these factors refer to the overall time or the inference time? If it is only inference time, then it does not seem a fair comparison because the overall time matters more. Section III-B, the first paragraph in this paragraph may be removed since the features are summarized in the bullets next. Typo. Page 2, right column, first bullet, should be "features include"

**Recommended changes (Please indicate any changes that should be made to the paper if accepted.)**

Same as weak aspects.

**Submission Policy (Does the paper list the same author(s), title and abstract (minor wording differences in the abstract are okay) in its PDF file and EDAS registration? (yes/no))**

Yes