View Reviews

Paper ID
424

Paper Title
A Deep Learning Approach to Distributed Anomaly Detection for Edge Computing

Track Name
Main Conference

Reviewer #1

Questions

1. Recommendation
Borderline

2. Reviewer's confidence
High Confidence

3. Comments to authors
The paper discusses an approach towards anomaly detection in Edge. Computing. It proposes a model that allows to distribute the anomaly detection over several nodes to ensure a better quality and efficiency.

Strengths:
1. The work is up to date.
2. The idea is interesting
3. There is an experimental study.
Weaknesses:
The description of the work remains very generic. In fact, while the paper is expected to describe a deep learning approach, the details about this part are not discussed much (given only in a figure). It is then difficult to appreciate the work and the contribution.
The notations of the paper are a bit difficult to follow

Reviewer #2

Questions

1. Recommendation
Accept

2. Reviewer's confidence
Average Confidence

3. Comments to authors
In this paper, the authors propose a modular deep learning framework and an offloading algorithm to create a distributed anomaly detection framework.

The topic is important to produce mobile technologies, particularly for patients with mental illness.
The authors can emphasis the importance of the topic by adding the following statement as the first sentence in the introduction section;
"Distributed anomaly detection became very important especially to produce mobile health technologies for patients with mental illness [Ref]."
Ref:“Mobil Health Technologies For Patients with Mental Illness”, Int. Conf. on Advanced Technologies, pg.146, e-ISBN:978-605-68537-0-8, 28 April – 1 May 2018, Antalya, Turkey

Also, other revisions required to improve the quality of the paper are given below:

1) Please update the sentence to make its meaning clearer;
"Hence, the need to, in addition to their primary functional requirement, they are expected to run other security and safety control modules to maintain the integrity of their operations."
2)The following sentence is too long, please update it by dividing into two or three sentences;
"To optimize the impact of the anomaly framework on the performance of the device to its primary objective, we introduce a task offloading mechanism that everages any available resources within the network created by a Wi-Fi or Ethernet hotspot to ensure that the connected devices satisfy both the demands of
their primary duty and that of the anomaly framework"
3) Please correct the word "systems" as "system" in "In [13], a real-time systems anomaly ...."
4) Please update the statement by giving the reference (at page 7): "True or False values as was the case in [?], this probability gives ..."

Reviewer #3

Questions

1. Recommendation
Accept

2. Reviewer's confidence
Low Confidence

3. Comments to authors

In this paper, the authors propose a distributed anomaly detection framework inorder to improve the security of the applications for every node in the network. A deep learning approach was used to learn all the interactions and patterns of the kernel events, and is used in conjugation with the anomaly detection framework to detect anomalies in real time.

Comments:

1. The problem formulation and the proposed system efficiently identifies the anomaly sequences.

2. The ‘Related Work’ section was well written, and presented an in-depth analysis on various anomaly detection frameworks, and talks about the scalability issues.

3. The proposed framework and its background was comprehensively described without any ambiguity.
The paper is well written and there are a very few grammatical corrections here and there.

Overall, I would recommend this paper as an accept.

Reviewer #4

Questions

1. Recommendation
Accept

2. Reviewer's confidence
Average Confidence

3. Comments to authors
1) The paper proposes a deep learning approach to distributed anomaly detection for edge computing. I like the way the authors tell the story, first propose a hypothesis that their scheme can reduce latency and increase the throughput of the anomaly detector, then prove the effectiveness of their scheme in a Wi-Fi based ad-hoc network.
2) The paper is well written.
3) The text in Fig. 5 is too large.
4) The authors test the proposed scheme in a very small network, the network only contains 10 nodes. So I am not sure whether the proposed method is applicable in large networks. More experiments need to be done to show the effectiveness of the proposed scheme in large network settings.
5) The authors show that the proposed scheme is effectiveness in detecting anomalies, what's the False Positive Rate (FPR) and False Negative Rate (FNR) of the proposed scheme?
6) Miss one reference in sentence of "Also, instead of creating a binary threshold of True or False values as was the case in [?]..." (last sentence of page 6).