/

CSE 543: Information Assurance and Security

Using Machine Learning to detect classifying Malware in IoT Systems

Group 14 Weekly Report - 7

Person prepared this report: All the members of the group

Person approved this report: Priyadarshini Venkatesan

Person submitted this report: Priyadarshini Venkatesan

List of members

1. Amogh Manoj Joshi (Group Leader)
2. Priyadarshini Venkatesan (Deputy Leader)
3. Vignan Varma Chekuri
4. Venkata Karthik Reddy Peddireddy
5. Siva Priya Bollineni
6. Anusha Akuthota
7. Sarika Naidu Chirki
8. Ramya Thota

Meeting Notes

03/03/2023: [7:30 pm - 8:00 pm] [Mode: Virtual]

- The week before midterm, Vignan had a meeting with ASU Writing Center where he received some tips to improve the writing format of the weekly reports
- After the midterm exam, the team held a meeting to discuss the tips and feedback which Vignan received. Some of the key point which Vignan presented during the meeting are:
    - **Academic Writing Format:** The writing should be in APA 7 formatting, which includes Times New Roman font size 12 and double spacing in paragraphs.
    - **Usage of Complete Sentences:** The author's should try to use complete sentences instead of incomplete ones. For instance, they can rephrase sentences to improve the flow and coherence of text, such as using transitional words and phrases like 'However, Furthermore, Moreover' to link ideas.
    - **Referencing:** According to the APA 7 format, the author should include the author(s) of the work, year of publication, title of the work, information about the source, DOI or URL (if available). The references should be written in a hanging indent format, where the first line of each reference starts at the left margin, and subsequent lines are indented.
    - **Consistency:** By following these guidelines, authors can ensure that their references are consistent, clear, and easy to read. APA 7 format is commonly used in social sciences, such as psychology, sociology, and education.
- The team members discussed these points one-by-one and made sure to implement them in the upcoming weekly reports
- **Attendance:** All the members were present

03/05/2023: [7:30 pm - 8:00 pm] [Mode: Virtual]

- The group finished their paper set 2 i.e 14 papers
- A meeting was held to discuss the next plan: To focus on casual papers and take a wider grasp of the topic (since the group had majorly focused on in-depth papers only)
- The group leader told the members to put in more efforts and take advantage of the spring break by reading 2 casual papers per member in the week: March 6 - 12
- Thus, by the end of spring break, each member of the group would have read 2 in-depth and 2 casual papers in the domain of the project
- **Attendance:** All the members were present

Tasks Summary

Task Number	Task Name	Description of Task	Member	Task Status
1	Tips and Feedback for report writing were discussed.	Discussed points on how to effectively write a report and plan to implement them in the next weekly reports.	All Members	On-going
2	Reading of casual papers	All the members of the team will be working on reading the remaining two casual papers within this week.	All Members	On-going

Task Progress

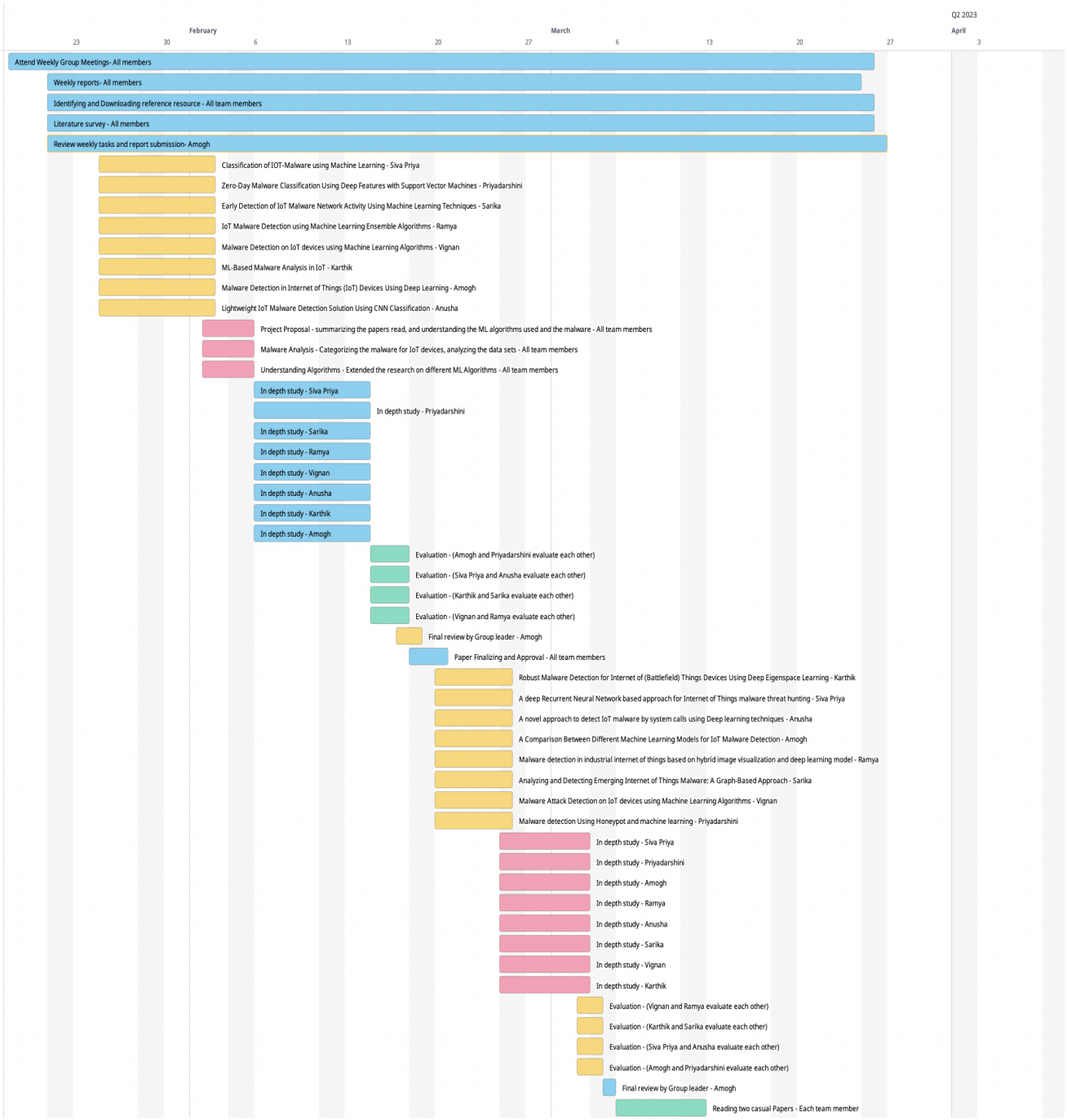
Task Name	Member	Date and time of Review	Reviewer(s)	Mode of Review	Review Conclusion	Recommended Action
1)Tips and Feedback for report writing were discussed.	All the members of the group	03/03/2023	All the members of the group	Group meeting	Needs work	Ongoing
2)Reading of Casual papers	All the members of the group	03/05/2023	All the members of the group	Group meeting	Needs work	Ongoing

Problems:

Faced by: All Team Members
Status: In Progress
Problem: One of our team members attended the ASU Writing Center after which we are trying to implement all the suggested changes within the report.

Gantt Chart:

[Link to Gantt Chart]



References:

In Depth

1.F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020, doi: 10.1109/COMST.2020.2986444.

2.S. Madan and M. Singh, "Classification of IOT-Malware using Machine Learning," 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 2021, pp. 599-605, doi: 10.1109/ICTAI53825.2021.9673185.

3.R. El-Sayed, A. El-Ghamry, T. Gaber and A. E. Hassanien, "Zero-Day Malware Classification Using Deep Features with Support Vector Machines," 2021 Tenth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, 2021, pp. 311-317, doi: 10.1109/ICICIS52592.2021.9694256.

4.A. Kumar and T. J. Lim, "EDIMA: Early Detection of IoT Malware Network Activity Using Machine Learning Techniques," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 289-294, doi: 10.1109/WF-IoT.2019.8767194.

5. Santhadevi D, Janet B, “IoT Malware Detection using Machine Learning Ensemble Algorithms”, International Journal of Advanced Science and Technology (IJAST), vol. 29, no. 10s, pp. 8006-8016, Jun. 2020.

6.Achary, Rathnakar, and Chetan J. Shelke. "Malware Attack Detection on IoT Devices Using Machine Learning." In Smart Data Intelligence: Proceedings of ICSMDI 2022, pp. 11-22. Singapore: Springer Nature Singapore, 2022.

7.S. Riaz et al., “Malware Detection in Internet of Things (IoT) Devices Using Deep Learning,” Sensors, vol. 22, no. 23, p. 9305, Nov. 2022, doi: 10.3390/s22239305.

8.A. M. N. Zaza, S. K. Kharroub and K. Abualsaud, "Lightweight IoT Malware Detection Solution Using CNN Classification," 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 212-217, doi: 10.1109/5GWF49715.2020.9221100.

9.A. Azmoodeh, A. Dehghantanha and K. -K. R. Choo, "Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning," in IEEE Transactions on Sustainable Computing, vol. 4, no. 1, pp. 88-95, 1 Jan.-March 2019, doi: 10.1109/TSUSC.2018.2809665.

10.Hamed HaddadPajouh, Ali Dehghantanha, Raouf Khayami, Kim-Kwang Raymond Choo,A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting,Future Generation Computer Systems,Volume 85,2018,Pages 88-96,ISSN 0167-739X,https://doi.org/10.1016/j.future.2018.03.007.

11.M. Shobana and S. Poonkuzhali, "A novel approach to detect IoT malware by system calls using Deep learning techniques," 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2020, pp. 1-5, doi: 10.1109/ICITIIT49094.2020.9071531.

12.Nakhodchi, S., Upadhyay, A., Dehghantanha, A. (2020). A Comparison Between Different Machine Learning Models for IoT Malware Detection. In: Karimipour, H., Srikantha, P., Farag, H., Wei-Kocsis, J. (eds) Security of Cyber-Physical Systems. Springer, Cham. https://doi.org/10.1007/978-3-030-45541-5_10

13.Hamad Naeem, Farhan Ullah, Muhammad Rashid Naeem, Shehzad Khalid, Danish Vasan, Sohail Jabbar, Saqib Saeed,Malware detection in industrial internet of things based on hybrid image visualization and deep learning model,Ad Hoc Networks,Volume 105,2020,102154,ISSN 1570-8705,https://doi.org/10.1016/j.adhoc.2020.102154.

14..H. Alasmary et al., "Analyzing and Detecting Emerging Internet of Things Malware: A Graph-Based Approach," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8977-8988, Oct. 2019, doi: 10.1109/JIOT.2019.2925929.

15..I. M. M. Matin and B. Rahardjo, "Malware Detection Using Honeypot and Machine Learning," 2019 7th International Conference on Cyber and IT Service Management (CITSM), Jakarta, Indonesia, 2019, pp. 1-4, doi: 10.1109/CITSM47753.2019.8965419.

16.Achary, R., Shelke, C.J. (2022). Malware Attack Detection on IoT Devices Using Machine Learning. In: Asokan, R., Ruiz, D.P., Baig, Z.A., Piramuthu, S. (eds) Smart Data Intelligence. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-19-3311-0_2

Casual

1. ElMouatez Billah Karbab, Mourad Debbabi, Abdelouahid Derhab, Djedjiga Mouheb, MalDozer: Automatic framework for android malware detection using deep learning,Digital Investigation,Volume 24, Supplement,2018,Pages S48-S59, ISSN 1742-2876, https://doi.org/10.1016/j.diin.2018.01.007.

2.J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng and K. Sakurai, "Lightweight Classification of IoT Malware Based on Image Recognition," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 2018, pp. 664-669, doi: 10.1109/COMPSAC.2018.10315.

3.S. Ali, O. Abusabha, F. Ali, M. Imran and T. ABUHMED, "Effective Multitask Deep Learning for IoT Malware Detection and Identification Using Behavioral Traffic Analysis," in IEEE Transactions on Network and Service Management, 2022, doi: 10.1109/TNSM.2022.3200741.

4.Riaz S, Latif S, Usman SM, Ullah SS, Algarni AD, Yasin A, Anwar A, Elmannai H, Hussain S. Malware Detection in Internet of Things (IoT) Devices Using Deep Learning. *Sensors*. 2022; 22(23):9305. https://doi.org/10.3390/s22239305.

5.Kumar, Rajesh & Zhang, Xiaosong & Wang, Wen & Khan, Riaz & Kumar, Jay & Sharif, Abubakar. (2019). A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2916886.

6.Al-Sarem M, Saeed F, Alkhammash EH, Alghamdi NS. An Aggregated Mutual Information Based Feature Selection with Machine Learning Methods for Enhancing IoT Botnet Attack Detection. Sensors (Basel). 2021 Dec 28;22(1):185. doi: 10.3390/s22010185. PMID: 35009725; PMCID: PMC8749651.

7.S. Sharma and S. Bharti, "Malware Analysis using Ensemble Techniques: A Machine Learning Approach," 2021 International Conference on Artificial Intelligence and Machine Vision (AIMV), Gandhinagar, India, 2021, pp. 1-5, doi: 10.1109/AIMV53313.2021.9670949.

8./Zhongru Ren, Haomin Wu, Qian Ning, Iftikhar Hussain, Bingcai Chen,End-to-end malware detection for android IoT devices using deep learning,Ad Hoc Networks,Volume 101,2020, 102098,ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2020.102098.

9.M. Dib, S. Torabi, E. Bou-Harb and C. Assi, "A Multi-Dimensional Deep Learning Framework for IoT Malware Classification and Family Attribution," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1165-1177, June 2021, doi: 10.1109/TNSM.2021.3075315.

10.K. D. T. Nguyen, T. M. Tuan, S. H. Le, A. P. Viet, M. Ogawa and N. L. Minh, "Comparison of Three Deep Learning-based Approaches for IoT Malware Detection," 2018 10th International Conference on Knowledge and Systems Engineering (KSE), Ho Chi Minh City, Vietnam, 2018, pp. 382-388, doi: 10.1109/KSE.2018.8573374.

11.Riaz S, Latif S, Usman SM, Ullah SS, Algarni AD, Yasin A, Anwar A, Elmannai H, Hussain S. Malware Detection in Internet of Things (IoT) Devices Using Deep Learning. Sensors (Basel). 2022 Nov 29;22(23):9305. doi: 10.3390/s22239305. PMID: 36502007; PMCID: PMC9735444.

12.Peters, W., Dehghantanha, A., Parizi, R.M., Srivastava, G. (2020). A Comparison of State-of-the-Art Machine Learning Models for OpCode-Based IoT Malware Detection. In: Choo, KK., Dehghantanha, A. (eds) Handbook of Big Data Privacy. Springer, Cham. https://doi.org/10.1007/978-3-030-38557-6_6

13.M. Fahim and A. Sillitti, "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review," in IEEE Access, vol. 7, pp. 81664-81681, 2019, doi: 10.1109/ACCESS.2019.2921912.

14.R. Vishwakarma and A. K. Jain, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1019-1024, doi: 10.1109/ICOEI.2019.8862720.

15.Asam, M., Khan, S.H., Akbar, A. *et al.* IoT malware detection architecture using a novel channel boosted and squeezed CNN. *Sci Rep* 12, 15498 (2022). https://doi.org/10.1038/s41598-022-18936-9.