CSE 543: Information Assurance and Security

Using Machine Learning to detect classifying Malware in IoT Systems

Group 14 Weekly Report - 6

Person prepared this report: All the members of the group

Person approved this report: Amogh Manoj Joshi

Person submitted this report: Amogh Manoj Joshi

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

02/23/2023: [7:30 pm - 8:00 pm] [Mode: Virtual]

- A team meeting was held to discuss on the feedback received from the TA and the professor during Wednesday's review session
- As suggested by the TA, the group was organized into 2 teams: 4 members focusing on Machine Learning based approaches and the other 4 members focusing on Deep Learning based approaches. This would organize the reading efforts of the group and eventually help form the final report in a structured manner
- Also, the group was focusing on finding and reading the best and highly cited papers in the domain till now, as instructed by the professor, the group members decided to also include casual papers in the next week, which will broaden their knowledge in the domain
- **Attendance:** All the members were present

02/25/2023: [7:30 pm - 8:00 pm] [Mode: Virtual]

- The group members had some common concerns and hence a meeting was scheduled
- Most of the members had a major assignment's submission on Sunday and were caught up in that and hence were finding it difficult to complete their study report before the deadline. Also, with the midterms coming in a few days, everyone was prioritizing studying for their exams.
- A collective decision was made to shift the study report deadline from 25th Feb to 3rd March. The week following that is spring break and hence the group decided to put in more hours during that break to cover up the lag.
- **Attendance:** All the members were present

Tasks Summary

Task Number	Task Name	Description of Task	Member	Task Status
1	Splitting of the group into 2 teams	Members were divided into 2 group, one group for focusing on papers related to Deep learning techniques and the other group on machine learning techniques	All members	Completed
2	Adding more casual papers for the next week	The team will be working on casual paper reading next week.	All members	On-going
3	Reading of paper set 2	The members of the team are working on analyzing the paper 2.	All members	On-going

Task Progress

Task Name	Member	Date and time of Review	Reviewer(s)	Mode of Review	Review Conclusion	Recommended Action
1)Splitting of the group into 2 teams	All the members of the group	02/25/2023	Amogh Joshi	Individual	Satisfactory	Completed
2)Adding more casual papers for the next week	All the members of the group	02/26/2023	All the members of the group		Needs work	Ongoing
3)Reading of paper set 2	All the members of the group	02/27/2023	All the members of the group	-	Needs work	Ongoing

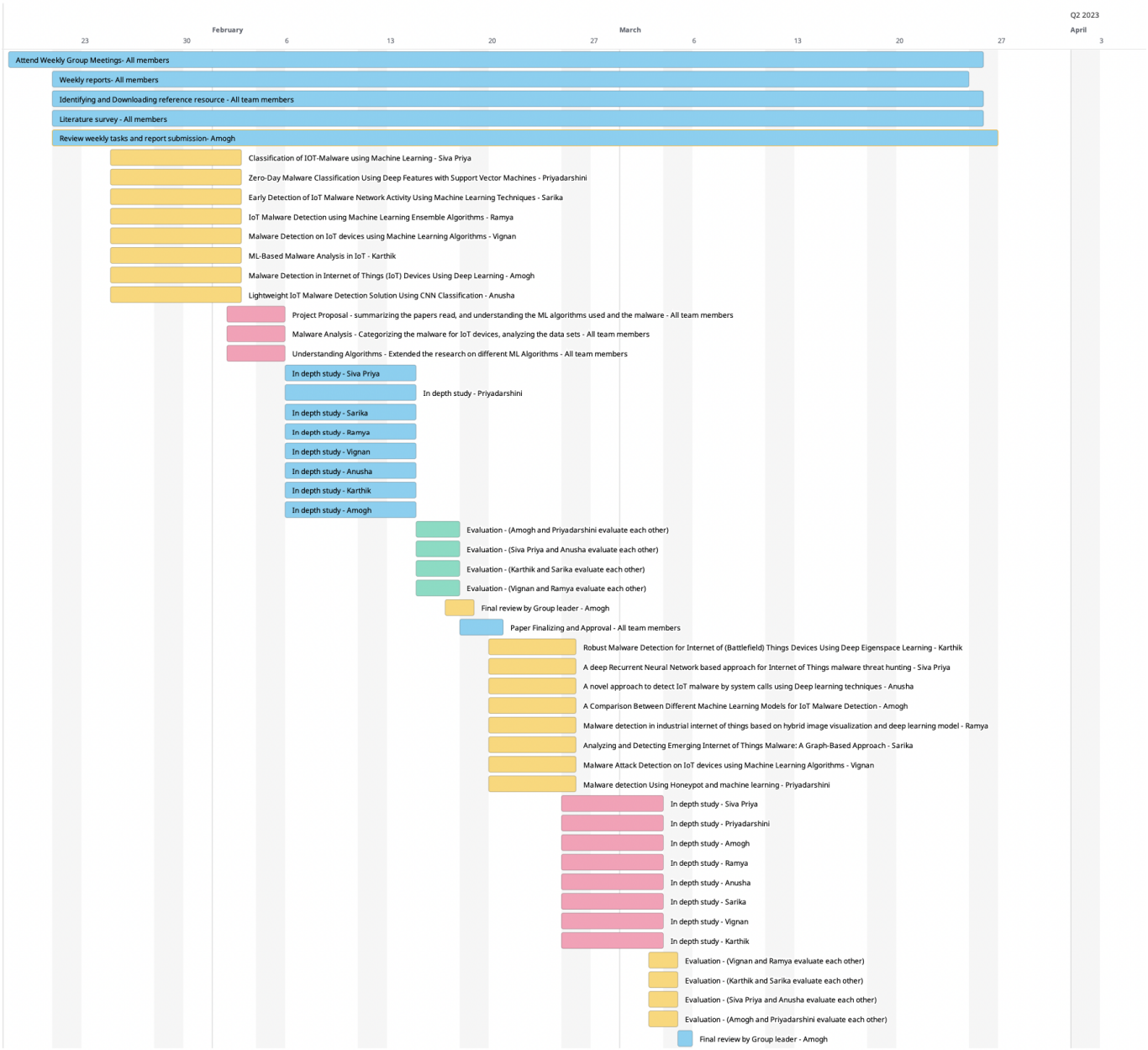
Problems:

Faced by: All Team Members
Status: Solved
Problem:

- We split the group into two half, with each group focusing on a different research area to enable broader comprehension of topics such Machine learning and Deep learning approaches.
- According to the other submissions and midterm preparation which were encountered by the team, due to these reasons, postponed the assignment of analyzing individual team members in-depth paper reports to the following week.

Gantt Chart:

[Link to Gantt Chart]



References:

In Depth

1.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.

2.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.

3.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.

4.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

5.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.

6.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.

7.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.

8.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

9.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.

10.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.

11.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.

12.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.

13.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.

14.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.

15.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.

16.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.