ARIZONA STATE
UNIVERSITY

CSE 543: Information Assurance and Security

Using Machine Learning to detect classifying Malware in IoT Systems

Group 14 Weekly Report - 5

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

02/18/2023: [7:30 pm - 8:00 pm] [Mode: Virtual]

- The reading, evaluation and final evaluation for the first set of papers was completed. So all the members were asked to search and decide their next paper for reading i.e paper set 2
- The paper deciding and approval by the group leader was done by 20 Feb.
- The members are supposed to read and generate the study report by 25 Feb, the evaluation by 27 Feb and the final evaluation by 28 Feb
- **Attendance:** All the members were present

Tasks Summary

Task Number	Task Name	Description of Task	Member	Task Status
1	Study report for paper set 1	Each team member studied a paper and submitted the study report.	All the members of the group	Completed
2	Study report evaluation for paper set 1	Each study report was evaluated by one of the team members and final evaluation was done by the team lead.	All the members of the group & Group Leader (Final Evaluation)	Completed
3	Deciding and approving paper set 2	Read some journals and decided on the paper set 2 on IOT malware detection using ML/ DL.	All the members of the group	Completed

4	Reading paper set 2	Understanding and summarizing the chosen paper set 2	All the members of the group	Ongoing

Task Progress

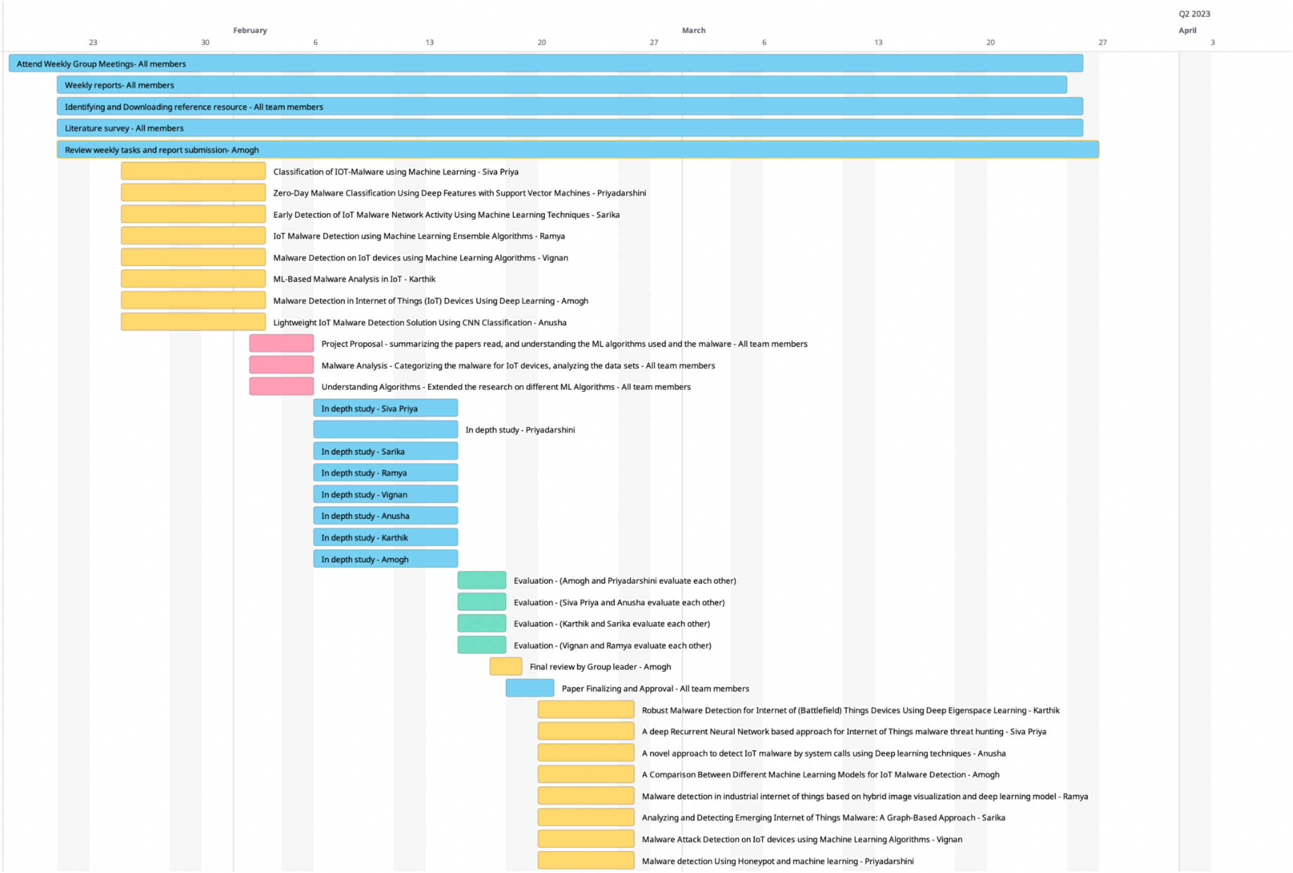
Task Name	Member	Date and time of Review	Reviewer(s)	Mode of Review	Review Conclusion	Recommended Action
Study report for paper set 1	All the members of the group	02/17/2023	All the members of the group	Individual	Satisfactory	Accepted
Study report evaluation for paper set 1	All the members of the group	02/18/2023	All the members of the group	Individual	Satisfactory	Accepted
Deciding and approving paper set 2	All the members of the group	02/20/2023	All the members of the group	Individual	Satisfactory	Accepted
Reading paper set 2	All the members of the group	02/21/2023	All the members of the group	Individual	—	—

Problems:

Faced by: All Team Members
Status: Solved
Problem: Selecting and analyzing a second journal on malware detection in IoT.

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