



CSE 543: Information Assurance and Security

---

## **Using Machine Learning to detect classifying Malware in IoT Systems**

### **Group 14 Weekly Report - 9**

**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

03/18/2023: [ 7:30 pm - 9:00 pm ] [ Mode: Virtual ]

- A group meeting was held to discuss what each member had learnt after reading 3 in-depth papers and 2 casual papers
- Each member was asked to curate a list of 2-3 topics which he/she had covered through the 5 papers so far
- The topics covered by all the members were together concatenated which formed the layout of the final report meeting that the final report would cover all these topics
- The plan of action for the final week before report submission was decided
- **Attendance:** All the members were present

## Tasks Summary

Task Number	Task Name	Description of Task	Member	Task Status
1	Reading of 3rd set of in-depth papers	All the members successfully finished their respective 3rd in-depth paper.	All members	Done
2	Group Discussion (for finalizing list of topics)	Group discussed the topics that read and curated 2-3 topics from them.	All members	Done
3	Plan of Action for final week	The team finalized on what and how to proceed for the final report.	All members	Done
4	Final report making	The team is working on the final report.	All members	On-going

### **Task Progress**

Task Name	Member	Date and time of Review	Reviewer(s)	Mode of Review	Review Conclusion	Recommended Action
Reading of 3rd set of in-depth papers	All members	03/14/2023	All the members of the group	Group meeting	Satisfactory	Completed
Group Discussion (for finalizing list of topics)	All members	03/16/2023	All the members of the group	Group meeting	Satisfactory	Completed
Plan of Action for final week	All members	03/18/2023	Amogh Joshi	Group meeting	Satisfactory	Completed
Final report making	All members	03/25/2023	Amogh Joshi	Group meeting	Needs work	Ongoing

### **Problems:**

**Faced by:** All Team Members

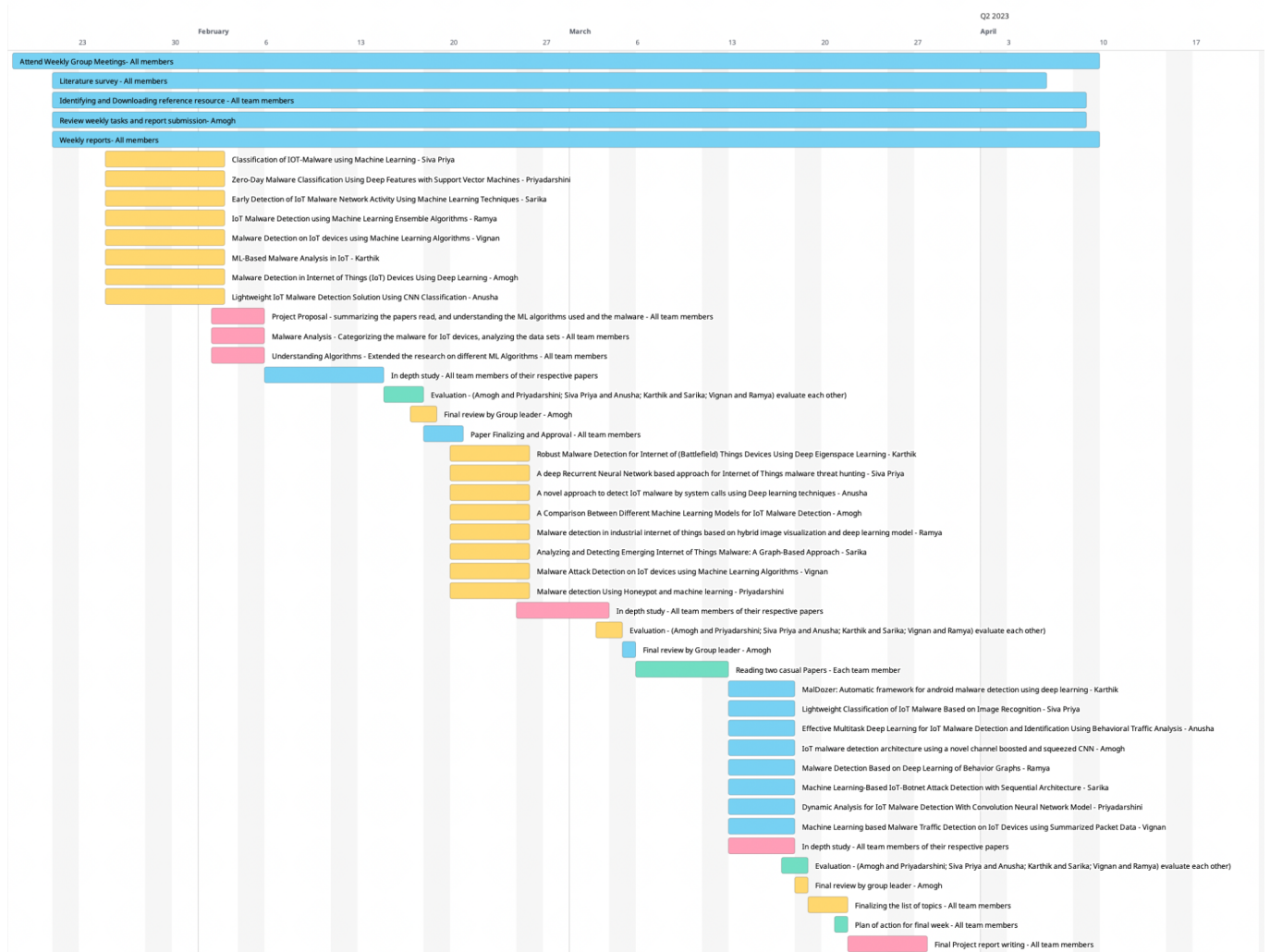
**Status:** Solved

### **Problem:**

- On summarizing and analyzing all of the 5 papers by each individual, organizing and summarizing into 2-3 major topics by each individual in the team was challenging.

## Gantt Chart:

### [Link to Gantt Chart](#)



## **References:**

For complete list of all the in depth references and causal references please check the following link: ([https://docs.google.com/spreadsheets/d/1hab4PAWxRHrmEo-6p4pZzyuUIFz8\\_H-qxlXJsQ3uvbU/edit#gid=0](https://docs.google.com/spreadsheets/d/1hab4PAWxRHrmEo-6p4pZzyuUIFz8_H-qxlXJsQ3uvbU/edit#gid=0))

## **In Depth**

- 1.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.
- 2.ElMoataz 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, doi: <https://doi.org/10.1016/j.diin.2018.01.007>.
- 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.J. Jeon, J. H. Park and Y. -S. Jeong, "Dynamic Analysis for IoT Malware Detection With Convolution Neural Network Model," in IEEE Access, vol. 8, pp. 96899-96911, 2020, doi: 10.1109/ACCESS.2020.2995887.
- 5.Nakahara, Masataka & Okui, Norihiro & Kobayashi, Yasuaki & Miyake, Yutaka. (2020). Machine Learning based Malware Traffic Detection on IoT Devices using Summarized Packet Data. 78-87. 10.5220/0009345300780087.
- 6.Asam M, Khan SH, Akbar A, Bibi S, Jamal T, Khan A, Ghafoor U, Bhutta MR. IoT malware detection architecture using a novel channel boosted and squeezed CNN. Sci Rep. 2022 Sep 15;12(1):15498. doi: 10.1038/s41598-022-18936-9. PMID: 36109570; PMCID: PMC9477830.
7. Fei Xiao, Zhaowen Lin, Yi Sun, Yan Ma, "Malware Detection Based on Deep Learning of Behavior Graphs", *Mathematical Problems in Engineering*, vol. 2019, Article ID 8195395, 10 pages, 2019. <https://doi.org/10.1155/2019/8195395>
- 7.SOE, Yan Naung, FENG, Yaokai, SANTOSA, Paulus Insap, HARTANTO, Rudy, SAKURAI, Kouichi (2020): Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture. *Sensors*, 20 (16), S. 4372 Online verfügbar unter: URL: <http://dx.doi.org/10.3390/s20164372>.

## **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, Alkhamash 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](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>.