Intrusion Detection in IIOT Network

Figure 1: Illustration [14]

Supervisor : **Prof. Dr.-Ing. Axel Sikora**

Students : **Sakshi Kulkarni**
Vishal Sivakumar

Introduction to IoT Networks

A network of physical devices, vehicles, home appliances, and other objects that are embedded with sensors, software, and connectivity, enabling them to collect and exchange data over the internet.

IOT ?

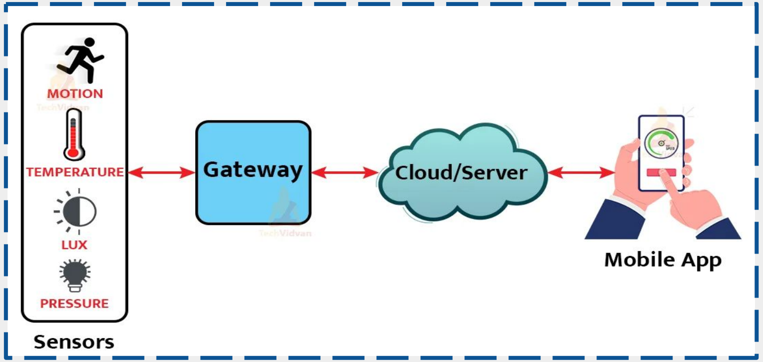


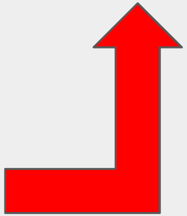
Figure 2: **IoT Network** [10]

The application of these networks ranges from Automotives, Consumer electronics, Industries, and many other Automation oriented products.

Figure 3: Illustration [11]

Figure 4: Illustration [12]

Figure 5: Illustration [13]



GROWING

Security Challenges in IoT Networks

With the scaling-up in number of devices and networks, the vulnerability towards information breach and intrusion scales-up.[8]

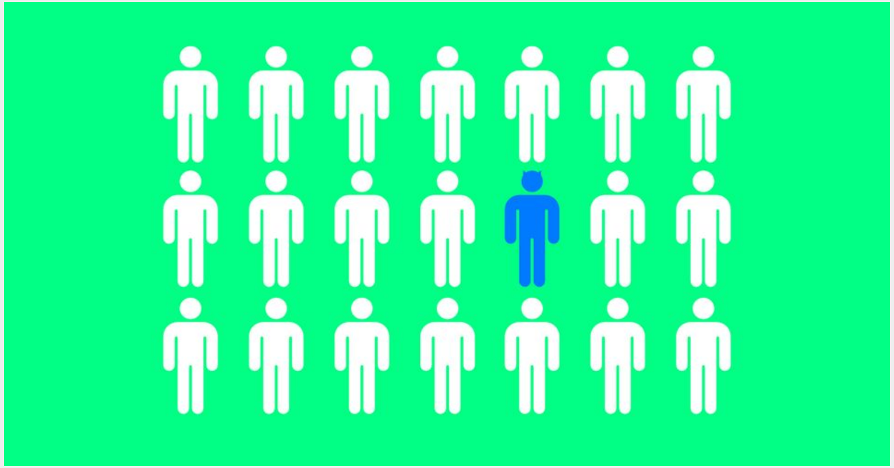


Figure 7: Illustration [17]

We'll see some of the major impacts of these security threats in the upcoming slides.

IOT Botnets

- A network of hijacked internet-connected devices that are installed with malicious codes known as malware. [1]
- Botnet consists of :
  1. Bots
  2. Botmaster

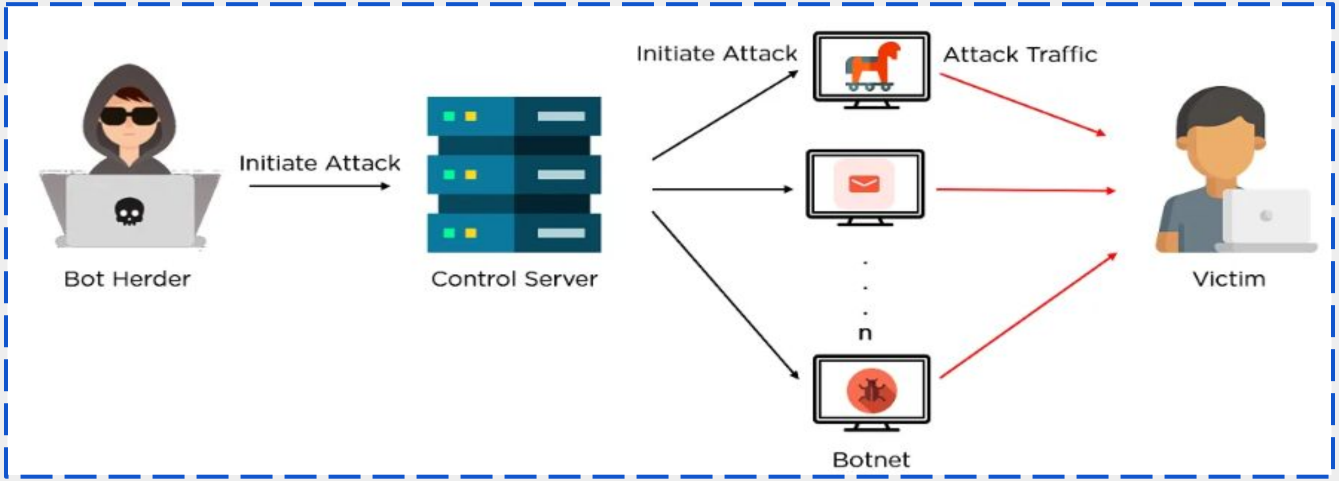


Figure 8: Working of a Botnet [1]

Examples of Impact on Businesses

The world has already experienced notable IoT botnet attacks.

Mirai botnet- CNN, Netflix, Paypal, Visa or Amazon under Dyn were attacked in 2016

- 100,000 IoT devices and reaching up to 1.2 Tbps
- websites unreachable by the legitimate users for several hours
- lost around 8% of its customers (i.e., 14000 domains)

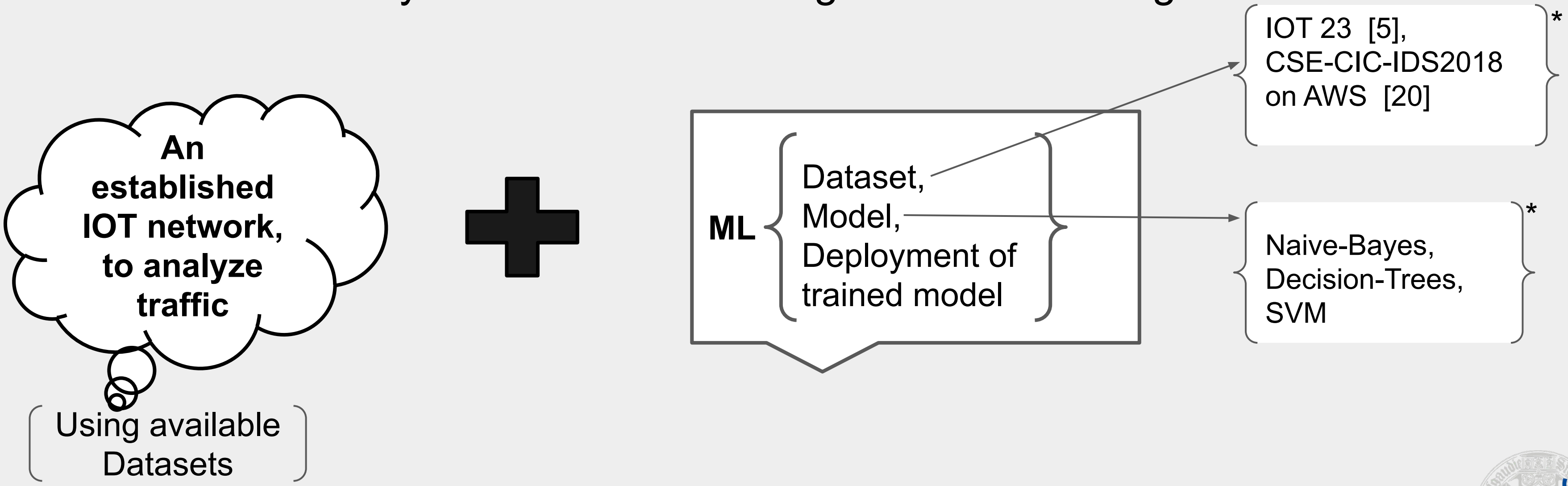
Fig. 9: Illustration [18]

Figure 10: Illustration [18]

Figure 11: Illustration [19]

Project Goals and Methods

- Detect intrusions and malicious activities in IoT networks.
- Identify botnet-generated traffic patterns.
- Enhance the security of IoT networks using machine learning models.



An established IOT network, to analyze traffic

Using available Datasets

ML Dataset, Model, Deployment of trained model

IOT 23 [5], CSE-CIC-IDS2018 on AWS [20] *

Naive-Bayes, Decision-Trees, SVM *

* probable datasets and models, which are subject to change based on evaluation-metrics.

Machine Learning for IoT Security

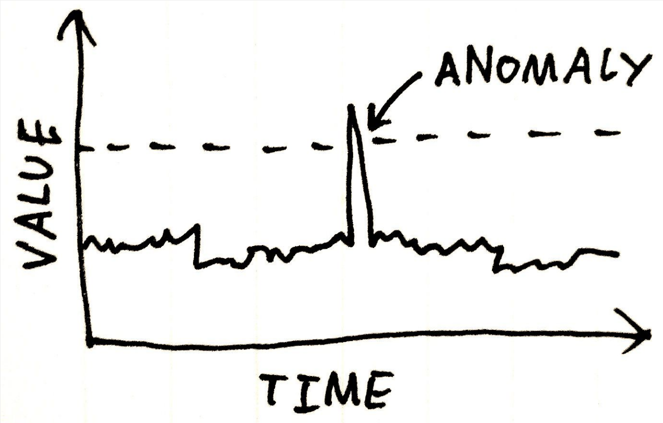


Figure 12: **Visualization of Anomaly** [16]

Anomaly Detection - Identifying unusual patterns or behavior in device data that may indicate a security breach or other problem.[16]

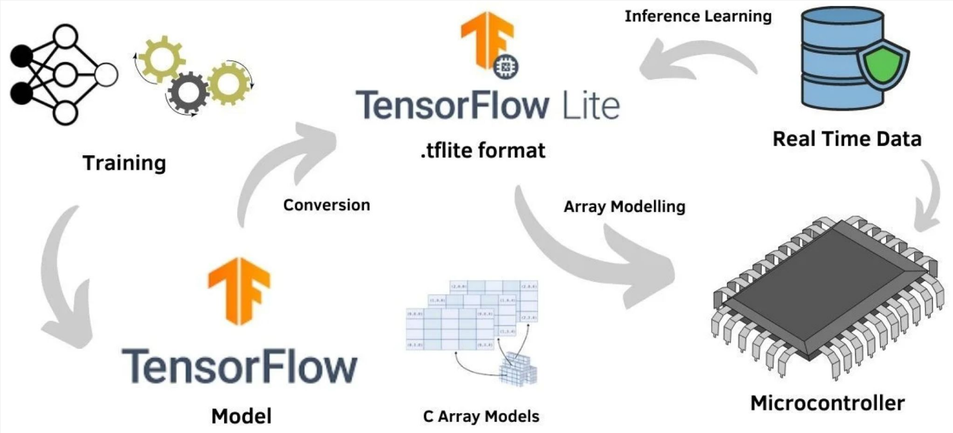
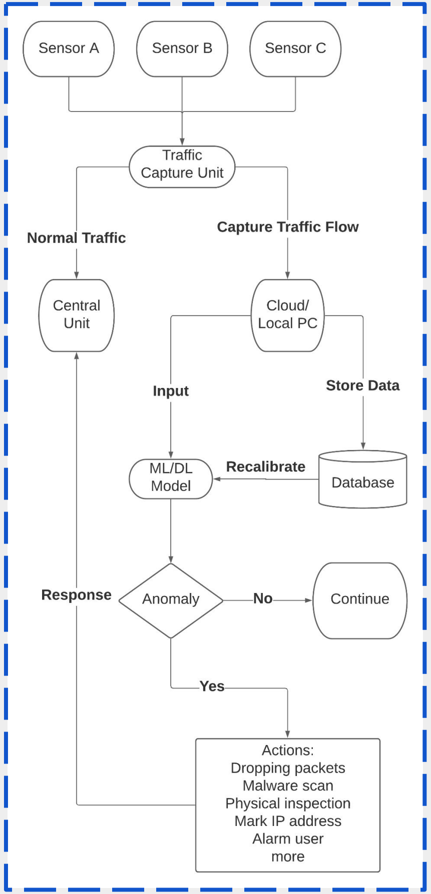


Figure 13: Illustration [18]

Flow of Network Traffic and Anomaly Detection



Flow Chart 1: **Flow of Traffic** [4]

Data-sets for IoT Anomaly based IDS

Sr. no.	Dataset	Botnets	ML techniques
1.	N-Baiot	Mirai, BashLite	Deep Autoencoders, Local Outlier Factor, One-Class Support Vector Machines and Isolation Forest algorithms
2.	Doshi et al. (2018)	DDoS attacks using Mirai-derived IoT botnets	k-Nearest Neighbors, Support Vector Machines, Decision Tree, Random Forest and Artificial Neural Networks algorithms
3	McDermott et al. (2018)	Mirai	text recognition deep learning algorithm
4	Shire et al. (2019)	IoT Malware Traffic	Convolutional Neural Networks

Business Prospects of IOT Security

Analyzed the target market to be:

- Health-Care facilities
- Smart cities
- Finance
- Manufacturing\Production facilities

Global Market Survey

According to a report by **MarketsandMarkets**, the global IoT security market size is expected to grow from **USD 12.5 billion in 2020 to USD 36.6 billion by 2025**, at a compound annual growth rate (CAGR) of 23.9% during the forecast period.

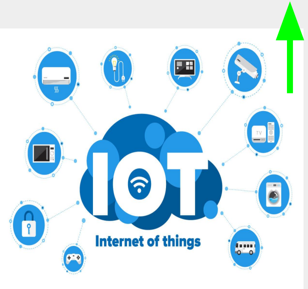
Product Definition: ML for “IDS in IIOT Nets”, using Stable - Classifiers such as Naive-Bayes / Decision-Trees and a dataset (IOT 23) considering multiple cyber attack profiles.

Development: Implementation of Software and validation for detection of Anomalies.

Pricing: Strategy of Pricing will be based on the cost utilized for SW development + Time consumed(days per resource) + considerable profit margin for further development.

Sales: Strategy for sales will be classified regionally considering regulations.

Support: Further customer support



GANTT Chart

NUMBER	TASK TITLE	START DATE	DUE DATE	May				June				July			
				1	2	3	4	1	2	3	4	1	2	3	4
1	Survey of existing dataset	05/01/23	5/16/23	🟩	🟩										
2	Examine existing methologies	05/01/23	5/16/23	🟦	🟦										
3	Approach Selection	5/16/23	5/23/23			🟪									
4	Implementation	5/23/23	6/13/23				🟨	🟨	🟨	🟨					
5	COSIMA submission	5/23/23	5/31/23				🟥								
6	Testing	06/06/23	07/04/23						▨	▨	▨				
7	Documentation	6/13/23	7/12/23							🟦	🟦	🟦			
8	Final Presentation	7/12/23	7/17/23										🟥	🟥	

Workflow

- Survey of existing datasets available for IoT networks
- Examine existing methodologies or concepts for IoT security.
- Approach selection for IoT security
- Implementation
- Testing
- Documentation

References

1. Jena, B. K. (2023b). What Is a Botnet, Its Architecture and How Does It Work? Simplilearn.com. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-a-botnet
2. Meidan, Y. *et al.Baiot: Network-based detection of IOT botnet attacks using deep autoencoders*, *N*. Available at: https://www.arxiv-vanity.com/papers/1805.03409/.
3. *Medbiot: Generation of an IOT botnet dataset in a medium-sized IOT network*. Available at: https://www.researchgate.net/profile/Alejandro-Guerra-Manzanares/publication/338765489_MedBIoT_Generation_of_an_IoT_Botnet_Dataset_in_a_Medium-sized_IoT_Network/links/5e7d058292851caef4a1ec74/MedBIoT-Generation-of-an-IoT-Botnet-Dataset-in-a-Medium-sized-IoT-Network.pdf.
4. Yliang725 *YLIANG725/anomaly-detection-IOT23: A research project of anomaly detection on dataset IOT-23*, *GitHub*. Available at: https://github.com/yliang725/Anomaly-Detection-IoT23.
5. *IOT-23 dataset: A labeled dataset of malware and benign IOT traffic. Stratosphere IPS*. Available at: https://www.stratosphereips.org/datasets-iot23.
6. Chart logo with a arrow Free Vector. (2015, December 10). Freepik. https://www.freepik.com/vectors/increase-logo
7. *Metamorworks. (n.d.). Smart City und Kommunikationsnetzkonzept. 5G. LPWA . Drahtlose Kommunikation. - Stockfoto. https://www.istockphoto.com/de/search/2/image-film?phrase=iot+security*
8. Tsymbal, O. (2023). How to Mitigate IoT Security Threats in 2023. *MobiDev*. https://mobidev.biz/blog/mitigate-internet-of-things-iot-security-threats
9. *Monton, A. L. (2021). What is the Internet of Things and how does it Work? GlobalSign. https://www.globalsign.com/en-sg/blog/what-internet-things-and-how-does-it-work*
10. Taylor, K. (2021). IoT Solutions for the Automotive Industry. *HitechNectar*. https://www.hitechnectar.com/blogs/iot-solutions-for-the-automotive-industry/
11. *Meola, A. (2021, March 2). Smart Farming in 2020: How IoT sensors are creating a more efficient precision agriculture industry. Business Insider. https://www.businessinsider.com/smart-farming-iot-agriculture*
12. *3rd, M. T. (2023, April 26). What is consumer IoT and its applications? | Onomondo. Onomondo. https://onomondo.com/blog/what-is-consumer-iot-and-its-applications/*
13. Cyrus, C. (2022). Public Clouds Join Telcos to Enable 5G at the Edge. *IOT*. https://www.iotworldtoday.com/connectivity/public-clouds-join-telcos-to-enable-5g-at-the-edge
14. *R, S. (2021). Anomaly Detection using AutoEncoders – A Walk-Through in Python. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/05/anomaly-detection-using-autoencoders-a-walk-through-in-python/*
15. *Guida, R. (n.d.). What is a Compromised Account? The Meaning & 5 Tell-Tale Signs. https://www.avanan.com/blog/5-signs-of-a-compromised-account*
16. IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. (n.d.). https://www.unb.ca/cic/datasets/ids-2018.html
17. Shire, R., Shiaeles, S., Bendiab, K., Ghita, B., and Kolokotronis, N. (2019). Malware squid: A novel iot malware traffic analysis framework using convolutional neural network and binary visualisation. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems, pages 65–76. Springer.
18. Doshi, R., Apthorpe, N., and Feamster, N. (2018). Machine learning ddos detection for consumer internet of things devices. In 2018 IEEE Security and Privacy Workshops (SPW), pages 29–35. IEEE.
19. McDermott, C. D., Majdani, F., and Petrovski, A. V. (2018). Botnet detection in the internet of things using deep learning approaches. In 2018 International Joint Conference on Neural Networks (IJCNN), pages 1–8. IEEE.

Questions

?