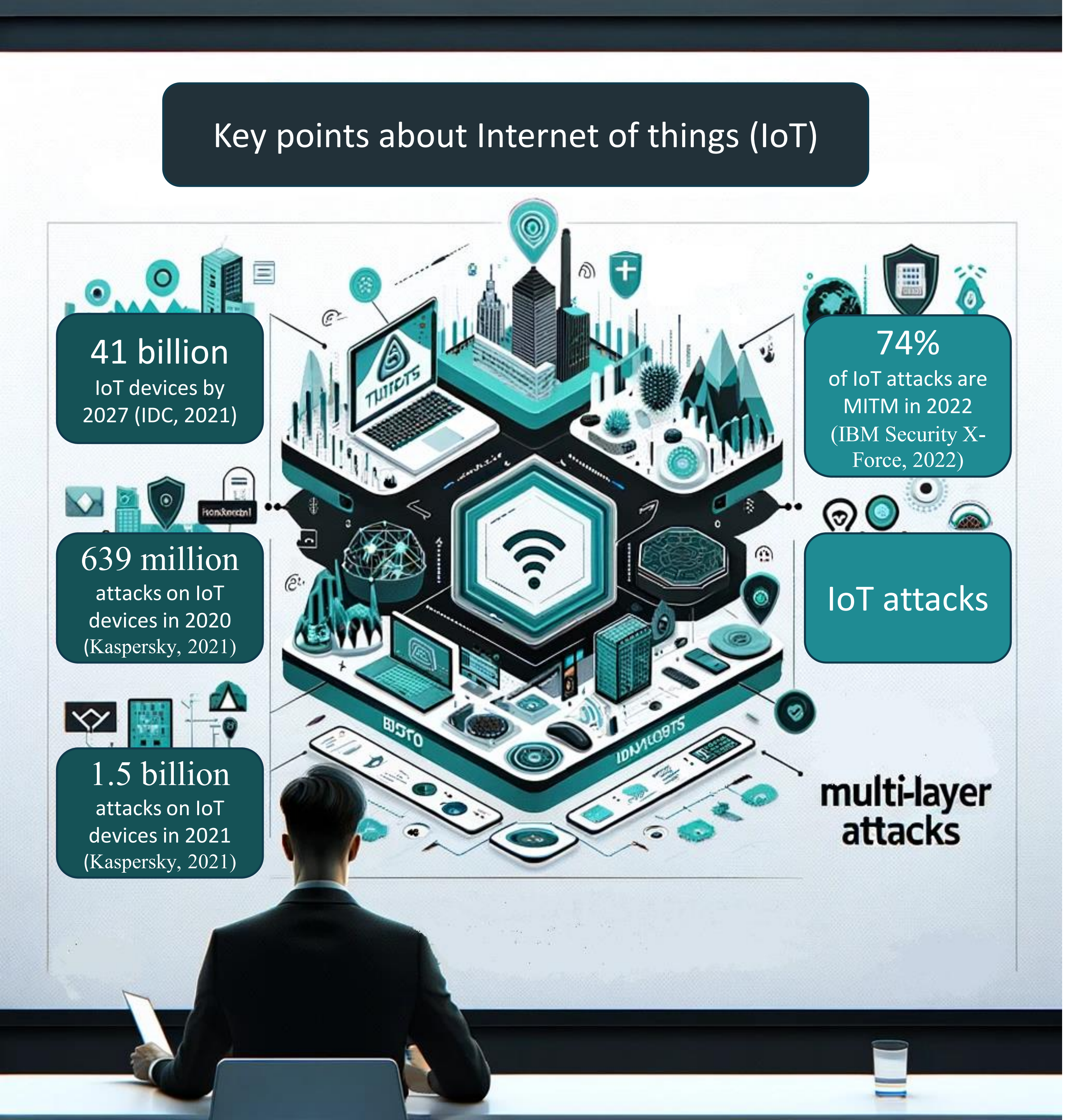
Investigating Security Issues (Multilayer Attacks) on IoT Devices Using Machine Learning

Presented by: Badeea Al Sukhni

Supervisors: Soumya Manna and Leishi Zhang



Canterbury Christ Church University

Background

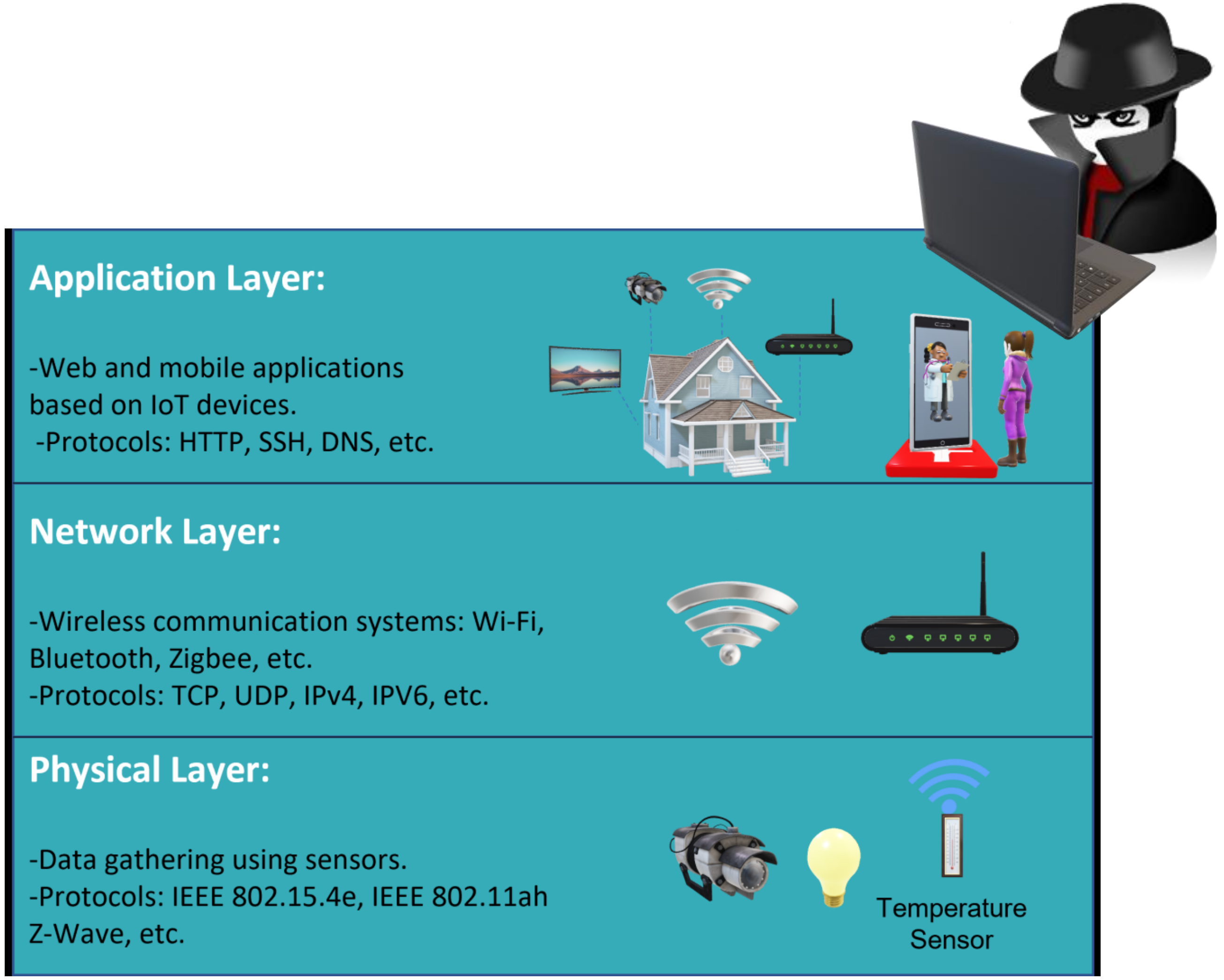
IDC: International Data Corporation

Background

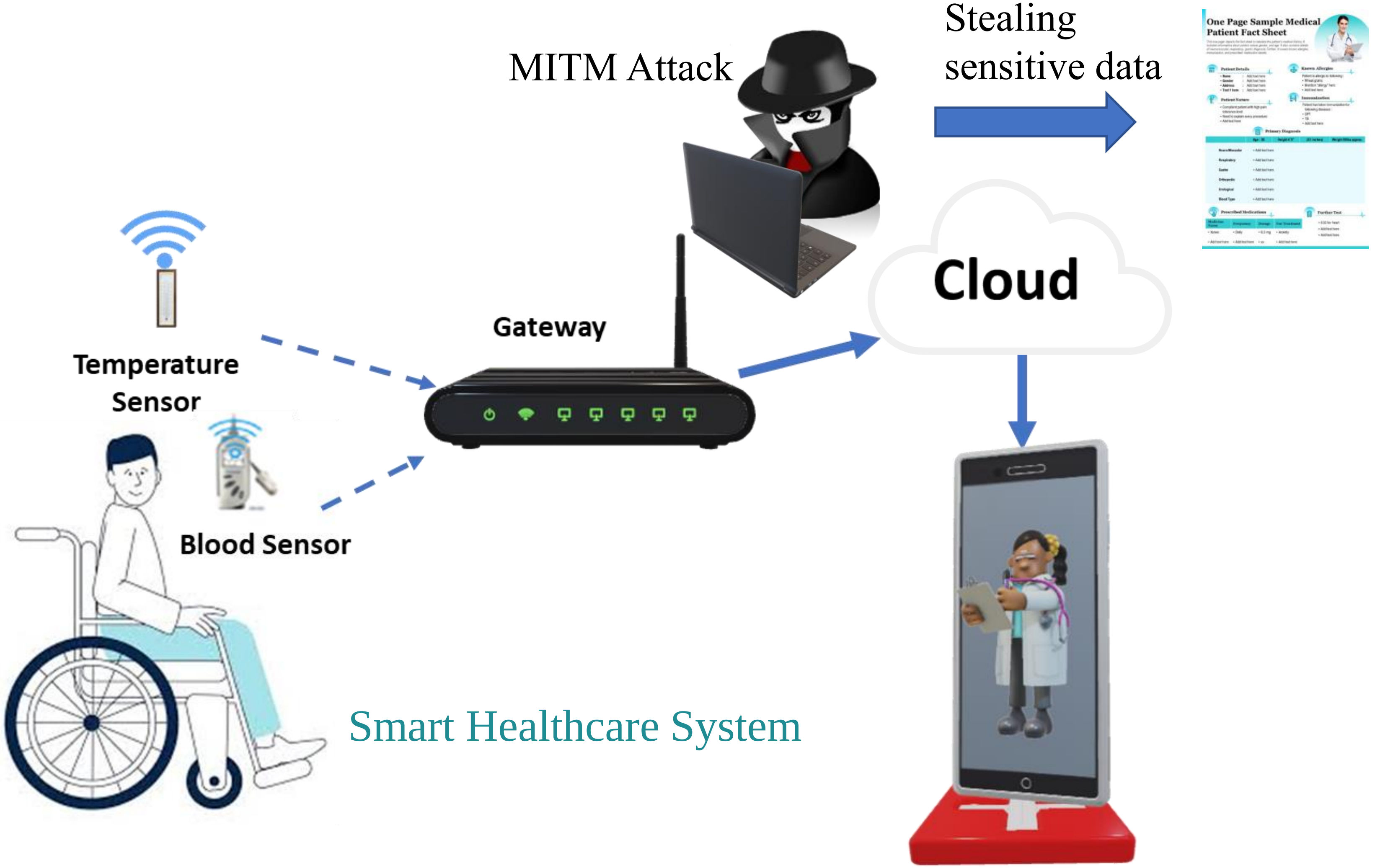
Canterbury Christ Church University

IoT Security Impacts:

- Significant financial losses
- Reputational damage
- Personal information theft



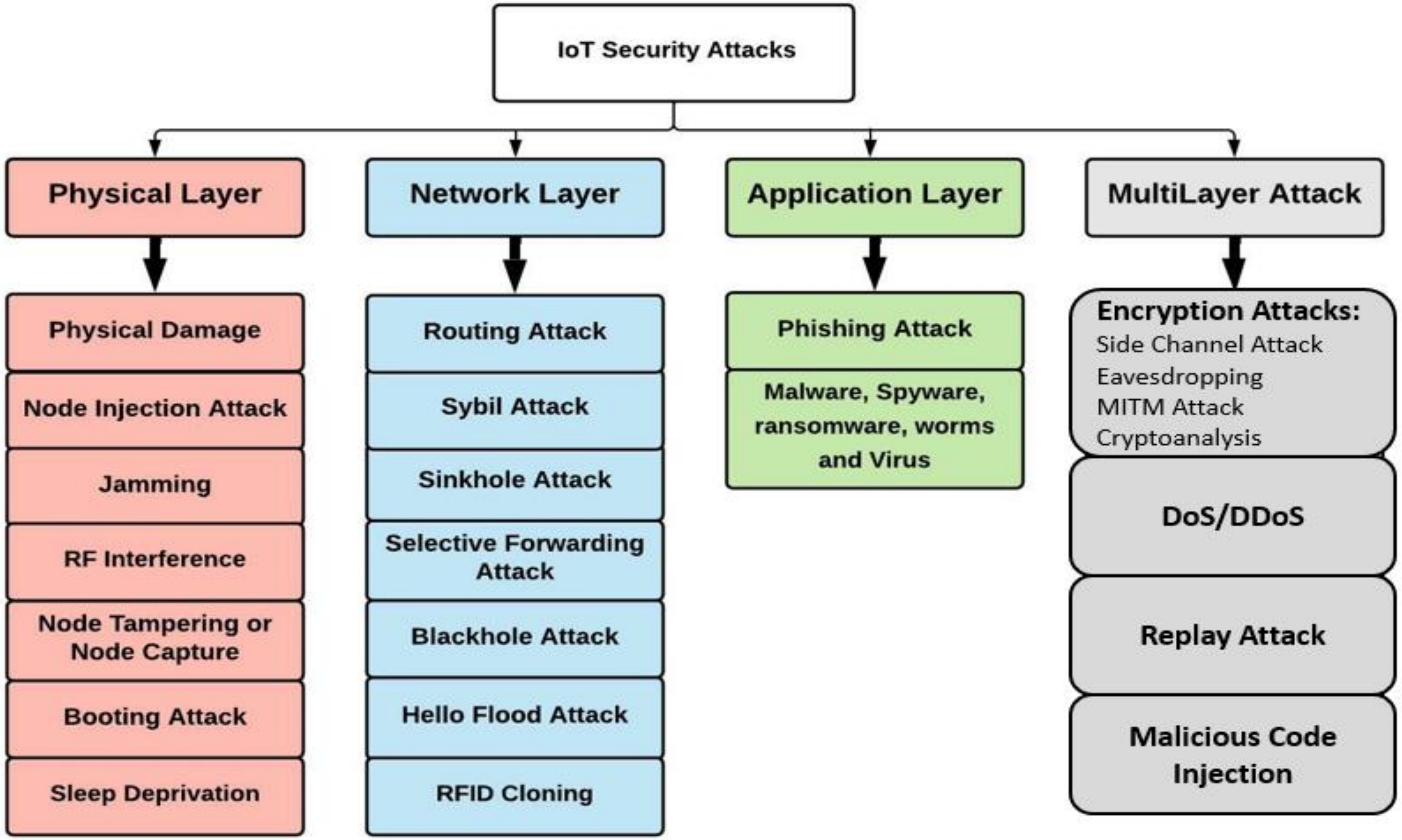
Background



Smart Healthcare System

MITM: Man-in-the-middle attack

The IoT Security Attacks



Al Sukhni, B., Dave, J.M., Manna, S.K. and Zhang, L., 2022, December. Investigating the security issues of multi-layer IoT attacks using machine learning techniques. In 2022 Human-Centered Cognitive Systems (HCCS) (pp. 1-9). IEEE.

Aims and Objectives

Canterbury Christ Church University

Aims

In this research, we aim to create a robust multilayer attack detection through machine learning.

Objectives

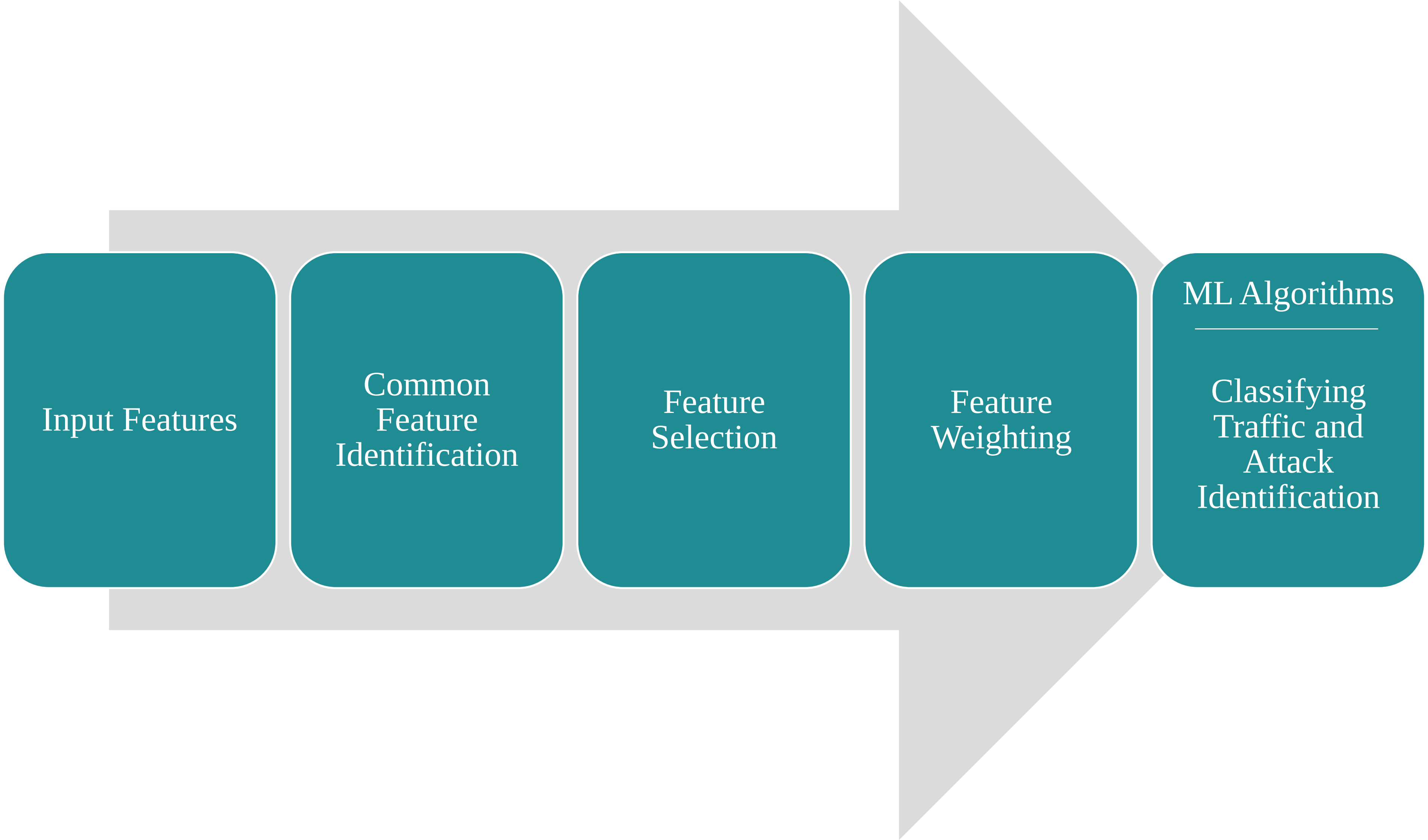
1. Identify MultiLayer security attacks and their behavioral patterns.
2. Investigate ML and datasets that enhance IoT security against multilayer attacks.
3. Explore a variety of feature selection algorithms..
4. Apply feature weighting.
5. Increase detection efficiency by utilizing significant features.
6. Fine-tune hyperparameters for ML classification models.

Datasets Analysis

Dataset	Year	IoT Specific	Total Features	Total Attacks	Multilayer Attacks
KDDCUP 99	1999	No	41	4	DoS
NSL-KDD	2009	No	43	4	DoS
UNSW-NB15	2015	No	49	9	DoS
CICIDS2017	2017	No	80	14	DoS, XSS, SQL Injection
BoT-IoT	2018	Yes	45	10	DoS/DDoS
N-BaIoT	2018	Yes	115	2	Botnet attacks (Mirai and Gafgyt)
ToN-IoT	2020	Yes	44	9	DoS/DDoS, SQL Injection, XSS, MITM
Edge-IIoTset	2022	Yes	62	14	DoS/DDoS, SQL Injection, XSS, MITM

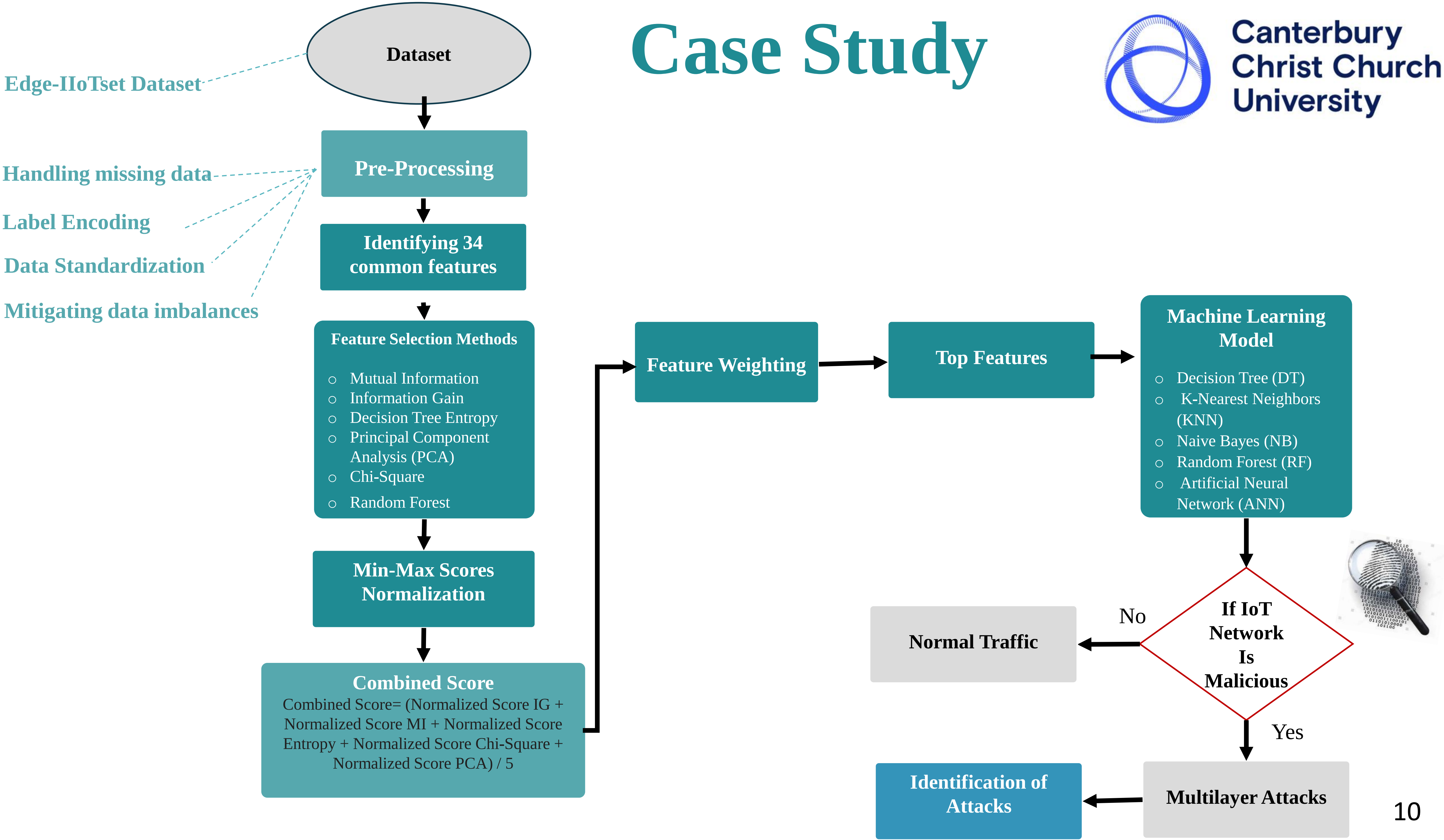
Methodology

Canterbury Christ Church University



Case Study

Canterbury Christ Church University



Common Feature Selection

Canterbury Christ Church University

Iterate over attack_type feature

Feature listing for selected attack

Count feature occurrences

Identify common features

Feature Selection Methods

Canterbury Christ Church University

- Chi-Square: All 34 features are critical.
- Mutual Information: 26 out of 34 features as significant.
- Information Gain: 31 significant features.
- PCA: 33 significant features.
- Decision Tree Entropy: Seven significant features.
- Random Forest: 27 out of 34 features as significant.

Hyperparameter Tuning

- Hyperparameter Tuning via Randomized Search
- Goal: Classify IoT Network Traffic into Normal and Multilayer Attacks

- Tuned Classifiers:
  - Random Forest (RF)
  - Decision Tree (DT)
  - k-Nearest Neighbors (KNN)
  - Artificial Neural Network (ANN)
  - Naïve Bayes (NB)

Decision Tree	Random Forest	KNN	ANN	Naïve Bayes
• Criterion: entropy • max_depth: 5 • min_samples_split: 10 • max_features: sqrt • min_samples_leaf: 4	• criterion: gini • max_depth: 10 • n_estimators: 10	• n_neighbors: 5 • P: 1 • Metric: manhattan	• Activation: ReLU • Optimizer: adam • loss function: • Metrics: accuracy binary_crossentropy • Epochs: 10 • batch_size: 32	• var_smoothing: 1.232846739442066e-08

Results of Feature Selection

Canterbury Christ Church University

Evaluation of Five ML Classification Models

- Considered a full set of 62 features of Edge-IIoTset dataset.
- 34 common features.
- Significant features by applying Feature selection methods.

Accuracy Rates

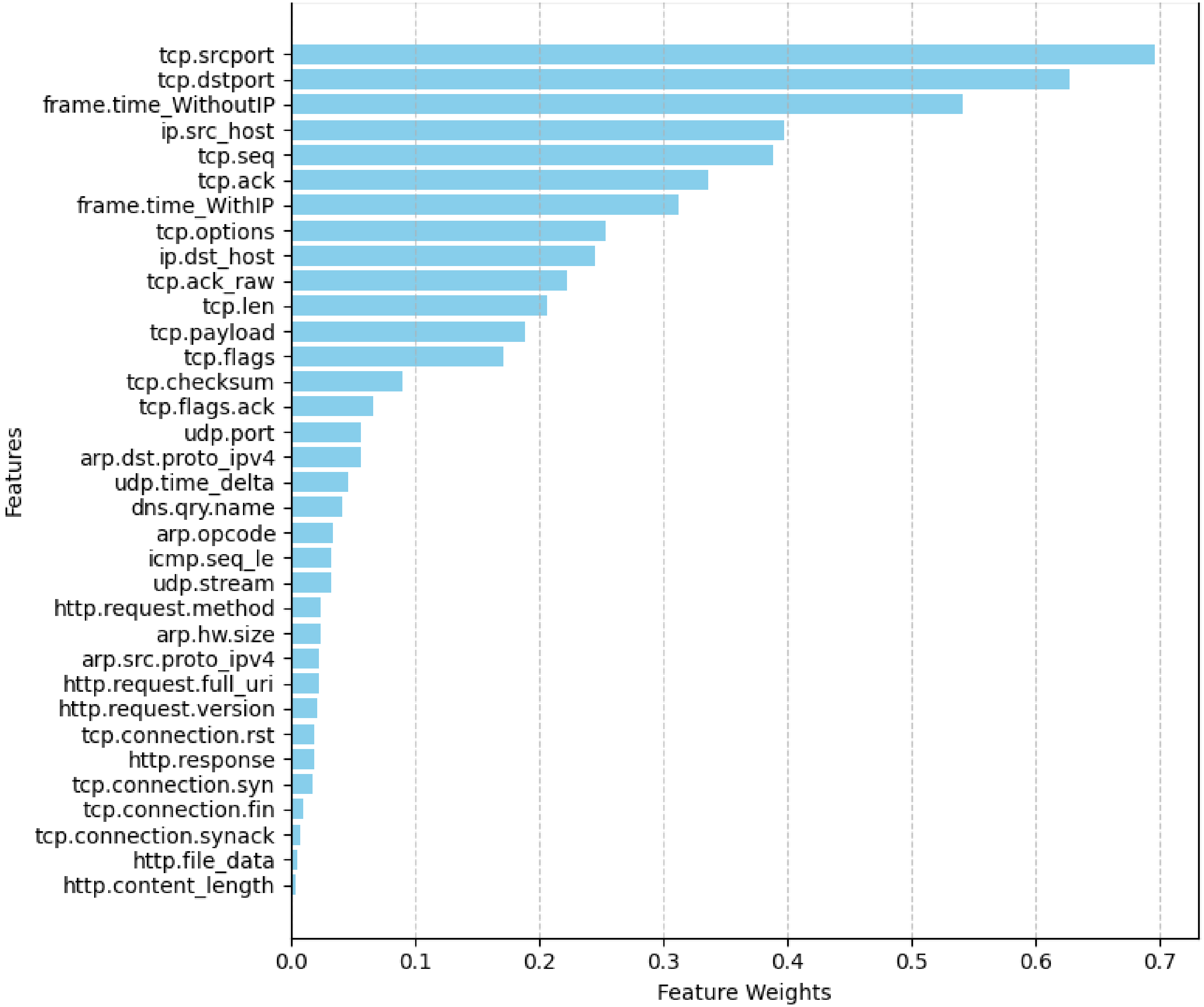
	FS Methods							
Ml	**All 62**	**All 34**	**IG**	**DTE**	**MI**	**Chi²**	**PCA**	**RF**
DT	94.3	99.87	85.74	71.03	97.13	99.87	99.87	94.32
RF	94.58	95.78	98.41	99.84	99.86	95.78	98.46	84.9
KNN	98.4	97.89	97.89	99.93	97.95	97.89	84.84	97.88
ANN	76.1	86.41	98.88	92.92	92.7	86.41	80.56	92.25
NB	66.77	61.22	61.19	38.48	61.17	61.22	43.96	61.31

The Least Significant → The Most Significant

- Mutual Information feature selection: impressive accuracy with only 26 features.
- RF classifier achieved the highest accuracy, while Naïve Bayes model achieved the lowest accuracy.

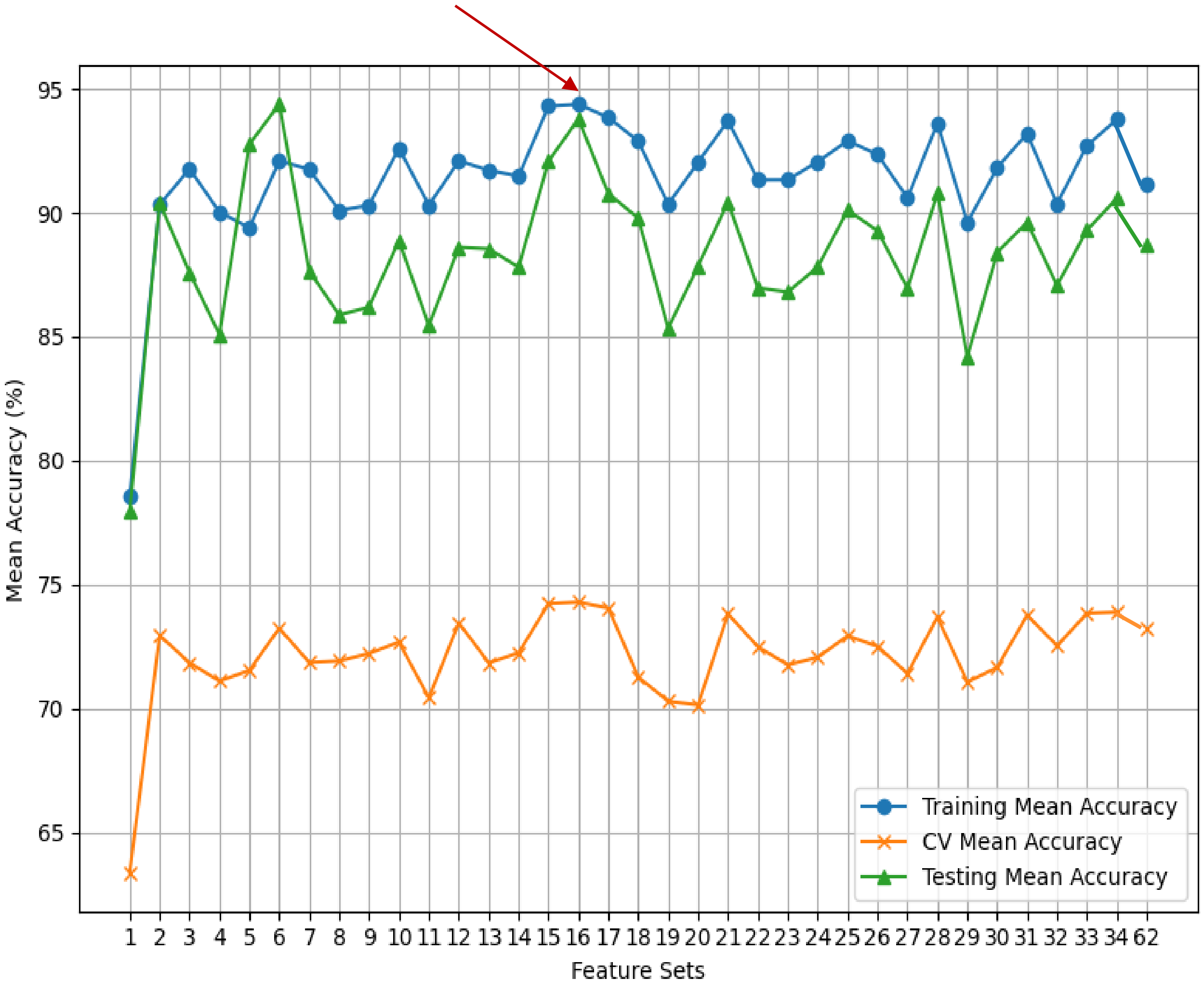
AL Sukhni, B. A., Manna, S. K., Dave, J. M., and Zhang, L. 2023. Exploring Optimal Set of Features in Machine Learning for Improving IoT Multilayer Security in IEEE 9th World Forum on Internet of Things. Aveiro, Portugal, Oct 2023, in Press

Feature Weighting

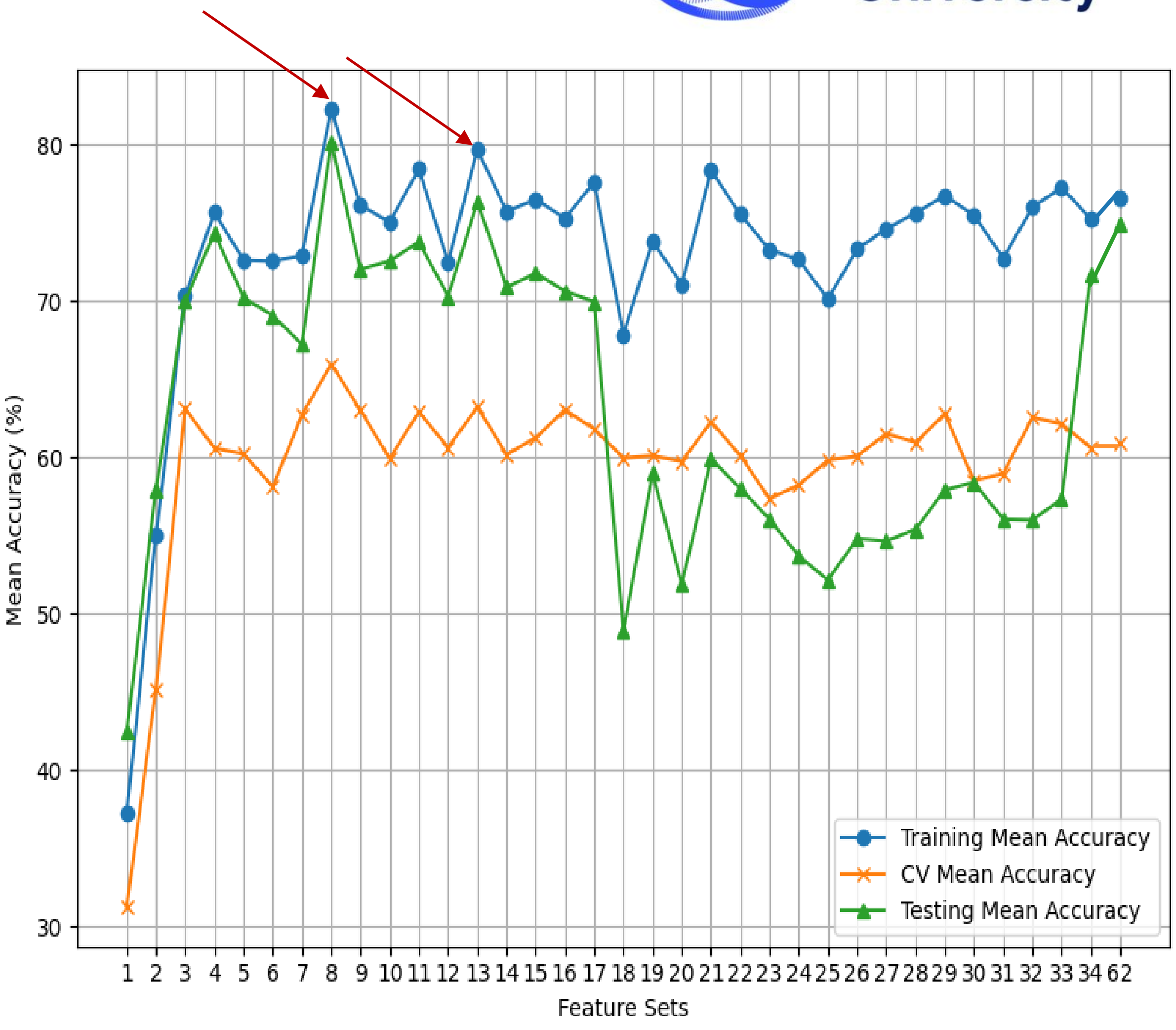


Semi-Automated Tool

Canterbury Christ Church University



Binary Classification



Multiclass Classification

Evaluation of 13 Features

Canterbury Christ Church University

Alg	Metric	Normal	DDoS_TCP	DDoS_UDP	DDoS_HTTP	DoS_ICMP	SQL injection	XSS attacks	MITM	Password
NB	Pr	0.99	1.00	1.00	0.36	0.96	0.84	***0.02***	1.00	1.00
	Rc	0.22	0.63	1.00	0.99	1.00	0.42	***0.04***	1.00	1.00
	f1	0.36	0.77	1.00	0.53	0.98	0.56	***0.03***	1.00	1.00
RF	Pr	0.79	0.84	1.00	1.00	0.99	0.60	0.59	0.72	1.00
	Rc	0.73	0.60	1.00	1.00	1.00	0.98	0.46	1.00	1.00
	f1	0.76	0.70	1.00	1.00	0.99	0.74	0.52	0.83	1.00
DT	Pr	0.96	0.99	1.00	0.85	1.00	0.30	0.66	0.71	1.00
	Rc	0.60	0.65	1.00	0.38	0.99	1.00	0.34	1.00	0.97
	f1	0.74	0.78	1.00	0.52	0.99	0.47	0.45	0.83	0.98
ANN	Pr	0.93	0.85	1.00	0.45	0.99	0.58	0.36	0.97	0.38
	Rc	0.44	0.88	1.00	0.30	0.99	0.89	0.82	1.00	0.30
	f1	0.60	0.86	1.00	0.36	0.99	0.70	0.50	0.98	0.33
KNN	Pr	1.00	1.00	1.00	0.70	1.00	0.70	0.83	1.00	0.79
	Rc	1.00	1.00	1.00	0.72	1.00	0.80	0.95	1.00	0.54
	f1	1.00	1.00	1.00	0.71	1.00	0.75	0.89	1.00	0.64

Evaluation of 8 Features

Alg	Metric	Normal	DDoS_TCP	DDoS_UDP	DDoS_HTTP	DoS_ICMP	SQL injection	XSS attacks	MITM	Password
NB	Pr	0.99	1.00	1.00	0.45	0.96	0.71	***0.02***	1.00	1.00
	Rc	0.17	0.60	1.00	0.99	1.00	0.63	***0.04***	1.00	1.00
	f1	0.29	0.75	1.00	0.62	0.98	0.67	***0.03***	1.00	1.00
RF	Pr	0.79	0.66	1.00	1.00	0.96	0.46	***0.00***	1.00	1.00
	Rc	0.96	1.00	1.00	0.99	1.00	0.98	***0.00***	1.00	1.00
	f1	0.79	0.79	1.00	0.99	0.98	0.98	***0.00***	1.00	1.00
DT	Pr	0.98	0.97	1.00	0.85	1.00	0.93	0.79	0.63	1.00
	Rc	0.89	1.00	1.00	1.00	0.98	0.98	0.93	0.78	0.99
	f1	0.93	0.99	1.00	0.92	1.00	0.95	0.85	0.69	1.00
ANN	Pr	0.57	1.00	1.00	0.19	0.91	0.56	***0.12***	0.95	0.42
	Rc	0.64	0.67	1.00	0.18	1.00	0.87	***0.11***	1.00	0.17
	f1	0.60	0.80	1.00	0.19	0.95	0.68	***0.11***	0.97	0.25
KNN	Pr	1.00	0.99	1.00	0.83	1.00	0.87	0.90	1.00	1.00
	Rc	1.00	0.98	1.00	0.80	1.00	0.87	0.96	1.00	0.98
	f1	1.00	0.98	1.00	0.81	1.00	0.87	0.93	1.00	0.99

Conclusion and Future Work

Canterbury Christ Church University

Conclusion:

- Broader focus on multilayer attacks (physical, network, and application layers).
- Extracted common features from the dataset.
- Utilized multiple feature selection methods.
- Enhanced accuracy through hyperparameter tuning.
- By using the results of Mutual Information features, the RF model achieved the highest accuracy, while Naïve Bayes model achieved the lowest accuracy.
- Implemented feature weighting to identify optimal features for multilayer IoT attack detection.
- Only 13 features are critical for efficient detection and classification of multilayer attacks.

Future Work:

- Expand the research to diverse IoT datasets.
- Real-time implementation and deployment assessment.

Research Outputs

Canterbury Christ Church University

1. Sukhni, B. A., Dave, J. M., Manna, S. K., and Zhang, L. 2022. Investigating the Security Issues of Multi-layer IoT Attacks Using Machine Learning Techniques in International Conference on Human-centred Cognitive Systems (IEEE_HCCCS), 17th -18th December, Shanghai, China pp. 1-9, doi: 10.1109/HCCS55241.2022.10090400.
2. Sukhni, B. A., Manna, S. K., Dave, J. M., and Zhang, L. 2022. Investigating the security issues of multi-layer IoMT attacks using machine learning techniques (Poster presentation). In Exploring Research and Development in the MedTech, Life Science and Healthcare sectors, Maidstone Innovation Centre, 9 Nov 2022.
3. Al Sukhni, B., Manna, S.K., Dave, J.M., Zhang, L. (2023). Machine Learning-Based Solutions for Securing IoT Systems Against Multilayer Attacks. In: Tomar, R.S., et al. Communication, Networks and Computing. CNC 2022. Communications in Computer and Information Science, vol 1893. Springer, Cham. https://doi.org/10.1007/978-3-031-43140-1_13
4. AL Sukhni, B. A., Manna, S. K., Dave, J. M., and Zhang, L. 2023. Exploring Optimal Set of Features in Machine Learning for Improving IoT Multilayer Security in IEEE 9th World Forum on Internet of Things. Aveiro, Portugal, Oct 2023, in Press.

References

[1] Malhotra, P. et al. (2021) “Internet of Things: Evolution, concerns and security challenges,” Sensors (Basel, Switzerland), 21(5), p. 1809. doi: 10.3390/s21051809.

[2] Hassija, V. et al. (2019) “A survey on IoT security: Application areas, security threats, and solution architectures,” IEEE access: practical innovations, open solutions, 7, pp. 82721–82743. doi: 10.1109/access.2019.2924045.

[3] Tahsien, S. et al. (2020) “Machine learning based solutions for security of Internet of Things (IoT): A survey,” Journal of network and computer applications, 161(102630), p. 102630. doi: 10.1016/j.jnca.2020.102630.

[4] Atlam, H. F. and Wills, G. B. (2020) “IoT security, privacy, safety and ethics,” in Internet of Things. Cham: Springer International Publishing, pp. 123–149.

[5] Khanam, S. et al. (2020) “A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things,” IEEE access: practical innovations, open solutions, 8, pp. 219709–219743. doi: 10.1109/access.2020.3037359.

[6] Ahmad, R. and Alsmadi, I. (2021) “Machine learning approaches to IoT security: A systematic literature review,” Internet of Things, 14(100365), p. 100365. doi: 10.1016/j.iot.2021.100365.

[7] Kumar, R. and Sharma, R. (2022) “Leveraging blockchain for ensuring trust in IoT: A survey,” Journal of King Saud University - Computer and Information Sciences, 34(10), pp. 8599–8622. doi: 10.1016/j.jksuci.2021.09.004.

[8] Mohanta, B. K. et al. (2021) “Addressing security and privacy issues of IoT using blockchain technology,” IEEE internet of things journal, 8(2), pp. 881–888. doi: 10.1109/jiot.2020.3008906.

Thank you