List of Figures

Figure 1.1: Types of Cyber Threats [2]........2
Figure 1.2: Categories of Cyber Security [4]........3
Figure 1.3: Evolution and Relationship of AI, ML, and DL........6
Figure 1.4: Categorization of AI........6
Figure 1.5: Components of Narrow/Weak AI [24]........7
Figure 2.1: Architecture of MalCrawler........22
Figure 2.2: Focused Crawler Module........22
Figure 2.3: Thread Wise Software Design of MalCrawler........28
Figure 2.4: Malicious Page Seek Rate (α)........30
Figure 2.5: Entanglement Avoidance........30
Figure 3.1: Snapshot of the Webpages Dataset........38
Figure 3.2: Class Label Distribution- Malicious & Benign........38
Figure 3.3: URL Plot (Vectorized using Profanity Score)........39
Figure 3.4: Geographic Distribution of IP Addresses - Malicious........39
Figure 3.5: Geographic Distribution of IP Addresses - Benign........39
Figure 3.6: Univariate Plots: URL Length, JS Length & Obfuscated JS Length........40
Figure 3.7: Trivariate 3D Plot........40
Figure 3.8: Trivariate Correlation Matrix........41
Figure 3.9: Tri-variate Pairwise Plot........41
Figure 3.10: Tri-variate Parallel Coordinates Plot........41
Figure 3.11: Bivariate Pairwise Plot........42
Figure 3.12: Bivariate Density Plot........42
Figure 3.13: Plot of Top Level Domain ('tld') Attribute........42
Figure 3.14: Plot of Who Is Registration ('who_is') Attribute........43
Figure 3.15: Plot of HTTPS ('https') Attribute........43
Figure 3.16: Web Content: Sentiment Score........44
Figure 3.17: Web Content: Profanity Score........44
Figure 3.18: Web Content- Word Count........44
Figure 3.19: 3D Plot of Complete Dataset........45
Figure 3.20: Tri-surface Plot of Complete Dataset........45

Figure 3.21: 2D SOM Hexagonal Plot of Webpages Dataset (with Classes Superimposed)........46
Figure 3.22: SOM Rectangular with Classes Marked on Top........47
Figure 3.23: SOM Plot on World Map (Showing Country Wise Density Distribution)........47
Figure 3.24: Country Name ('geo_loc') Attributes Plotted on the Rectangular SOM Grid........48
Figure 3.25: Domain Name ('tld') Attribute Plotted on Rectangular SOM Plot Grid........49
Figure 3.26: Snapshot of the Hybrid Apps Dataset........52
Figure 3.27: Class Labels Distribution- Malicious & Benign Hybrid Apps........53
Figure 3.28: Plot of WebView_or_ ChromeTabs & JavaScript_ Enabled Attributes........53
Figure 3.29: Plot of JavaScript_Interface_Defined & Access_to_System_Calls Attributes........53
Figure 3.30: Plot of 'Obfuscated_JavaScript_Permitted' & 'Interface_Android_Code_Obfuscated Attributes'........54
Figure 3.31: Plot of 'Outside_URL' & 'Google_Safe_Browsing' Attributes........54
Figure 3.32: Plot of 'HTTP_or_HTTPS' & 'JavaScript_Input_Validation' Attributes........54
Figure 3.33: Plot of 'Web_redirection' Attribute........55
Figure 3.34: Univariate Plot of 'JavaScript_Interface_length'Attribute (in KB)........55
Figure 4.1: Malicious Website Detection Process Using Conventional ML........59
Figure 4.2: Classification Accuracy of Attributes........69
Figure 4.3: Confusion Matrices using Conventional ML Algorithms (All 25 Attributes used)........71
Figure 4.4: Computation Resources Used by Attributes........72
Figure 4.5: Confusion Matrix- Conventional ML Algorithms with Top Five Attributes........73
Figure 5.1: DNN Model for Malicious Webpage Classification........79
Figure 5.2: A Single Computation Unit in DNN........81
Figure 5.3: Training and Validation Accuracy........88
Figure 5.4: Training and Validation Loss........88
Figure 5.5: Impact of Initial Bias........89
Figure 5.6: Confusion Matrix........90
Figure 5.7: AUC-ROC Graph........90
Figure 6.1: Hybrid Deep Learning Model........96
Figure 6.2: Stage-I: Unsupervised Pre-training AE for Web Content & JS Encoding........98
Figure 6.3: Stage-II: DNN Model for Classification........100
Figure 6.4: Loss for Stage-I Unsupervised Training........106

Figure 6.5: Training and Validation Accuracy 106
Figure 6.6: Validation Loss 107
Figure 6.7: Impact of Initial Bias 107
Figure 6.8: Confusion Matrix 108
Figure 6.9: AUC-ROC Graph 108
Figure 7.1: Schematic Diagram Describing the ML Process...121
Figure 7.2: Confusion Matrix after Validation 122
Figure 7.3: Attribute Ranking Based on Classification Accuracy 124
Figure 7.4: The "WebView Monitor" App 128
Figure 8.1: A Typical Federated Learning (FL) Round 136
Figure 8.2: Client Process..138
Figure 8.3: DNN Model Used for FL Learning 139
Figure 8.4: Hierarchical Federated Learning (HFL) Topology 143
Figure 8.5: Test Accuracy vs. Communication rounds (with various values of *E, B*, & *n*) 146
Figure 8.6: Conventional Centralized ML vs. FL 146
Figure 8.7: Impact of Initial Bias, Class Wt & iid-data (*E=20, B=5, n=1000* for all scenarios)...147
Figure 8.8: Confusion Matrix FL vs. ML...148
Figure 8.9: HFL vs. FL Accuracy Plot..149
Figure 8.10: Confusion Matrix FL vs. HFL..149
Figure A.1: Code Snippet for Extracting 'url_len'...156
Figure A.2: Code Snippet for Computing 'geo_loc'..157
Figure A.3: Code Snippet for Computing 'js_len'..157
Figure A.4: Code Snippet for Extracting 'tld'...157
Figure A.5: Code Snippet for Computing 'who_is'...158
Figure A.6: Code Snippet for Computing 'https'..158
Figure A.7: Code Snippet for Class Labels..158
Figure B.1: Code Snippet for Disassembling APKs Using JADX Disassembler.....................160
Figure B.2: Code Snippet for Checking WebView or Chrome Tab Usage 161
Figure B.3: Code Snippet for Checking Whether JavaScript is Enabled or Not 161
Figure B.4: Code Snippet for Checking JavaScript Interface...162
Figure B.5: Code Snippet to Check Access to System Calls...162
Figure B.6: Code Snippet to Check Permission for Obfuscated JavaScript...........................163

Figure B.7: Code Snippet to Check for Obfuscation of JavaScript Interface Code 163

Figure B.8: Code Snippet to Check Permission for Outside URLs...164

Figure B.9: Code Snippet to Check Whether Safe Browsing is Being Used or Not................164

Figure B.10: Code Snippet to Check Usage of HTTPS 164

Figure B.11: Code Snippet to Check the Usage of JavaScript Input Validation 165

Figure B.12: Code Snippet to Check Whether Web Redirection is Permitted or Not...........165

Figure B.13: Code Snippet for Checking Android Code Length in JavaScript Interface.........166

List of Tables

Table 1.1: Types of Malwares 3

Table 2.1: Summary of Results- MalCrawler 29

Table 2.2: Summary of Webpages Dataset..31

Table 2.3: Summary of Hybrid Apps Dataset...32

Table 3.1: Specifications of Webpages Dataset...35

Table 3.2: Attributes of Webpages Dataset..36

Table 3.3: Specifications of Android Hybrid Apps Dataset 50

Table 3.4. Attributes of Hybrid Apps Dataset...51

Table 4.1: List of Attributes Considered- Conventional ML......................................61

Table 4.2: Attribute Selection using 'Gain Ratio' & '10-Fold Cross Validation' 68

Table 4.3: Classification Results with Conventional ML Algorithms (all 25 attributes used)..70

Table 4.4: Meaning of the Classification Metrics Used 70

Table 5.1: Feature (Input) layer- DNN with Structured Data...................................79

Table 5.2: Layer-wise Tunable Parameters (DNN with Structured Data)................................80

Table 5.3: Evaluation on Test Dataset (DNN with Structured Data)..89

Table 6.1: Attributes in Dataset File (DNN with Unstructured Data) 99

Table 6.2: Evaluation on Test Dataset (Hybrid DNN with Unstructured Data) 107

Table 7.1: Summary of the WebView Class 117

Table 7.2: Validation Results of ML on Hybrid Apps...122

Table 7.3: Classification Results- Hybrid Apps on Google Play...123

Table 8.1: Layer Wise Tunable Parameters 140

Table 8.2: FL Algorithm for Android Web Security...141

Table 8.3: Hierarchical FL (HFL) Algorithm for Android Web Security 143

Table 8.4: Evaluation of Test Dataset 147

List of Abbreviations/Symbols

Abbreviation/Symbol	Definition
α	Symbol for Malicious Page Seek Rate (A value defined for the seek rate of a Malicious Webpage by MalCrawler) or Learning Rate in the Context of DNN
Adam	Adaptive Moment Estimation (A Replacement Optimization Algorithm for SGD)
ADASYN	Adaptive Synthetic (An Algorithm for Generating Synthetic Samples in ML)
AE	Auto Encoder
AI	Artificial Intelligence
AJAX	Asynchronous JavaScript and XML
ANN	Artificial Neural Networks
API	Application Programming Interface (An interface that defines interaction between multiple software)
APK	Android Package (A Format of Archived Executable File in Android)
ASIC	Application Specific Integrated Circuit
AUC-ROC	Area Under Curve- Receiver Operating Characteristics
b	Bias
BERT	Bidirectional Encoder Representation from Transformers
C4.5	A Decision Tree Algorithm
CNN	Convolutional Neural Network
CPU	Central Processing Unit
CSS	Cascading Style Sheets (A Style Sheet Language)
DBN	Deep Belief Networks
DNN	Deep Neural Network
DNS	Domain Name System
DOM	Document Object Model
DP	Differential Privacy
DT	Decision Tree
E	Loss Function
ELMo	Embedding from Language Models
FFN	Feed Forward Network

Abbreviation/Symbol	Definition
FIFO	First In First Out (A method of queuing in memory)
FL	Federated Learning
FN	False Negative
FNR	False Negative Rate
FP	False Positive
FPR	False Positive Rate
FWS	Federated Learning based Web Security (An App Developed as Part of this Thesis)
GPU	Graphics Processing Unit
HFL	Hierarchical Federated Learning
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure (It is a HTTP Protocol that Supports Encryption)
IDF	Inverse Document Frequency (A Weighted TF that Increases Weight of Words that Occur Less Frequently)
IE	Microsoft Internet Explorer
iFrame	An HTML Element
IP	Internet Protocol
JADX	A JavaScript Disassembler
JDBC	Java Database Connectivity (A Java API for Database Connectivity)
jQuery	A JavaScript Library
JS	JavaScript
LSTM	Long Short Term Memory (A Type of RNN)
MalCrawler	Name given to a Customized Focused Crawler designed for this Research to Crawl Malicious Websites
ML	Machine Learning
NLP	Natural Language Processing (A Branch of AI Handling Interpretation of Human Language)
NN	Neural Network
PCA	Principal Component Analysis
RBF	Radial Basis Function
RELU	Rectified Linear Unit (An Activation Function for ANN)
RNN	Recurrent Neural Network
SDK	Software Development Kit
SGD	Stochastic Gradient Descent

Abbreviation/Symbol	Definition
SMOTE	Synthetic Minority Oversampling Technique (An Algorithm for Generating Synthetic Samples in ML)
SQL	Structured Query Language
SVM	Support Vector Machine
TF	Term Frequency (Count of Number of Times a Word Appears in a Document)
TFF	Tensor Flow Federated (A Python Library for Federated Learning)
TLD	Top Level Domain
TN	True Negative
TNR	True Negative Rate
TP	True Positive
TPR	True Positive Rate
TPU	Tensor Processing Unit (An ASIC for DNN Learning)
UI	User Interface
URL	Uniform Resource Locator (Address of a Webpage)
W	Weights
Web 2.0	Webpage Technology that supports User Generated Content
WebView	An Android Class
WebView-OAuth	WebView Authentication Method
WEKA	Waikato Environment for Knowledge Analysis (A Machine Learning Software)
WHOIS	Provides Domain Registration Details
X	Input to a NN
XHR	XML HTTP Request (An API for Transferring Data Between Web Server & Web Browser)
XML	eXtensible Markup Language
XML	Extensible Markup Language (A Markup Language for Encoding Documents)
XSS	Cross-site Scripting (A Type of Web Based Attack)
Y	Output of a NN
$\delta\, model$	A Small Incremental Model in Federated Learning with Each Participating Device