

INDEX

CHAPTER- I INTRODUCTION		1 – 31
1.1	Introduction	1
	1.1.1 The Relevance of the Project	1
	1.1.2 Internet of Things (IoT)	4
1.2	Sensors in Mobile Devices	9
	1.2.1 Accelerometer	9
	1.2.2 Gyroscope	11
	1.2.3 Magnetometer	13
	1.2.4 Ambient Light Sensor	14
	1.2.5 Fingerprint	15
	1.2.6 Heart rate sensor	15
	1.2.7 Barometer	16
	1.2.8 Global Positioning System (GPS)	16
	1.2.9 Near Field Communication (NFC)	17
	1.2.10 Humidity Sensor	17
	1.2.11 Ultrasonic sensors	18
	1.2.12 Deep Learning	18
	1.2.13 Advantages of Deep Learning for 1D Sensor Signals	19
1.3	RNN	20
1.4	LSTM	22
1.5	Modified sub-space KNN (msK)	26
1.6	Need for the proposed work	27
	1.6.1 Importance of suspicious activity detection using mobile sensor data	28
1.7	Objectives	29
1.8	Research Gap	30
1.9	Organisation of the thesis	30
CHAPTER- II REVIEW OF LITERATURE		32 – 48
2.1	Recent cases solved due to mobile phone activities	45

CHAPTER-III RESEARCH METHODOLOGY		49 – 100
3.1	Suspicious Activity Detection Using Mobile Sensor Data via Modified Subspace KNN (msK)	49
	3.1.1 Collection of mobile data	50
	3.1.2 Modified sub-space KNN	50
3.2	Activity classification	52
	3.2.1 Hardware details	54
	3.2.2 Data collection and training details	55
	3.2.3 Long Short-Term Memory	56
	3.2.4 DenseNET details	58
3.3	Mobile app	58
3.4	KNN and Gaussian SVM	64
3.5	Data Collection	65
3.6	LSTM feature extraction	66
3.7	IFDenseNET	67
3.8	Mobile App details	69
3.9	App building using flutter	71
	3.9.1 Creating an App in Flutter	71
	3.9.2 Creating a New Flutter Project	71
	3.9.3 Building the User Interface	72
	3.9.4 Running the App	72
	3.9.5 Customizing the App	72
	3.9.6 Deploying the App	72
3.10	Classification of actual Sensor data using python code	78
3.11	Extracting the information from the Sensor data app on android	80
3.12	Mobile Application for Sensor Data Collection	86
3.13	Firebase Configuration for Cross-Platform Development	99
3.14	Supabase Configuration	99
3.15	Deep learning code for data classification	100

CHAPTER- IV RESULTS		101 – 118
4.1	Suspicious activity detection using mobile sensor data with modified subspace KNN (msK)	101
4.2	Testing with trained actors	113
CHAPTER- V CONCLUSIONS AND FUTURE RECOMMENDATIONS		119 – 127
5.1	Detection of suspicious activity using mobile sensor data and Modified Sub-space K-NN for criminal investigations	122
BIBLIOGRAPHY		128 - 133
LIST OF PUBLICATION		134 - 134
IMPLEMENTATION CODE OF APP DEVELOPMENT		
PUBLICATIONS		
CERTIFICATES		

LIST OF TABLE

Table No.	Particulars	Page No.
1.1	Comparison of ANN, CNN, and RNN	21
1.2	Comparison of RNN, GRU, and LSTM	25

LIST OF FIGURE

Fig. No.	Particulars	Page No.
1.1	Classification of criminal activities	3
1.2	IoT as a centralized network connecting various societal components to a cloud infrastructure	5
1.3	Smart wearables monitoring vital signs, activity levels, and other physiological data	6
1.4	'IoTool' Mobile Application Interface for Sensor Data Acquisition	8
1.5	Accelerometer	10
1.6	Magnified view of an accelerometer chip on a mobile phone mother-board	11
1.7	Gyroscope	12
1.8	Magnetometer	13
1.9	The structure of a Recurrent Neural Network (RNN), designed to process sequential data. RNNs excel at learning long-term dependencies, making them suitable for tasks like natural language processing, machine translation, and speech recognition	20
1.10	Long short-term memory (LSTM) network structure	23
1.11	LSTM network structure, designed to learn long-term dependencies in data through gating mechanisms that control information flow	24
1.12	Concept diagram of proposed suspicious activity detector using msK	26
2.1	A Venn diagram showing the relationship between victim, threat, and defender in the context of crime	33
2.2	Big data and IoT interface [33]	36
2.3	IoT application developed for criminal tracking. The predicted routes the criminal could take based on the place where the crime occurred is found. [34]	36

Fig. No.	Particulars	Page No.
2.4	Multiple analytical perspectives and applications based on mobile phone data	41
2.5	Comparison of different methods and problems used in mobile phone data studies	42
3.1	Block diagram illustrating the application of modified subspace KNN for the detection of suspicious activities from mobile data	49
3.2	LSTM details	57
3.3	Thunkable software front user design interface	60
3.4	Sign-in window at Thunkable	62
3.5	Menu on thunkable app	63
3.6	The flow of the proposed work with KNN and Gaussian SVM	64
3.7	IFDenseNET-138 Conceptual Diagram for Classifying Mobile Phone Sensor Data	68
3.8	The block code outlines a mobile application designed for evidence collection	69
3.9	The EC mobile collection app exhibits different front-end states	70
3.10	File menu to flutter app	73
3.11	New flutter project	73
3.12	UI for new flutter application	74
3.13	Select main.dart as target file	77
3.14	The final app built	78
3.15	Installation UI for Sensordata app	80
3.16	UI to show progress-bar of installation	80
3.17	UI at the end of installation	81
3.18	Sign in window for app	82
3.19	UI to choose account during sign in	83
3.20	App main front UI offering user with an option to save	84

Fig. No.	Particulars	Page No.
	accelerometer data	
3.21	Version button in setting	85
3.22	Version button from android device	85
3.23	File menu to recover the data	86
3.24	Storage device setting to turn on bug reports	87
3.25	Setting to turn on Bug Report	88
3.26	Enabled Bug report in file	89
3.27	Bug report folder contents	90
3.28	Android folder to be opened inside the device Oppo A79 5G in this case	91
3.29	Data folder inside the android folder where app data is stored	92
3.30	Folders inside data folder showing installed app folder com. example. Sensordata	93
3.31	Files inside com.example.sensordata	94
3.32	Sensordata folder inside files	95
3.33	Files under sensor data	96
3.34	Sample file selection : Gyroscope.csv	97
3.35	Sample data stored for processing inside csv file	98
4.1	Capture rate versus error. Capture rate increases in packets per second percentage error in guessing the correct event decreases	101
4.2	The time between successive computations versus capture rate	102
4.3	The Confusion matrix for classifier accuracy out of 5994 test events 2988 normal events were classified as normal, whereas 9 of the normal events were classified as suspicious events	104
4.4	Scatter plot of the original data set	105
4.5	Receiver Operating Characteristic (ROC) curve and Area	106

Fig. No.	Particulars	Page No.
	Under the Curve (AUC) for Model 1	
4.6	Standard deviation of predictions	107
4.7	Results with two classification methods	108
4.8	Sample of sensor data points collected during a fight sequence	109
4.9	Proposed system flowchart. Data is collected using various mobile sensors, and the data is stored in an object called MobileDev	111
4.10	Confusion matrix illustrating the performance of the proposed IFDenseNet-138 model for 10-class classification	112
4.11	Event accident	114
4.12	Image from acted session where Attacker is about the attack victim	116
4.13	Two people recreating fighting scene	117
4.14	Person acting for scenario like suicide	118