IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 12, December 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

Mobile Device Anti-theft Motion Pattern Recognition Using LSTM

Ms. Ujwala Phere, Mr. Ramesh V. Shahabade

Student, Department of Computer Engineering, TEC, Nerul, India

Professor, Department of Computer Engineering, TEC, Nerul, India

ABSTRACT: Mobile phones have become extremely common and hence anti-theft detection has become a necessary need of the day. The anti-theft mechanism is supposed to determine if the phone has landed into the hands of a thief. It does so by detecting stealing behavior, which in turn is done by applying long short-term memory deep learning network to the accelerometer signals. The aim is to accurately detect ongoing unauthorized movement of the device. Locating lost phone GPS, remotely wiping and locking device, locking the SIM card service provider is only anti-theft mechanisms to discovery of the actual occurrence. They cannot detect the stealing behavior. Anti-theft mechanism will determine if the phone is in hands of thief, which detect stealing behavior by using long short-term memory is classifier to enhance accuracy of reorganization. We detect ongoing unauthorized movement of device notify its motion pattern inherent to actual movement. We use the waveform of accelerometer provided in mobile devices to research the pattern. We apply Long short-term memory classifier is depending upon matching patterns. Therefore, LSTM requires the step cycles store in database that is acceleration data. LSTM verify the unknown behavior, if mobile device hand of thief. Motion pattern to verify the identity of the person possession of the device immediately whenever it has moved. We provide a device detection system for performing authentication whenever the mobile device is move. We use the accelerometer data, which monitors the device's acceleration because of human movement. We collect data from 100 people one of which will be owner himself. Data from each person will store the accelerometer signals from the walking patterns of up to 20 to 30 steps. We aim to recognize unauthorized motion of the device in real time with up to 99.1% accuracy; an accuracy quite better than what we get in existing methods.

KEYWORDS: Mobile Handsets, Authentication, Pattern Matching, Acceleration**.**

I. INTRODUCTION

In today's world everyone has, mobile devices became personal and valuable item in human life. Per report in 2014, 3.1 million people had their devices stolen, as result, much private information is leak to the final public so on defeat of mobile device theft, lots of anti- theft mechanisms verifies the users identity for example, In order to defeat mobile device theft, a lot of anti-theft mechanisms have been designed. For example, Find My Device app allows users to locate their devices on google map, ring even when the phone has silent mode turned on and an option to remotely wipe their phones. Remotely wipe and lock device allows users to wipe their Android phone, as well as remotely lock or call the device. Lock SIM card once the user realizes his/her device has been stolen, he/she can use the GPS information to locate or remotely wipe and lock his/her device. Call the service operator to lock service user can call their mobile service provider to lock the device by disabling their SIM card. We use some methods require discovery of the unknown person before any security actions can be made. Although there are many device anti-theft mechanisms, all of them have one single limitation. In another word, none of these mechanisms can detect the stealing behavior. They need users' interaction to active these mechanisms. If users do not understand their device has stolen, an attacker will have many times to full physical access of the device. Therefore, the mechanisms are detecting the stealing behavior that is ongoing movement of the device. Furthermore, we employ motion patterns to comparing with the unknown person possession of the device immediately whenever it is move. We propose some way wherein we detect unauthorized movement of the device using its motion pattern. We use the waveform of accelerometer provided altogether mobile devices to analyze the motion pattern. Likewise, we apply long short term memory is classifier to reinforce accuracy of recognition. LSTM classifier to classify where the step cycle belongs to the owner's or not and extract the normalized waveform of step cycles and match with the database of the owner's step cycle.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

I.I Typical phases of system

Generally, the task of our system is divided into four phases is as follows-:

I. Training stage

Ii Testing stage

Iii Classification

Iv. Theft Detection

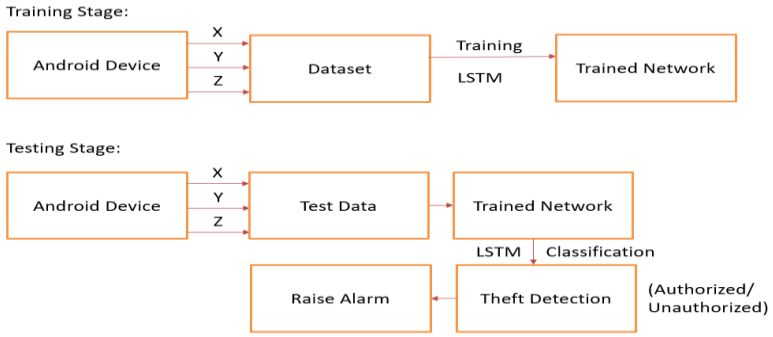

Figure 1: Flow of System.

I. Training-: Training phase functions as a means to populate the identification database with owner is the unique data. The device having owner data with normal motion behavior. The dataset is stored unauthorized motion behaviors comparing with current data. Whenever we open the device, its starts recording the data for the first 10 secs, so we start the app and start walking to record walking patterns. We collect 100 samples from 100 people including the owner in dataset. We label them as 'Authorized' for the owner and 'Not Authorized' for the others. In training phase, we collect 155083 steps/waveforms of samples. Long short-term memory deep learning network to the accelerometer signals is used in trained network. Train the LSTM network with the specified training options.

II Testing-: The testing module test the corrective pattern in waveform which is label them as authorized or unauthorized during an ongoing action of theft . The pattern waveforms from accelerometers provided within the mobile device. LSTM network analyze data, which is classify and detect. When the owner pattern waveforms are match with unknown data that is label as unauthorized raise the alarm means authorized and unauthorized waveforms are founded. Classify the test data. Specify the same mini-batch size used for training.

III Classification-: After training & testing stage is completed, data will be store in class wise to find out the result and predict using the model. The stored data in database identifying with unknown user data have test data is comparing to the owner's data. LSTM network is used for classification.

IV Theft Detection-: Theft detection phase is responsible for discovering that the device is currently experiencing normal motion behavior. Through the development of an algorithm which compares only the repetitive walking pattern using elementary arithmetic which is using comparison function and discover the pattern. We have been also created an identical algorithm to seek out and compare signature step cycle for a behavior. The matching phase compares unknown step cycles storing in training database to spot unauthorized moves. We are using methods to check with unknown behavior cycles further as cycle per behavior, which is within the database.

II. LITERATURE SURVEY

In this section, we discuss related work in three aspects: Testing, Training & Identification. The Introduction discusses related work in walking gait authentication and the unique challenges and goals of our system in comparison with these efforts, so this section will focus on other theft-reactant, authentication strengthening, and gait authentication work.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

Gadget Track is one popular anti-theft application implemented both on Android and iOS systems. Theft-reactant application currently available are based on combination of GPS, Wi-Fi positioning and cell tower triangulation to track location. For example is Gadget track is popular anti-theft application implemented on both IOS system and android.

According to report in March 2005[1] J. Mantyjarvi E. Vildjiounaite H. J. Ailisto, M. Lindholm and S. Makela. Identifying people from gait pattern with accelerometers. In that the method is uses other gait analysis techniques such as correlation and spectrum analysis, respectively to extract step cycles. We find that those methods can only work in ideal situation out of the presence of noise and without common irregular behavior.

Human gait has been studied in [2] and used in several previous behavioral biometric schemes using various classification algorithms different from ours to authenticate users. Human movement monitoring using wireless sensors has become an important area of research today. The use of wireless sensors in human identification is a relatively new idea with interesting applications in portable device security and user recognition. A real-time wireless sensor system based on inexpensive inertial sensors that uses gait analysis to uniquely identify subjects.

According to report in 2009[3] Human gait has been studied and used in several previous behavioral using various classification algorithms different from ours to authenticate users [2]. A novel channel coding approach for biometric authentication based on distributed source-coding principles is proposed. Biometric recognition is for mutated as a channel coding biometric schemes problem with noisy side information at the decoder and error-correcting codes are employed for user verification.

In 2010 [4] M. O. Derawi, C. Nickel, P. Bours, and C. Busch. Unobtrusive user authentication on mobile phones using biometric gait recognition. Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. In that, Dynamic Time Warping (DTW) is used to extract the similar cycles as step data. The benefit of DTW is that it can compare two data patterns with different size.

The report 2011 [5]is represented a solution to keep data secured by ensuring that only the authorized user can access the data in a mobile phone. By using gait recognition as an important element for the authentication process, we propose an automatic gait recognition system to be used for continuous authentication. Since recent gait recognition research only focuses on manual extraction of walking activities from the accelerometer signal, a solution to this issue could be activity recognition that would reduce the disadvantages of gait recognition by identifying the activities of a person continuously and automatically.

A smart phone anti-theft solution based on locking SIM card of mobile phone [6] is in 2011 is proposed. The solution proposed in this work mainly consists of software components, according to which hardware needs to be selected. It also gives the overall structure of mobile phone anti-theft system, the main software functional blocks and the implementation flow chart of each module. The functions of locking and unlocking of mobile and SIM card, anti-theft and short messaging service control are realized by adding locking SIM card setting module, locking SIM card control module and anti-theft processing module. By the use of software algorithm, users may find stolen mobile phone and protect critical information.

In report 2012[7] represent the human foot and heel-sole-toe walking strategy .It studied the human gait analysis to behavioral biometric schemes using various classification algorithms different from ours to authenticate users.
L .Li unobservable re-authentication for smartphones in 2013[8] reported to protect sensitive information on stolen devices from being compromised and implement re-authentication for mobile devices using users' finger movement classified by support vector machines.

According to report in 2013[9] Ren et al. also proposed a user verification scheme leveraging gait patterns derived from acceleration readings to mitigate against user spoofing attacks.

In 2014 [10] T. Saha H. Lu, J. Huang and L. Nachman. Unobtrusive gait verification for mobile phones. It proposed a gait verification method for mobile phones, which extract the gait features by spectrum analysis.

Children and adults minimize activated muscle volume by selecting gait parameters that balance gross mechanical power and work demands represented in 2015[11] gait patterns.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

In 2017[12] M. Muaaz and R. Mayrhofer. Smartphone-based gait recognition from authentication to imitation. IEEE Transactions on Mobile Computing. In that, it propose another mobile phone based gait authentication method using DTW.

According to report in May 2016 ,[13] Monitoring system for detecting mobile theft International Journal of Computational Science and Information Technology Vol.4,No.2,May 2016. In that to detect and monitoring of theft or misplace mobile phones, this paper develops a unique and efficient android application. The tracking application has the capability of SIM card detection, call monitoring, image capturing based on some predefined SMS. The application installed will be running in the background and will not be shown in the task manager as well. Once the mobile phone is lost, this application enables the user to track a mobile device and to receive notification via SMS to a predefined number. Some specified formatted messages can be used to control the theft mobile phone.

Unauthorized walking behavior

Our approach is based on gait analysis techniques on mobile devices. Some existing methods have been proposed in this field.

Table 1: Comparison of various methods proposed for long short-term memory.

SR No.	Author	Method	Outcome	Limitations	Year
1	D.Dakun Shen, Ian Markwood, Dan Shen, Yao Liu[14]	Statistical correlation test and k-s statistical test	Uses correlation to extract human walking data and identify users current gait pattern	Comparison tools should be used	March 2018
2	M. Muaaz and R. Mayrhofer, "Smartphone based gait recognition: From authentication to imitation".[13]	Gait authentication method	Develop the android application to capture gait data.	No false positives under impersonation attack	May 2017
3	P. Fernandez-Lopez, J. Liu-Jimenez, C. Sanchez-Redondo and R. Sanchez-Reillo, "Gait recognition using smartphone".[12]	Biometric gait analysis	Users have to carry the sensor device and walk as normally	it is an unobtrusive biometric modality,	Oct 2016
4	T. Y. Hubel and J. R. Usherwood [11]	Gait kinematics	Measurement of ground reactions forces in walking children and adult humans	Reduces activation requirement of power	March 2015
5	T. Saha, H. Lu, J. Huang and L. Nachman, "Unobtrusive gait verification for mobile phones"[10]	gait verification method	extracts gait features	Addressed before unobtrusive gait verification is practical.	Feb 2014
6	L.Li ,X.Zao and G.Xue[9]] "Unobservable re-authentication for smartphones"	K-s Test, correlation, Classification	Monitors users current figure movement	A good candidate for such passwords is the owner's biological data.	Feb 2013
7	Y. Ren, Y. Chen, M. C. Chuah, and J. Yang[8]+	Gait recognition	Analyze and understand peoples physical and mental states	Device should be registered	June 2013

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

8	J. R. Usherwood, A. J. Channon, J. P. Myatt, J. W. Rankin and T. Y. Hubel, "The human foot and heel–sole–toe walking strategy[7]	Human gait analysis	M'-shaped walking ground reaction force profile does not require the plant grade human foot or heel–sole–toe stance	Shin muscles that dissipate energy,	May 2012
9	G. Bajrami, M. O. Derawi and P. Bours, "Towards an automatic gait recognition system using activity recognition[5]	Gait recognition	For the authentication process	*I*dentifying the activities of a person continuously and automatically.	Oct 2011
10	S. Argyropoulos, D. Tzovaras, D. Ioannidis and M. G. Strintzis, "A channel coding approach for human authentication from gait sequences[3]"	Biometric recognition	Error correcting codes are employed for user verification	The noise channel distribution in the decoding process improves performance	May 2009
11	A. Annadhorai, E. Guenterberg, J. Barnes, K. Haraga and R. Jafari, "Human identification by gait analysis",[2]	Human gait analysis	It involves analyzing the walking pattern of a person and identifying features	it is an unobtrusive biometric modality	March 2008
12	J. Mantyjarvi, M. Lindholm, E.Vildjiounaite, S. M. Makela and H. A. Ailisto[1]	Biometery,Gait analysis	Describe gait identification using cumulatnts of accelerometer data	Gait cycles detected first	March 2005

III. MOTION PATTERN RECOGNISATION

Motion pattern identification is responsible for discovering that the device is currently experiencing normal motion behaviors. The in identification module, the step cycles extracted from previous procedure need to be assigned into database. In training process, step cycles are compared with each behaviors in database. If they have a high correlation, the step cycle is assigned into this behavior. If the step cycle does not match any of these behaviors, this step cycle will be identified as a new behavior and stored into database. In testing process, if these step cycles is matched with the database, then the current user is identified. Otherwise, alarm will be active behavior. Existing tools like statistical and K-S statistical are identified the pattern waveform which is required more comparisions.so due to more comparison LSTM (Long-short term memory) is best to all. LSTM network is a latest offering from deep learning. LSTM Specify the input size as 1 (the number of features of the input data).
A simple LSTM neural network for classification. The neural network starts with a sequence input layer followed by an LSTM layer. To predict class labels, the neural network ends with a fully connected layer, a softmax layer, and a classification output layer.

III.I LSTM (Long short- term memory) Network

The LSTM (long short-term memory) network enables to input sequence data into a network and make predictions based on the patterns of data. LSTM network specify in five layers is as follows-: Sequence Input layer, Bilstm layer, Softmax layer, fully connected layer, Classification layer .The syntax of Long shot-term memory network, which is train network with sequence of

```
Layers = [...
sequenceInputLayer (input Size)
bilstmLayer (numHiddenUnits, output mode= "last")
FullyConnectedLayer (numClasses)
SoftmaxLayer
```

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

Classification Layer].

Above all these layers construct and train the LSTM network, Long short-term memory network to make predictions about the current input have a separate memory cell that can store long-term information without being affected by the current input or output. This allows them to learn long-term dependencies.

When a device is sitting on desk, the data recorded by its accelerometer contains valuable information that can be used to identify users. Hence, we should ignore this data rather than attempting process into step cycles. However, we do need to detect the beginning of a motion pattern in timely. This is important in training and testing stage to avoid wasting any time in the user identification process. In order do our approach should in device is in two state

III.II Mobile device is in hand of thief-:Figure 3 shows accelerometer reading for device is n hand being operated by walking user, carried by walking user respectively. The peaks represents device is in hand of thief. So there is no change of acceleration.it completes peak valuue10.2 represents device state

Figure2: Device States (in hand) waveforms.

III.III Rest operation state-: When device is on desk represents buffer size and sensitivity is more than 10.2. Therefore, device is in rest state.

Figure 3 shows device is on desk state.

III.IV Running State- : Figure 4 represents when device is in running state peaks is in disturb they can be in out of peak value and cannot completed cycle fully.

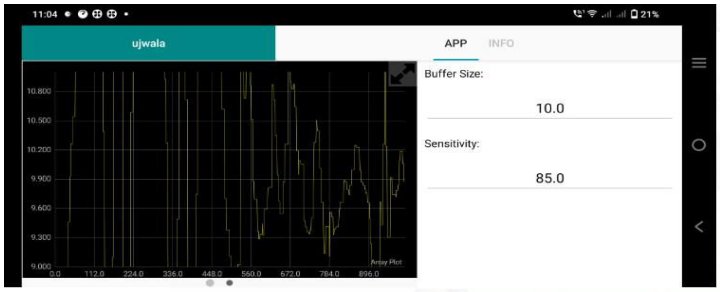

Figure.4: Running state.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

III.V Train network-: Train a deep learning network with an LSTM projected layer for sequence-to-label classification. Reducing the number of learnable parameters by projecting an LSTM layer rather than reducing the number of hidden units of the LSTM layer maintains the output size of the layer and, in turn, the sizes of the downstream layers, which can result in better prediction accuracy. Train the LSTM network with the specified training options. Train with a mini-batch size of 27 for 50 epoch because the mini-batches are small with short sequences, net = trainnetwork (XTrain, YTrain, layers, options);

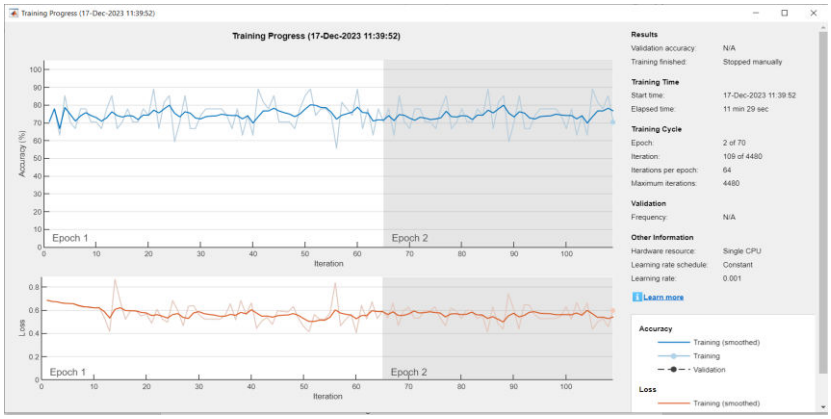

Figure 5: Training Progress

Trainings accuracy- Training accuracy is used in both 2 on number of correct prediction and total number of prediction. For example For example, if your model predicts the sentiment of 100 tweets as positive or negative, and 99of them match the true sentiment, then your accuracy is 99/100 = 0.99 or 99%.

Training Loss- Curve records the actual difference between the model's prediction and the actual true output.

III.VI Test data

Calculate the classification accuracy of the predictions on the test data. For this, the test data will need to go through the same processing as the training data. We will first evaluate the model against the test data and check for the loss. Then we proceed to use this model and predict for both the training dataset and the test

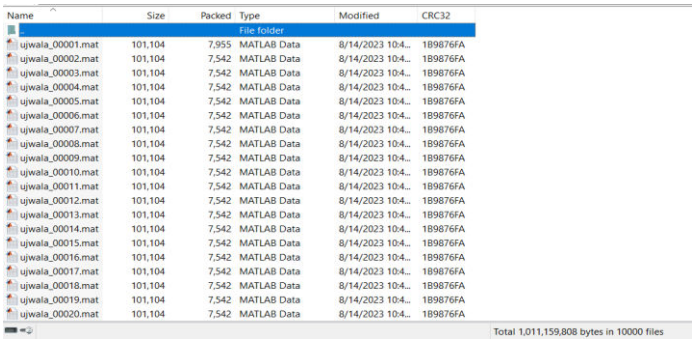

Figure6: Dataset files screenshot

III.VI Pattern matching method

After running pattern synchronization on test data and collecting a set of cycles corresponding to one behavior, we attempt to match it to some behavior in the database to verify the user identity as device owners. For this pattern matching method, we use confusion matrix that represents the authorized and not authorized user, confusion matrix is a table that summarizes how successful the classification is at predicting belonging to various classes. For example,

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

authorized user is 15500 and not authorized user is 248 we get 99.1% accuracy. In Walking State, the application records data for 10 seconds while walking with the device. The figure13 shows complete cycle or how the device is in walking state. The device is start to walk within 10 seconds. In horizontal line aeelerometer signal shows user is standing still first two cycles are omitted, next cycles used in analysis, in first peak device start to walking

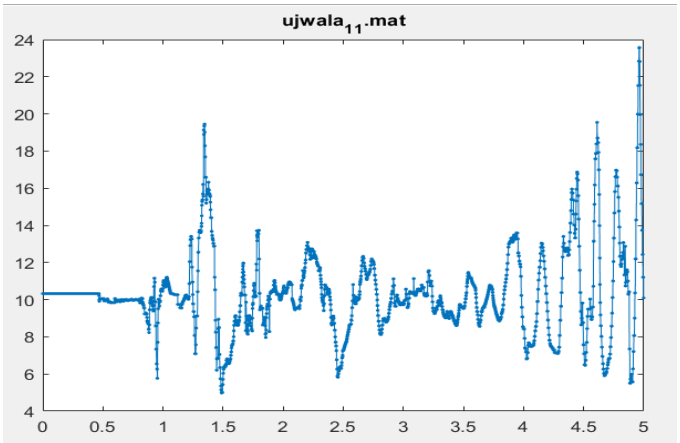

Figure7: Walking State Behavior.

IV. PROBLEM STATEMENT

Currently available mobile anti-theft mechanisms are

1. Locating lost phone using GPS-:"Find Lost Phone" is one of best-lost phone finder application that uses online GPS Tracking functionality to find your stolen/lost/misplaced phone.
2. Remotely wiping and locking the device-: It allows users to wipe their Android phone, as well as remotely lock or call the device.
3. Locking the SIM by informing service providers-: Once the user realizes his/her device has been stolen, he/she can use the GPS information to locate or remotely wipe and lock his/her device. However, these mechanisms work only after the discovery of the occurrence of the actual theft. We need to raise an alarm during an ongoing action of theft by analyze the pattern in waveforms from accelerometers provided within the mobile device. Long short-term memory deep learning network will be employed to accurately detect ongoing unauthorized movement of the device thereby making subsequent corrective actions feasible.

V. PROPOSED SYSTEM

This work argues that Long short term memory is very crucial for identify the motion patterns, which in turn benefits many real-world applications that need to It is intended to build a waveform of . A user may exhibit different behaviors like walking and running. Thus, when the training phase is complete, the database will include multiple behavior sets, each containing the step cycles that are extracted from the corresponding behavior.

V.I Framework overview-: In that flow diagram represents how to classify the data using LSTM and how it works

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

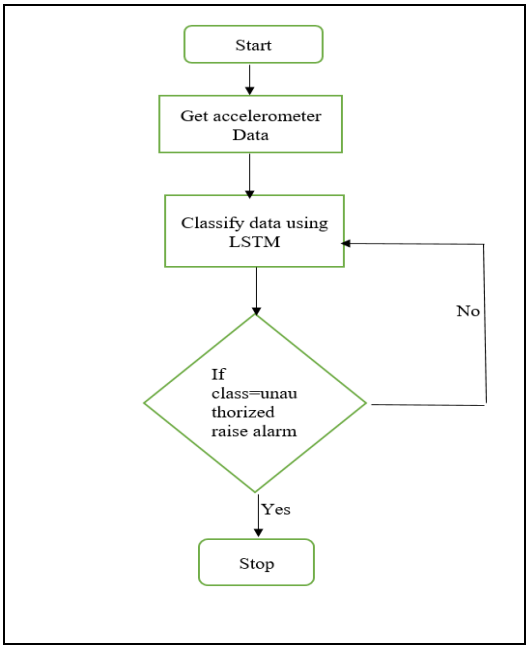

Figure 8: Flow diagram of proposed method.

V.II Working of Proposed System

The proposed system working is divided into two phases namely training and testing. As name suggests, Long short-term memory network is built and trained in first phase and it is used to predict and classify input in second phase. In the training phase, the dataset is used to train LSTM (long short-term memory). The trained network is stored so that it can be subsequently used to predict the test data. The dataset is created using the owner's mobile device and walking waveforms (patterns) from accelerometer are recorded with labels/classes with the owner and when people other than the owner are walking with the phone. The dataset created has 66464 records that are used to predict unauthorized walking motion pattern.

V.III Simplified LSTM Algorithm –In doing pattern synchronization for input data, we identify step cycle width and partition the data accordingly for later use in the database and matching components. In that algorithm for getting data,

```
//Algorithm for getting data
Step 1:  Start
Step 2:  For 10 seconds get accelerometer reading.
//Algorithm for creating dataset
Step 3: Start
Step 4: For each of 100 people.
Step 5: For each of 100 samples.
Step 6: Get data.
Step 7: Store data in a file in dataset folder.
//Algorithm for training
 Step 8: Start
 Step 9: create and configure LSTM network for training
 Step 10: Train the network on the dataset.
 Step 11: Store the trained network in a file.
//Algorithm for Testing
Step 12: Start
Step 13: For every 10 seconds.
Step 14: Get data
Step 15: Test data using the stored trained LSTM network.
Step 16: If class="Unauthorized" raise alarm.
Step 17: Stop
```

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

start walking for 10 seconds.

VI. RESULT ANALYSIS

The results of proposed knowledge-intensive approach are compared with existing state-of-art methods namely: Long short- term memory network. The performance of all the methods is evaluated via Accuracy, Precision, Recall and F1-score metrics.

VI.I Precision comparison-: The precision score is define as the actual correct prediction divided by total prediction made by model. As shown in figure blue color bar represent existing methods value is .0.96% and brown color bar is proposed method shows value is 0.98%. Hence, the proposed method has higher precision score compared to Statistical and K-S statistical analysis methods. $Precision = \frac{TP}{TP+FP}$

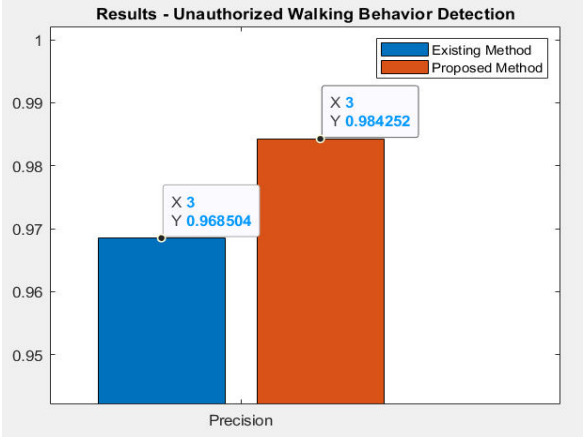

Figure 9: Precision score comparison.

VI.II Recall comparison-: The recall is calculated as the number of true positives divided by the total number of true positives and false negatives. .The figure shown the value of proposed is 0.97% represented in brown color bar and existing method shows value is 0.96% Proposed method has higher recall compared to Statistical and K-S statistical analysis method. $Recall = \frac{TP}{TP+FN}$

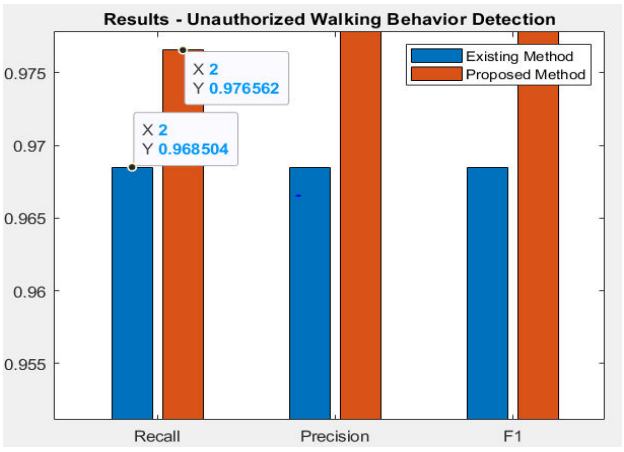

Figure10: Recall score comparison

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

VI.III F1-score comparison-:. F1-score measure single score balances the both precision& recall in one no. The figure shown the value of proposed is 0.98% represented in brown color bar and existing method shows value is 0.96% . Proposed method has higher F1 score compared to Statistical and K-S statistical analysis method. $F1_{score} = \frac{2*Recall*Precision}{Recall+Precision}$

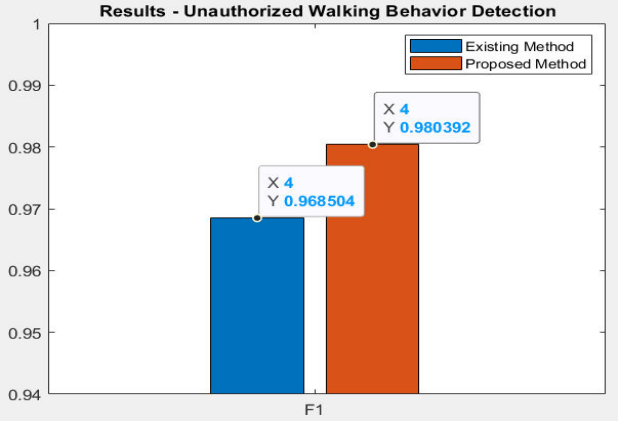

Figure11: F1-score comparison

VI.IV Accuracy comparison-: The accuracy is computes how many times model made a correct prediction across dataset. As shown in figure blue color bar represent existing methods value is .0.96% and brown color bar is proposed method shows value is 0.98%. Hence, the proposed method has higher precision score compared to Statistical and K-S statistical analysis method.$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$

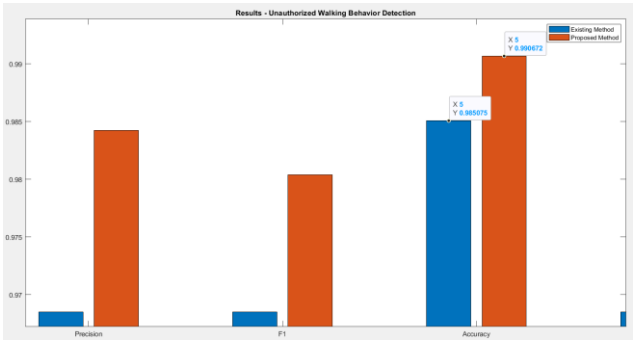

Figure12: Accuracy score comparison.

Table 2: Results comparison using Precision, Recall, F1-score and Accuracy

Method	Precision	Recall	F1 score	Accuracy
Statistical & K-S method	0.96%	0.96%	0.96%	0.98%
LSTM(long short term memory)	0.98%	0.97%	0.98%	0.99%

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212021 |

Table 2 depicts the Precision, Recall, F1-score and Accuracy score of all the methods in comparison. Results show LSTM (long short-term memory) is best among all. Proposed method has Precision almost similar as Statistical and K-S statistical analysis however, the Recall is lowerF1-score is usually more useful than accuracy. Proposed method is compares step cycles, the database size is reduced from “authorized”15500 step cycles to “notautorized”50344 cycles, while 99.1% detection rate is promised. Hence needs more improvement to compete with state-of-art methods.

VII. CONCLUSION

Accelerometer signals can be classified using long short -term memory classifier to detect unauthorized motion of a mobile device thereby making its theft detection feasible in real time. This could in turn make immediate corrective action possible like ringing or raising an alarm and catching of the thief in person red handed. Unlike existing methods that do not attempt to detect theft immediately giving a window of opportunity to the thief to escape thereby depriving the owner of his device causing him great agony along with risk to his data and misuse of the device; the proposed method alerts the owner and gives him/her ample opportunity to take corrective action. Comparison with existing methods like Statistical & K-S statistical analysis clearly illustrate the merit of the proposed approach.

REFERENCES

[1] J. Mantyjarvi, E. Vildjiounaite, H. J. Ailisto, M. Lindholm and S. Makela, "Identifying people from gait pattern with accelerometers", *Proc. SPIE 5779 Biometric Technol. Human Identification II.*, pp. 7-14, 2005.
[2] A. Annadhorai, E. Guenterberg, J. Barnes, K. Haraga and R. Jafari, "Human identification by gait analysis", *Proc. 2rd Int. Workshop Syst. Netw. Support Health Care Assisted Living Environments*, pp. 11:1-11:3, 2008.
[3] S. Argyropoulos, D. Tzovaras, D. Ioannidis and M. G. Strintzis, "A channel coding approach for human authentication from gait sequences", *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 428-440, Sep. 2009.
[4] M. O. Derawi, C. Nickel, P. Bours and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition", *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal* Process. pp. 306-311, Oct. 2010.
[5] G. Bajrami, M. O. Derawi and P. Bours, "Towards an automatic gait recognition system using activity recognition (wearable based)", *Proc. 3rd Int. Workshop on Security Commun. Netw.*, pp. 23-30, 2011.
[6] Y. Gao, C. Zhou and D. Shang, "A smart phone anti-theft solution based on locking card of mobile phone", Proc. Int. Conf. Comput. Inf. Sci., pp. 971-974, 2011.
[7] J. R. Usherwood, A. J. Channon, J. P. Myatt, J. W. Rankin and T. Y. Hubel, "The human foot and heel–sole–toe walking strategy: A mechanism enabling an inverted pendular gait with low isometric muscle force?", J. Roy. Society Interface, vol. 9, pp. 2396-2402, 2012.
[8] L. Li, X. Zhao and G. Xue, "Unobservable re-authentication for smartphones", *Proc. 20th Annu*. Netw. Distrib. Syst. Security Symp. pp. 1-16, 2013.
[9] Y. Ren, Y. Chen, M. C. Chuah and J. Yang, "Smartphone based user verification leveraging gait recognition for mobile healthcare systems", *Proc. IEEE Int. Conf. Sens. Commun. Netw.* pp. 149-157, Jun. 2013.
[10] T. Saha, H. Lu, J. Huang and L. Nachman, "Unobtrusive gait verification for mobile phones", *Proc. ACM Int. Symp. Wearable Comput.* pp. 91-98, 2014.
[11] T. Y. Hubel and J. R. Usherwood, "Children and adults minimise activated muscle volume by selecting gait parameters that balance gross mechanical power and work demands", J. Exp. Biol., vol. 218, no. 18, pp. 2830-2839, 2015.
[12] P. Fernandez-Lopez, J. Liu-Jimenez, C. Sanchez-Redondo and R. Sanchez-Reillo, "Gait recognition using smartphone", *Proc. IEEE Int. Carnahan Conf. Security Technol.*, pp. 1-7, Oct. 2016.
[13] M. Muaaz and R. Mayrhofer, "Smartphone-based gait recognition: From authentication to imitation", *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3209-3221, Nov. 2017.
[14] Dakun Shen, Ian Markwood, Dan Shen, Yao Liu University of South Florida, Tampa, FL Virtual Safe: Unauthorized Walking Behavior Detection for Mobile Device IEEE acess, 2018.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details