CYBER SECURITY CAMP II

USER ACTION AS AUTHENTICATION MECHANISM TO IMPROVE SMARTPHONE SECURITY

PRESENTED BY,

ARUL PRAKASH SAMATHUVAMANI
UNDER GRADUATE
DEPT. OF ELECTRONICS ENGG.
MADRAS INSTITUTE OF TECHNOLOGY
ARUL2810@GMAIL.COM

SHORT INTRO ABOUT SELF

SHORT INTRODUCTION

Currently Undergoing Under Graduate in Electronics And Communication

at Madras Institute Of Technology

I want my career to be meaningful, having impact in people's lives. Making their lives much more easier, accessible and much more simpler and secure.

Interested fields of work include

- Embedded Systems
- Machine Learning
- Image Processing
- Parallel and Distributed Processing

ABOUT INSTITUTION

Madras Institute Of Technology is public university located at Chennai.

It was founded in the year 1949 by visionary C.Rajam.

It is one of the four autonomous University Departments of Anna University

MIT has 8 departments with about 3000 UG and 300 PG students

It’s one of the biggest technical institutes in the country.

Former Indian President APJ.Abdul Kalam being an alumnus is a pride

for the institution.

NOW LET'S GET INTO BUSINESS

SMART PHONES HAVE BECOME AN INTEGRAL COMPONENT OF OUR EVERY DAY LIFE.

SMART PHONES – DAILY LIVES

- Smartphones are used to perform day to day tasks including banking.
- Our entire social and internet life is at our smartphones.
- Variety of security (Primary) protection measures to prevent someone from using our smartphones.

NONE OF THE SECURITY SYSTEM IS

“TRULY SECURE”

NEED FOR SECONDARY AUTHENTICATION MECHANISM

- This improves the need for an alternate authentication mechanism, a secondary authentication mechanism to improve smartphone security.
- The goal of this research is to develop a secondary authentication mechanism that is “continuous and implicit”

INTRODUCTION

- Use sensory data from various sensors that is available in the smartphones.
- Accelerometer - Axis based motion
- Magnetometer - Measure strength and direction of Magnetic field.
- Data closely relate to user’s behaviour, living environment and habits.

THE DATA FROM THE SENSORS IS USED TO RELATE HOW THE USER USES HIS MOBILE PHONE.

VARIOUS SENSORS IN SMARTPHONES

- ACCELEROMETER - Measure acceleration force in m/s2
- ORIENTATION - Measure degree of rotation in all three physical axis.
- MAGNETOMETER - Measure the ambient geomagnetic field.
- GYROSCOPE - Measure the device’s rate of rotation.
- PROXIMITY - Measure the proximity of the object in cms.
- GPS - Real time positioning
- MICROPHONE,LIGHT,CAMERA,TEMPERATURE etc.

FACTORS IN SELECTING THE SENSORS

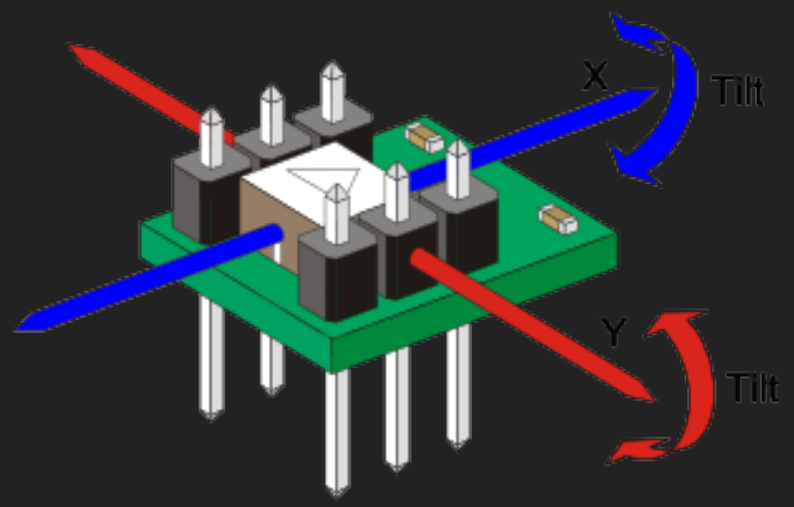
- Increase in the use of multiple sensors increases the accuracy.
- **AVAILABILITY OF SENSORS IN VARIETY OF DEVICES.**
- **eg.** Ambient light sensors are now omitted in variety of budget devices.
- Gyroscope is another sensor which is omitted in some budget devices.
- **POWER CONSUMPTION OF THE SENSORS.**

MOTION SENSING

- ACCELEROMETER
- ORIETATION SENSOR
- MAGNETOMETERS

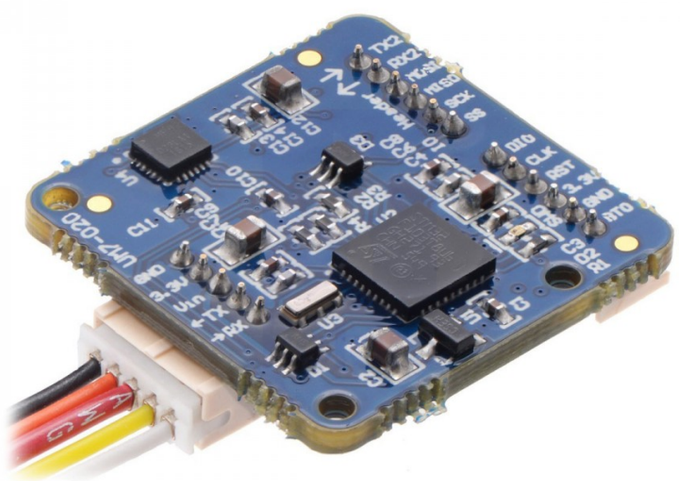
ACCELEROMETER

- Measures proper acceleration.
- At any point in space time the equivalence principle guarantees the existence of local inertial frame and the accelerometer measures the acceleration relative to that frame.
- Simple, stating it’s used to measure the coarse grained motion of the user.



ORIENTATION SENSOR

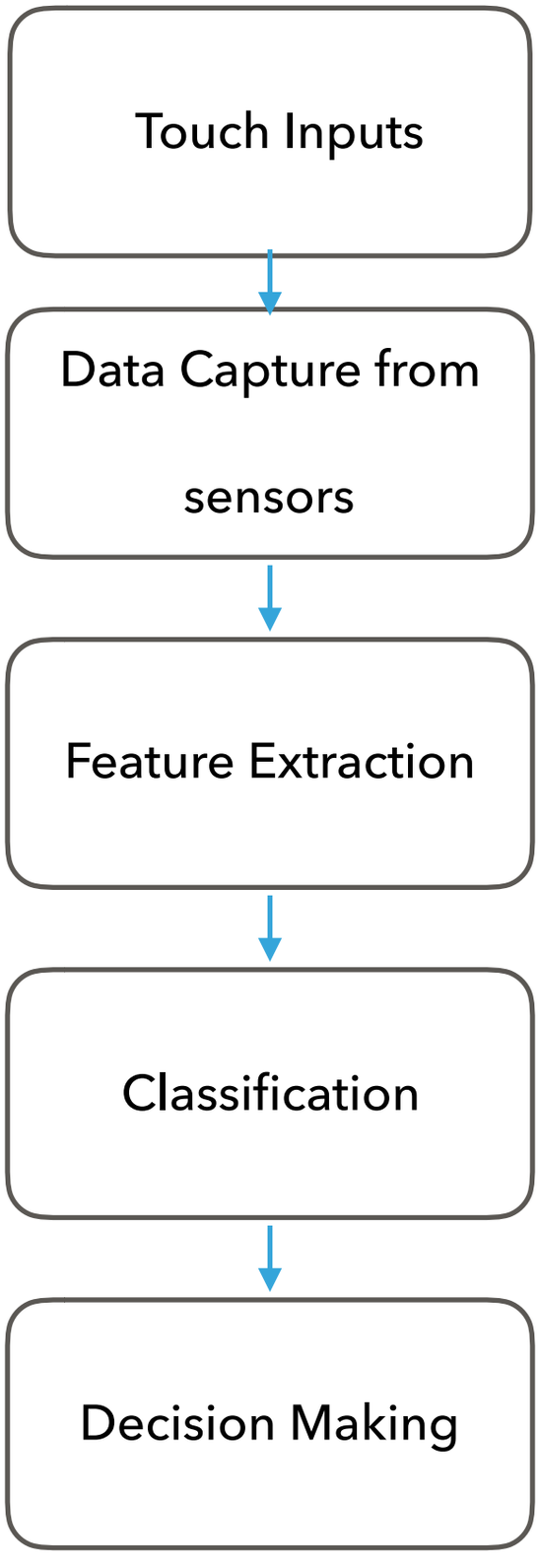
- Gives us the fine grained motion information
- Gives us the information of about how user holds the smartphone in their hands.



MAGNETOMETER

- Used to measure magnetism
- Measures magnetic flux density.
- Measures ambient geo-magnetic field for all three physical axis.

Basic Architecture of Authentication System.



COLLECTION OF DATA

- Collected in Two Ways.
- The data about way the user handles the phone is collected when the user first authenticates into the device.
- This is called Static Authentication Mechanism.
- Data is collected continuously when the touch inputs are given into the system.
- This is called Continuous Authentication Mechanism.

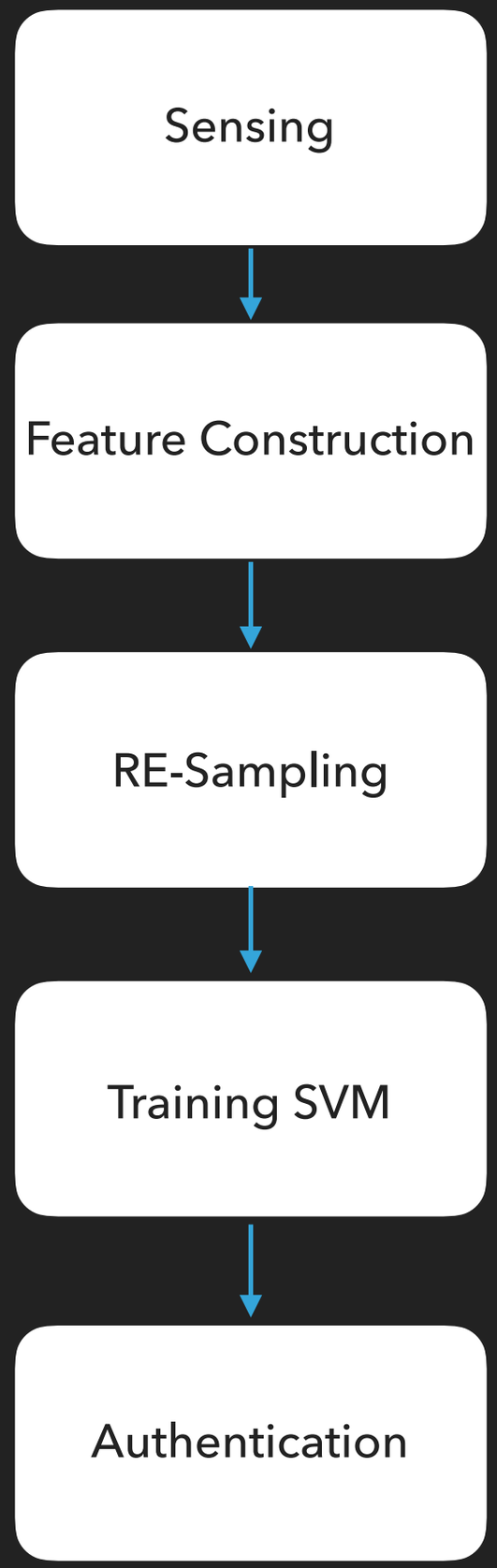
SENSOR BEHAVIOUR FEATURES

- Recorded information can be hardly used to classify the user.
- Behaviour features are extracted from these sequences.
- Various statistical parameters such as mean, variance and range is calculated from these stream of data.

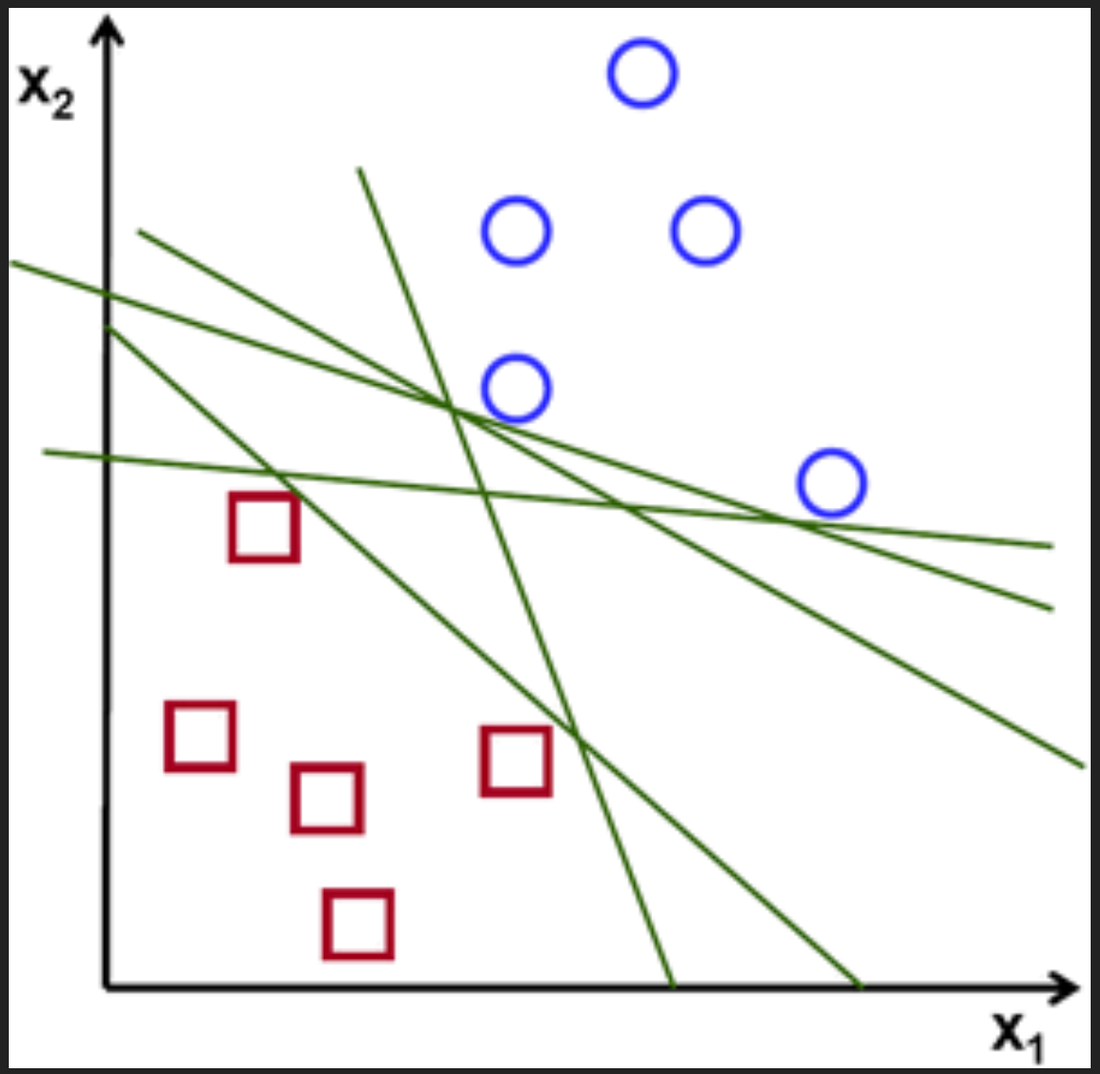
USAGE PATTERN

- Finding good features is essential for understanding the correlation between the collected data and identity information.
- Important for learning method in user discrimination.
- Information from variety of sensors is coupled with application under usage and touch input response.
- Descriptive characteristics from variety of sensors is used to identify the legitimate user.

Data Actions



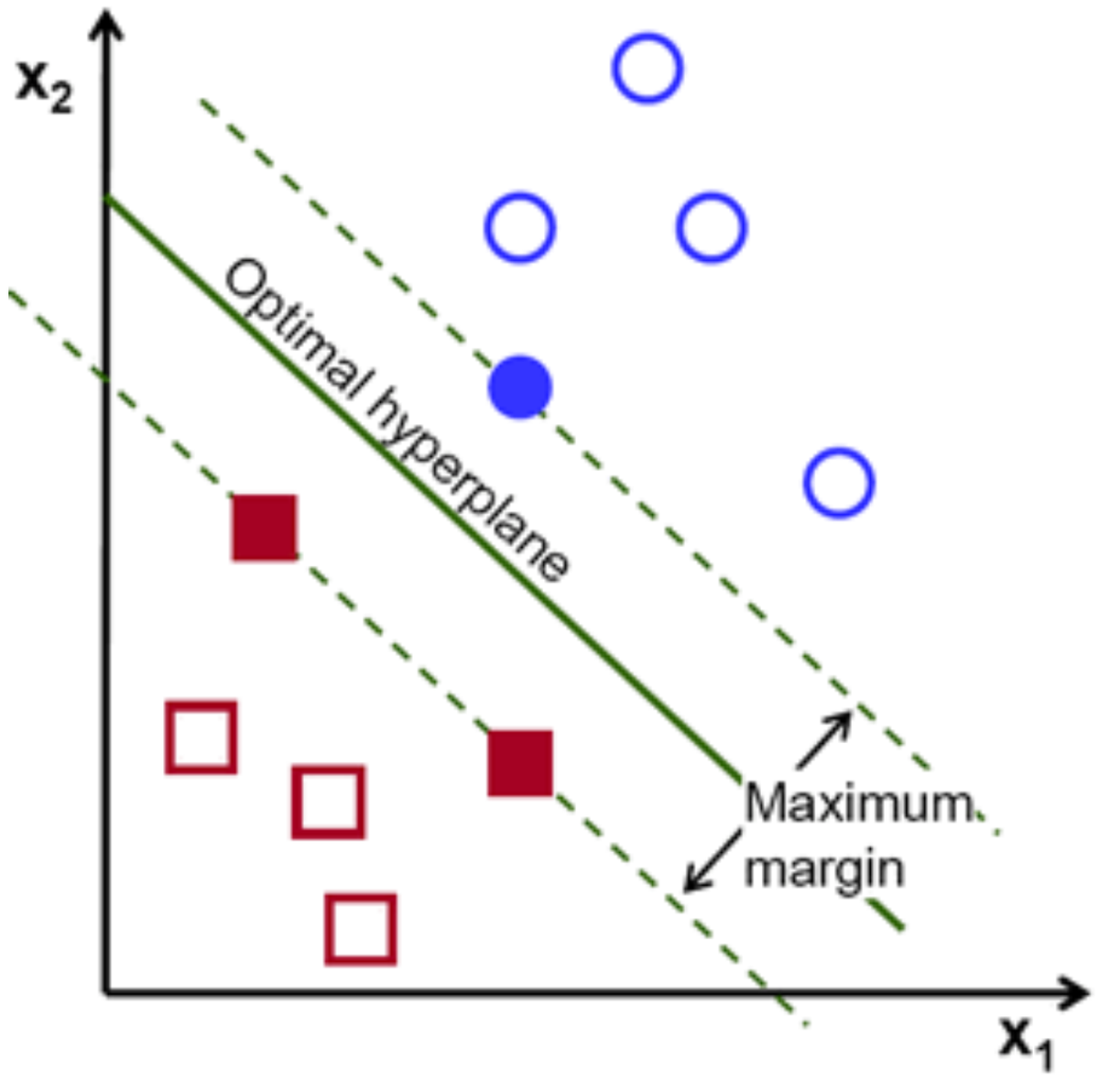
ONE CLASS SUPPORT VECTOR MACHINE



ONE CLASS SUPPORT VECTOR MACHINE

- Used in regression analysis and classification.
- Suppose there are two data classes, the goal is to classify the new data in any one of the two classes.
- A hyper plane separates the data into two classes.
- Hyper plane is chosen such that the distance between the two points on the either class is maximum.

ONE CLASS SUPPORT VECTOR MACHINE



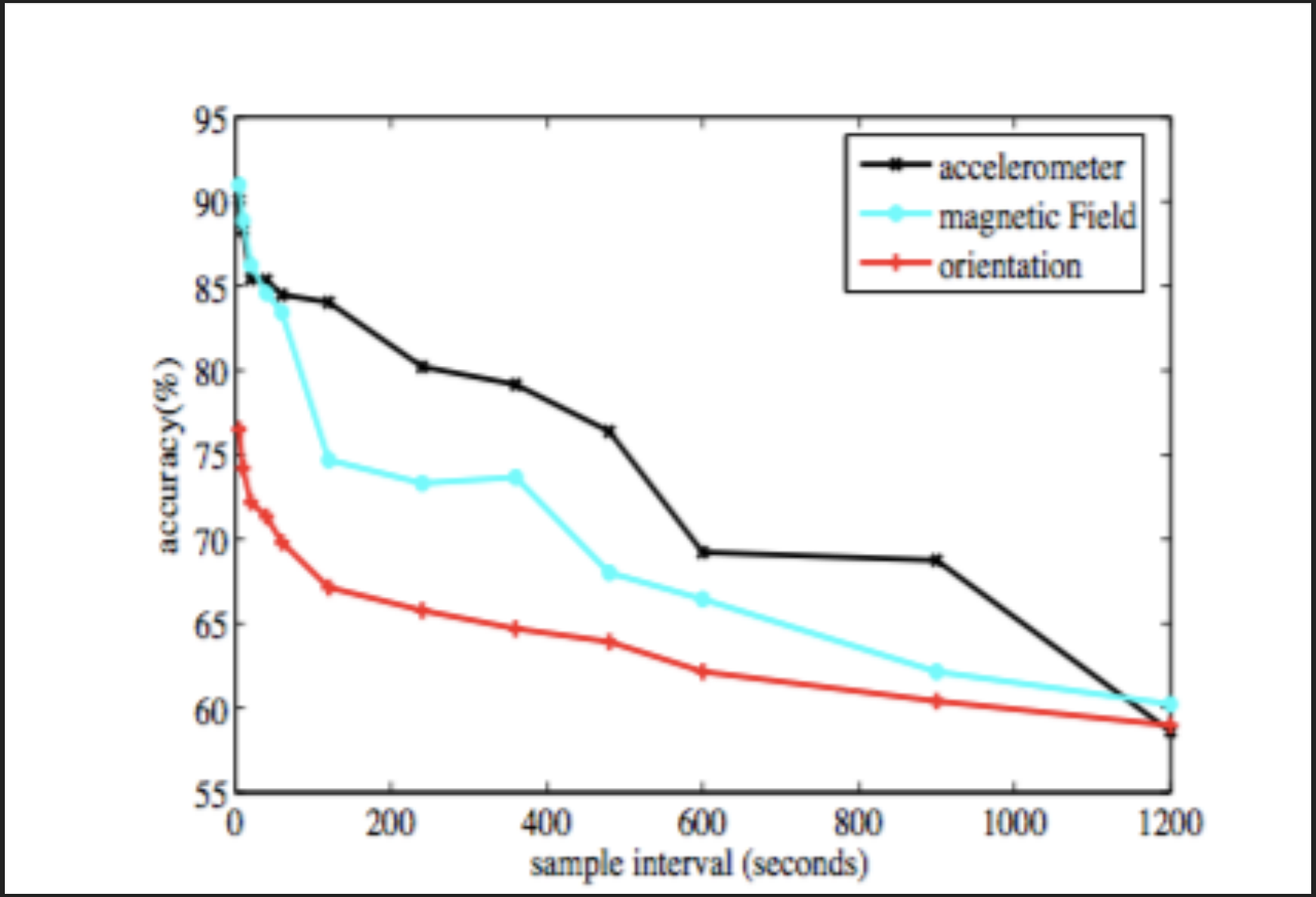
The training data is represented as S=P{(xi , yi)∈ XxY : i=1,2,....n} for n data-label pairs.

For binary classification , the data space is X-Rd and the label set is Y={-1,+1}. The predictor w is X→Y. The objective function is J(w,S).

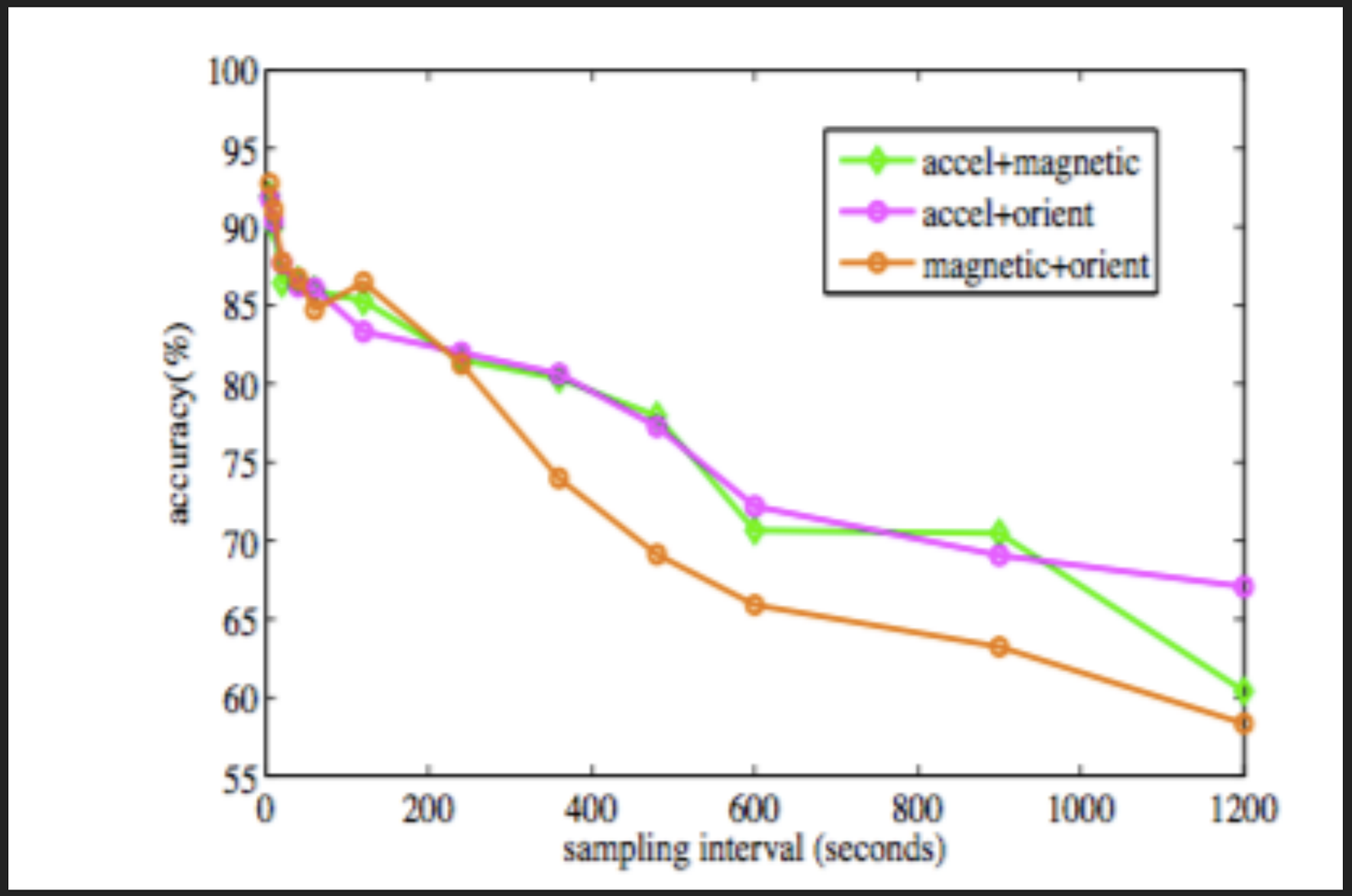
In our classification, we label all the user's data as positive and all other data as negative.

After building the Authentication for normal behaviour, we use this classification model to verify if the current input is normal.

EXPERIMENTAL RESULTS

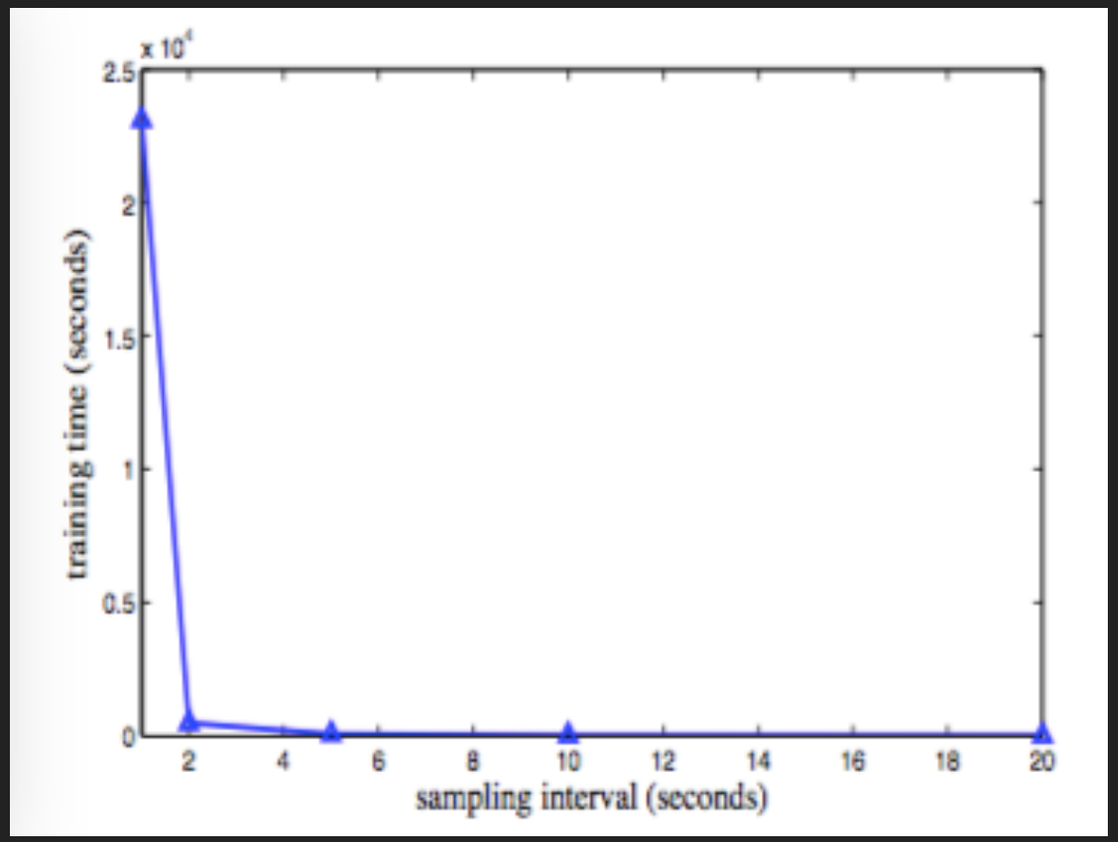


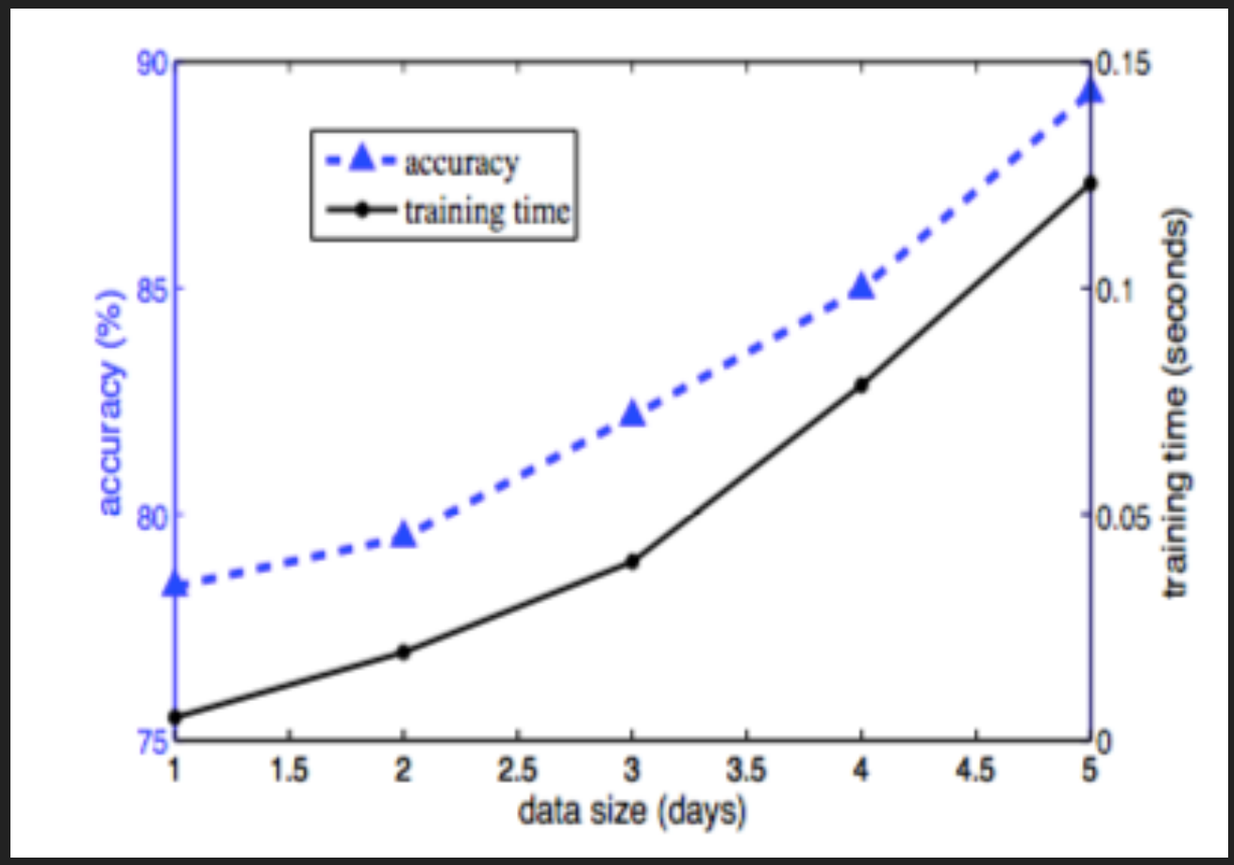
EXPERIMENTAL RESULTS



HIGHLIGHTING FEATURES

- Accuracy increases with faster sampling rate.
- Combination of sensors is better in accuracy when compared to single sensor authentication mechanism.
- Combination of variety of sensors affect the accuracy
- Therefore choosing the right combination of sensors is very important.


x 10^4
2.5
2
1.5
1
0.5
0
training time (seconds)
2
4
6
8
10
12
14
16
18
20
sampling interval (seconds)


90
85
80
75
accuracy (%)
0.15
0.1
0.05
0
training time (seconds)
accuracy
training time
1
1.5
2
2.5
3
3.5
4
4.5
5
data size (days)

CONCLUSION

- We use combination of sensors to obtain behavioural characteristics of the user.
- SVM classification technique is used to classify the user.
- Results from the tests indicate that the combination of sensors is important.
- Data from orientation sensor is not as important as data from accelerometer or magnetometer.
- Utilizing sensors to do implicit user authentication is very interesting and promising.

ACKNOWLEDGEMENTS

- I am grateful to various faculties in Madras Institute of Technology under the Department of Electronics Engineering who were very supportive throughout the entire research period.

REFERENCES

W.Lee and B.Lee "Multi Sensor Authentication to Improve Smart Phone Security" on Proc. *Information Security and Privacy*, February 2015

T. Feng, Z. Liu, K. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in Proc. IEEE Conference on Technologies for Homeland Security , 2012, pp. 451-456.

J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," in Proc. IEEE Symposia on Security and Privacy, 2012, pp. 538-552

A. J. Aviv, K. Gibson, et al., "Smudge attacks on smartphone touch screens," in Proc. the 4th USENIX conference on Offensive technologies, Washington, DC, 2010, pp. 1-7.

H. Lu, J. Yang, Z. Liu, N. Lane, T. Choudhury, and A. Campbell, "The Jigsaw continuous sensing engine for mobile phone applications," in Proc. ACM Conference on Embedded Networked Sensor Systems, 2010, pp. 71-84.

M. Antal, Z. Bokor, and L. Szabó, "Information revealed from scrolling interactions on mobile devices," Pattern Recognition Letters, 2015, vol. 56, pp. 7–13.

Vapnik, V. N. and Vapnik, V. (1998). Statistical learning theory, volume 2. Wiley New York.

Chang, C.-C., and Lin, C.-J. (2011). LIBSVM: A library for support vector machines. ACM Transactions on Intelligent Systems and Technology, 2:27:1–27:27.

Kayacık, H. G., Just, M., Baillie, L., Aspinall, D., and Mi- called, N. (2014). Data driven authentication: On the effectiveness of userbehaviour modelling with mobile device sensors. Mobile Security Technologies.

N. Zheng, K. Bai, H. Huang, and H. Wang, "You are how you touch: User verification on smartphones via tapping behaviors," in *Proc. IEEE Int. Conf. Netw. Protocols*, Oct. 2014, pp. 221–232

S.M. Kolly, R. Wattenhofer, R., and S. Welten, "A personal touch: Recognizing users based on touch screen behavior," in *Proc. Int. Work.* Sensing Applications on Mobile Phones, 2012.

Balagani, "HMOG: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, 11(5), pp. 877-892, 2016.

H. Xu, Y. Zhou, and M. R. Lyu, "Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones," in *Proc. Symp. Usable Privacy and Security*, 2014, pp. 187-198.

M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Trans. Inf. Foren. Sec.*, vol. 8, no. 1, pp. 136-148, 2013.

S. Bengio and J. Mariethoz, "A statistical significance test for person authentication," in *Proc. Speaker and Language Recognition Workshop*, 2004, pp. 237–244.

THANK YOU.