Real-Time Tracking and Alert System for Laptop using IoT for Anti-theft Purposes

Dr. N.R. Wankhade[1], Manasvi Ghodke[2], Akash Rokade[3], Aachal Vishwakarma[4], Kanchan Rane[5]

[1] Professor, Department of Computer Engineering, Late G. N. Sapkal College of Engineering, Nashik, Maharashtra, India
[2,3,4,5] Students, Department of Computer Engineering, Late G. N. Sapkal College of Engineering, Nashik, Maharashtra, India

ABSTRACT

Abstract - The methods for tracking a stolen laptop using GPS, GSM, Motion Sensors, and Cloud Services is described in this proposed work. Unlike previous laptop tracking solutions on the market, the methodology described in the study tracks the laptop even when it is turned off or not connected to the internet. With IoT, the owner will be able to follow his or her stolen laptop the instant it makes a slight movement and will be able to activate an alarm that will be incorporated into the laptop. The alarm will emit a noise that may be heard up to 10 meters away, making the thief reconsider carrying the laptop with him. Meanwhile, the owner will be able to track the whereabouts of his or her stolen laptop using a mobile application put on his or her phone, which will communicate with the laptop's GPS and GSM modules via the cloud.

Keywords: - *GSM, GPS, Microcontroller, IoT, Anti-theft, Cloud computing.*

1. INTRODUCTION

Taking India as an example, with a population of 1.3 billion people, around 10 million people own a laptop. It's nearly impossible to envision someone living without a computer or laptop in today's environment. They've evolved into electronic devices that people of all ages use practically every day, and they're now required in almost all business transactions. Every laptop contains crucial data and information that is very valuable to its owner, and its loss or theft can result in substantial financial loss. According to the National Crime Records Bureau, over 1.3 lac laptops were stolen in 2016, and unexpectedly, the number is increasing. The recovery rate was as low as 8 percent. It is the responsibility of police officers or the crime section to address such situations, but they are always preoccupied with more serious crimes. The officials' task of tracking the laptop is difficult and time-consuming. As a result, not all computers are tracked. If the laptop belongs to someone of importance or includes critical or crucial data of national interest or national security, the crime department will try to hunt it down as necessary. As a result, the common guy is the one who suffers in the end.

Laptops and all IT systems are extremely difficult to safeguard. Laptops are mobile and easily concealable, there is a large market for selling the hardware, and several of them can be found in a single building. With laptops' improved data storage capacities, the loss of even a single laptop might result in significant expenses to the enterprise. As a result, even if a business has a huge number of computers, losing even one laptop may be unacceptable. Laptop theft is especially dangerous in open-access organizations. Hospitals and universities, for example, admit hundreds of individuals every day, indicating that 46 percent of data breaches occur in institutions open to the public: education, health care, and government. In these conditions, laptops with critical medical or academic data become extremely insecure. The issue that security professionals face is how to protect laptops in such open environments.

2. LITERATURE SURVEY

Taking India as an example, with a population of 1.3 billion people, around 10 million people own a laptop. It's nearly impossible to envision someone living without a computer or laptop in today's environment. They've evolved into electronic devices that people of all ages use practically every day, and they're now required in almost all business transactions. Every laptop contains crucial data and information that is very valuable to its owner, and its loss or theft can result in substantial financial loss. According to the National Crime Records Bureau, over 1.3 lacs of laptops were stolen in 2016, and unexpectedly, the number is increasing. The recovery rate was as low as 8 percent. It is the responsibility of police officers or the crime section to address such situations, but they are always preoccupied with more serious crimes. The officials' task of tracking the laptop is difficult and time-consuming. As a result, not all computers are tracked. If the laptop belongs to someone of importance or includes critical or crucial data of national interest or national security, the crime department will try to hunt it down as necessary. As a result, the common guy is the one who suffers in the end.

All IT systems and laptops are particularly hard to protect. Laptops are mobile and easily concealable, there is a big market to sell the hardware and there can be many of them in a single building. With the increased data storage capabilities of laptops, the loss of even a single laptop can induce dramatic costs to the organization. Thus, although there can be a large number of laptops in an organization, losing even a single laptop may not be acceptable. Organizations open to the public are particularly at risk from laptop theft. Hospitals and universities, for example, accept hundreds of people that can wander on the premises every day pointing out that 46 percent of data breaches occur in institutions open to the public: education, health care, and the government. Laptops containing sensitive medical or academic data become highly vulnerable in these environments. The problem security professionals face is how to protect laptops in such open organizations.

In recent decades, urban populations have continuously increased by a rate that is greater than half a billion inhabitants per decennial on a worldwide basis [6]. This continuously growing urbanism has boosted the growth of various problems, which deteriorate the quality of living in civilian settlements. The collection of data is a necessary procedure in the context of smart cities to gather information regarding various parameters that are related to all aspects of human activity. Additionally, the data collected have to be processed and transmitted over various distances. Modern technological advances have enabled the inexpensive massive fabrication of wireless sensor nodes that, despite their fairly small dimensions, have remarkable sensing, processing, and communication capabilities. This is the reason why wireless sensor networks (WSNs) and IoT, which have a continuously growing range of applications [11–13], are generally considered to be technologies that, when combined with the application of appropriate algorithms, are ideally suited to be deployed in the framework of smart cities [14–16].

3. SYSTEM ARCHITECTURE

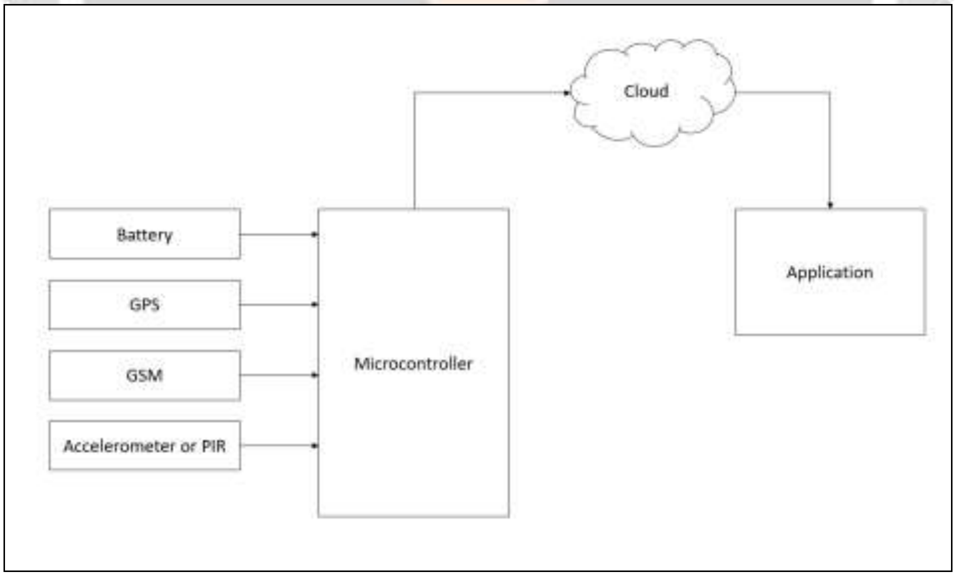


Figure 1 - System Architecture

Unlike previous laptop tracking solutions on the market, the methodology described in the study tracks the laptop even when it is turned off or not connected to the internet. With IoT, the owner will be able to follow his or her stolen laptop the instant it makes a slight movement and will be able to activate an alarm that will be incorporated into the laptop. The alarm will emit a noise that may be heard up to 10 meters away, making the thief reconsider carrying the laptop with him. Meanwhile, the owner will be able to track the whereabouts of his or her stolen laptop using a mobile application put on his or her phone, which will communicate with the laptop's GPS and GSM modules via the cloud.

4. RESULTS

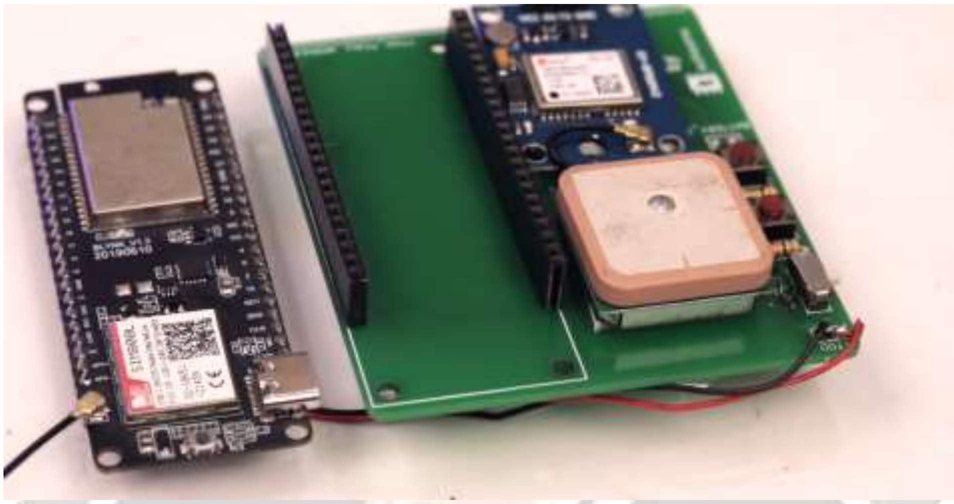
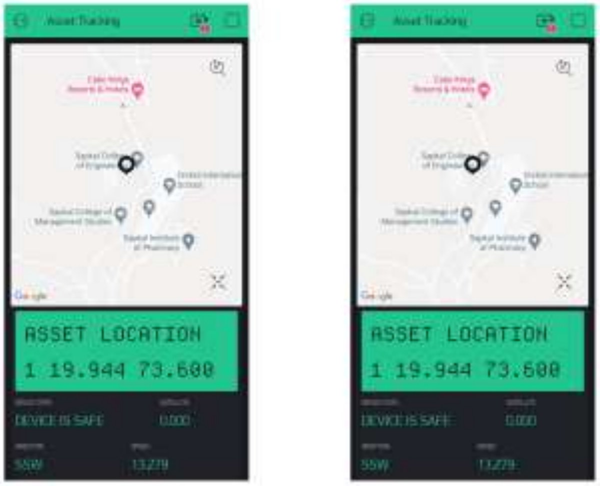


Figure 2 - Hardware setup



Asset Tracking

ASSET LOCATION
1 19.944 73.600

DEVICE IS SAFE 0.000

SSW 13.279

Asset Tracking

ASSET LOCATION
1 19.944 73.600

DEVICE IS SAFE 0.000

SSW 13.279

Figure 3 - Application

5. CONCLUSIONS

Laptops are always an important asset for its owner. It contains vital data and information about its owner. It becomes a huge problem for the owner if his or her laptop gets stolen. Laptop tracking techniques present in the current market are inefficient and not worth the money since they only can track the laptop if it is switched on and is connected to the internet. The methodology mentioned in the paper is an efficient way to track the laptop since it notifies the owner the moment anyone fiddles with the laptop. Also, the laptop will be continuously tracked even if it is switched off.

6. REFERENCES

[1] E. Edwan, F. Shaheen, A. Shaheen, and A. Sarsour, "Automated NFC-Based System for Management and Tracking of Assets in Sharing Economy," 2019 International Conference on Promising Electronic Technologies (ICPET), 2019, pp. 45-49, DOI: 10.1109/ICPET.2019.00016.

[2] K. Shruthi, P. Ramaprasad, R. Ray, M. A. Naik, and S. Pansari, "Design of an anti-theft vehicle tracking system with a smartphone application," 2015 International Conference on Information Processing (ICIP), 2015, pp. 755-760, DOI: 10.1109/INFOP.2015.7489483.

[3] A. P. Saikia Thengal, N. Rastogi, A. Medhi, R. Srivastava, and K. Datta, "Parameter sensing and object tracking using global positioning system," 2016 Sixth International Symposium on Embedded Computing and System Design (ISED), 2016, pp. 289-293, DOI: 10.1109/ISED.2016.7977099.

[4] M. Imran, A. Uddin, F. Rafath, M. Osman, A. Sultana, and K. Srikanth, "Real-Time Application of Advanced Exam Paper Leakage Detection and Alert System with Theft Protection," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), 2020, pp. 421-427, DOI: 10.1109/ICOEI48184.2020.9142950.

[5] W. Raad, M. -V. Bueno-Delgado, M. Deriche, and W. Suliman, "An IoT Based Inventory System for High-Value Laboratory Equipment," 2019 Sixth International Conference on Internet of Things: Systems, Management, and Security (IOTSMS), 2019, pp. 314-319, DOI: 10.1109/IOTSMS48152.2019.8939259.

[6] H. Talat, T. Nomani, M. Mohsin, and S. Sattar, "A Survey on Location Privacy Techniques Deployed in Vehicular Networks," 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 2019, pp. 604-613, DOI: 10.1109/IBCAST.2019.8667248.

[7] R. Kakadiya, R. Lemos, S. Mangalam, M. Pillai, and S. Nikam, "AI-Based Automatic Robbery/Theft Detection using Smart Surveillance in Banks," 2019 3rd International Conference on Electronics, Communication, and Aerospace Technology (ICECA), 2019, pp. 201-204, DOI: 10.1109/ICECA.2019.8822186.

[8] P. N. Saranu, G. Abirami, S. Sivakumar, K. M. Ramesh, U. Arul, and J. Seetha, "Theft Detection System using PIR Sensor," 2018 4th International Conference on Electrical Energy Systems (ICEES), 2018, pp. 656-660, DOI: 10.1109/ICEES.2018.8443215.

[9] P. Choudhary and J. N. Bera, "SMS Based Load Flow Monitoring and Analysis for Theft Location Detection in Rural Distribution Systems," 2020 IEEE Calcutta Conference (FALCON), 2020, pp. 386-390, DOI: 10.1109/CALCON49167.2020.9106499.

[10] S. Venkateswarlu, D. T. Ankireddy, N. K. Kumar, R. Meram, T. M. Prakash and J. S. Naik, "Controller Design For Detection of Various Power Thefts," 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), 2021, pp. 1-5, DOI: 10.1109/i-PACT52855.2021.9696752.

[11] C. Richardson, N. Race, and P. Smith, "A privacy-preserving approach to energy theft detection in smart grids," 2016 IEEE International Smart Cities Conference (ISC2), 2016, pp. 1-4, DOI: 10.1109/ISC2.2016.7580882.

[12] A. V. Christopher, G. Swaminathan, M. Subramanian, and P. Thangaraj, "Distribution line monitoring system for the detection of power theft using power line communication," 2014 IEEE Conference on Energy Conversion (CANCON), 2014, pp. 55-60, DOI: 10.1109/CENCON.2014.6967476.

[13] M. J. Lance, S. P. D. Chowdhury, and T. O. Olwal, "Detection of Underground Power Cable Theft: Strategies and Methods," 2018 IEEE PES/IAS PowerAfrica, 2018, pp. 1-9, DOI: 10.1109/PowerAfrica.2018.8521125.

[14] Shivashankar, Ravigatti, P Rajendra Prasad, S Santosh Kumar and K N Sunil Kumar “Improvement of speed in data collection rate in tree based wireless sensor network”, Proceedings of IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), ISBN: 978-1-5090-0774-5, 10.1109/RTEICT.2016.7807918, pp. 720 – 723, 2016.