# An efficient child activity tracker by using context-based learning techniques.

Anupama k [#], Deepti G. [*], Nageena Shetty [*], Saritha [*]

[#] Assistant Professor, * UG Students
Department of Computer Science and Engineering.
Moodlakatte Institute of Technology, Kundapura - 576217.

**ABSTRACT**

***Children use different types of mobile devices without any constraints. According to National Incidence Studies of Missing, Abducted, Run away, and Thrown away Children (NISMART), in 1999, an estimated 204,500 children were involuntarily missing from their care takers because they were lost, injured, or stranded; 68,100 of these children were reported to authorities. In today's information age, it is vital for kids to be tech savvy, but it's up to parents to find and maintain a balance. Since, today's most of the mobile phone users have an android phone, chances of children using it are more. This gives an opportunity to design an android application which is used to track the missing children. This tracking solution allows parents to monitor their child's cell phone. All calls, texts and multimedia messages can be seen and interrupted by the parents, who can also monitor where their children are and set up alerts if their children are going outside of approved geographical zones. The parent can also block calls or messages to specified numbers. Our aim is to develop an efficient and improved geographical asset tracking solution and conserve valuable mobile resources by dynamically adapting the tracking scheme by means of context-aware personalized route learning techniques. The main challenge is to balance privacy and flexibility with the ease of use. This application plays an intermediate role between user and the guardian. Thus, trying to avoid the consequences caused through the negligence and be a part in reducing the number of missing incidences in this information age.***

## 1. INTRODUCTION

On the digital century where technology reaches kids hands, guardians may worry about the effect of this very open world on their kid's development. They may worry about the detrimental effect of this technology on their educational, emotional and social developments. To help overcome some of these worries, guardians may need to have some controlling technology to check and track their children usage for the personal devices. As mobile devices are one of the most used technologies by children on our society, guardians will need to have some automated technologies to observe and supervise the time and quality of their children's usage for these mobiles. Monitoring and controlling methodologies and approaches have been developed as the technologies are started or developed. As human being, there are some concerns when using emerging technology. These concerns push developers to innovate ways to test, control, and manage new technologies. One of the most known approaches is based on the use of distributed architecture for the monitoring and controlling connected devices. This distributed design allows for central controlling component over the connected devices either using client server approach, or mobile data management approach which will be the focus on this survey to monitor mobile devices. This survey is the base to help building up the proposed project, which will research the different methods available for technology usage surveillance. The project will focus more on the parental control over children's tablet devices. Furthermore, the project will develop a controlling application for parental use on children's tablet devices. The proposed application may help guardians to not only control, but also evaluate the way their children handle and utilize the technologies available at their tablet devices. This survey is the base part of the project that includes the background for researching and developing the proposed application. The structure for this survey includes the background, the research challenges, applications, and overview of related work. The background reviews the security and

network methodologies related to the main focus, and explains the main terminologies used in the related work. Then the survey includes the main difficulties that would face researchers on this area. Despite these challenges, there are vital applications for the monitoring and controlling concepts for education and work environment, which will be covered under the application part of this survey. Then the survey includes deeper insight on some experiments, studies, and methods related to monitoring and controlling mobile devices.

## 2. LITERATURE SURVEY

Monitoring mobile devices has been a concern for not only individual users, but also for organizations, communities, and scientific researchers. The challenge of using monitoring applications is about how the collected data will be handled and the how to build a macroscopic pattern from the collected data. This part of the survey discussed the summary of the selected research papers related to monitoring mobile devices. The framework architecture proposed is built upon using mobile phone sensing and the cloud computing. The paper discussed the different challenges with gathering data techniques using mobile and unexpected environment (mobile context), as well as, the privacy issues on gathering personal information from a third-party application. There are three different scales mobile sensing considered beneficial on: individual, group, and community data gathering. The scalability feature of gathering individual behavior to learn from community patterns may help improve communities in social, healthy and environmental studies. The study also explained the two sensing paradigms: participatory sensing, which involves users who lunch sensors manually, and opportunistic sensing, where sensors automatically collect data. The main focus of the introduced work in is about understanding how personal data travels through selected third-party applications. The authors raised the issue about violating privacy barriers when applications access the personal information by only ask for user's permissions to access the data with no explanation of how the data will be used. The research proposed a monitoring platform based on Android mobile phone to track the data flow through 30 selected applications. After testing the proposed the platform, the research concluded that 20 apps miss used the users' private data and 15 apps used users' locations to support marketing services. The main challenges in monitoring the use of mobile apps include the shortage of smart phone used data as a resource constrained, as well as, the dynamic nature of data flow using mobile devices. This dynamicity causes another context-based challenge because data could be sent at any time and any place. Further, mobile apps allow for across sharing data and information among different apps, which increase the difficulty in monitor single flow between an app and the operating system. The proposed platform only tracks data flows but not control flows. Data flows are the explicit flowing of data through the apps. Control flows are the implicit flowing of data that require analytical analysis. Furthermore, the research focus in proposed a cloud service application to track and monitor android programs and performs static and dynamic analysis. The goal of using the Sandbox application is to maintain smart phones security by detecting any malicious patterns or malware. The static analysis works by scanning software before installation, while dynamic analysis works by installing software on an isolated environment than does the analysis process. The researchers in also discussed the challenging and issues related to security and smart phones control. There is a difference between securing mobile phones and smart phones. Mobile phones only work through the secure and closed network for calls and messages services, while smart phones are enabled to be connected the Internet. The security risk using mobile smart phones increases as these devices being able to use the Internet and host third party applications. Resolving the tension between security and flexibility is one issue in this regard, as well as, caring about privacy when different sensors share personal data with third party. Furthermore, the limitation on smart phones hardware makes it more challenging to run or install sufficient detection software to analyse security threats.

## 3. APLICATION DESCRIPTION

For the proposed system, there are four main cases.

1. Parents Registration
2. Restriction choices
3. Report diagram
4. Recovery password

**1. Parent Registration:**

i. Download the application Parents are not register before.

ii. Application shows the window that contains the registration fields (password – E-mail).

iii. The application checks if fields are filled correctly then shows the window that contains the parent's information, if not shows the error message.

iv. If the displayed information is correct parents press OK button, now they are registered, if not press Cancel button.

v. If OK button is pressed, the application shows the window that contains the Welcome message. If Cancel button is pressed, the application shows the window that contains the registration fields again.

vi. If parents press Exit button, application is terminated.

**2.Restriction Choices:**

i. Parents logs in to the application by password only.

ii. The application shows a welcome window, then shows main interface of the application, which contains choice for lock the device and all applications downloaded on the device.

iii. Parents select lock device choice.

iv. The application shows a window that contains choices of locked (lock at, lock from-to).

v. Parents select the wont choice and write hours to lock

vi. Parents press Save button

vii. The application shows the main interface of the application again

viii. If Parents set restriction for kids press Exit button to exit from application

**3. Report View:**

i. Parents log in to the application by password only

ii. The application shows a welcome window, then shows the main interface of the application, which contains a choice for reporting diagrams

iii. Parents select the choice

iv. The application shows a window that contains a diagram for applications used or not used and ranks application based on usage time

v. Parents press Back button

vi. The application shows the main interface of the application again.

vii. If Parents see the diagram press Exit button to exit from application

**4.Recovery Password:**

i. Parents forget the password

ii. The application asked parents to send the password to registered E-mail

iii. Parents press Ok button

iv. The application sends the password to the E-mail

v. If Parents get password, then they can log in as usual.

## FUTURE WORK

The future work that can be done to expand this project includes the development for a website, as well as, the implementation for the IOS platform. The website would be helpful to the app users to connect and manage their accounts through different platforms. For example, if one family uses different devices, the family guardian would use the website to control and manage several devices at same time. Furthermore, the expansion to different platform, the IOS, is important to be developed in the future. Guardians would want to have such a great app regardless to the used platforms, IOS or Android.

## CONCLUSION

A special purpose programming language designed for managing data stored in a relational database management system. This project demonstrated a discussion on developing systems and approaches to control, manage, and monitor the use of different electronic devices. The project discussed some of research efforts related to monitoring mobile devices and some of the developed techniques. Accordingly, the project concluded some of the main research challenges when researching this area including the difficulty on maintain privacy and providing normal and clear data while using mobile devices. Furthermore, the project included the implementation of the monitoring system called Track Me application, which will help guardians to control and evaluate their kids use of mobile devices.

**REFERENCES**

[1] Lane, Nicholas D., et al. "A survey of mobile phone sensing." Communications Magazine, IEEE 48.9 (2010): 140-150.

[2] Enck, William, et al. "Taint Droid: an information-flow tracking system for Real time privacy monitoring on smart phones." ACM Transactions on Computer Systems (TOCS) 32.2 (2014): 5.

[3] Bläsing, Thomas, et al. "An android application sandbox system for suspicious software detection." Malicious and unwanted software (MALWARE), 2010 5th international conference on. IEEE, 2010.

[4] Rohr, Matthias, et al. "Kieker: Continuous monitoring and on demand visualization of Java software behaviour." (2008): 80-85.