Hardware based Anti-theft System for Smartphones

J. Caroline El Fiorenza, Dinesh Udayakumar, Chandrasekar Rajah, M. Karthikeyan

Abstract--- In the world of technology, smartphones and laptops play a major role and is actively used by millions of people around the world for the purpose of communication, entertainment and also as a tool for learning and updating our knowledge. Users store important information on their smartphones ranging from personal details, photos, videos and other confidential credentials such as banking information and even passwords. This possess a threat when the smartphone is stolen where this information can be misused for certain criminal activities and all our important information is at stake. The existing anti-theft systems are all software based where once stolen, these apps can be uninstalled by anyone and hence cannot be accessed by owner and all the confidential information is gone with it too. Therefore, the scope of this project is to propose a hardware based anti-theft system wherein a actual chip is embedded in to the smartphone which can be accessed anytime by the user to track the smartphone even after the phone is reset and also provide support for remotely erasing the data stored, hence data integrity is achieved and the data is not stolen. The chip can communicate with the GPS sensor in the mobile and will provide GPS location of the smartphone in real-time. The chip also has an dedicated storage where users can store important information and confidential data that can be secured and can access it anytime.

Keywords--- Anti-theft system, Cybersecurity, GPS, Information Security.

I. INTRODUCTION

As versatile innovation develops, representatives progressively need to utilize both association issued and by and by possessed cell phones to get to corporate endeavor administrations, information and assets to do business related exercises. Undertakings are experiencing strain to acknowledge the related security dangers intrinsic in the present cell phones due to, among different elements, saw cost reserve funds and representative want for more noteworthy comfort.

Numerous cell phones, especially those that are actually claimed, are not equipped for giving solid security confirmations to end clients and associations. Current cell phones do not have the equipment-based foundation of trust includes that are progressively incorporated with PCs and different sorts of hosts (e.g., Trusted Platform Modules, TPMs). Cell phones are additionally powerless against "jailbreaking" and "establishing," which give gadget proprietors more noteworthy adaptability and command over the gadgets, yet in addition sidestep essential security highlights which may present new vulnerabilities.

Associations may wish to check the honesty of a cell phone before conceding it access to the association's data. This confirmation gives affirmation that the association's data is appropriately ensured—for instance, the gadget's security isn't broken, the gadget is approved to get to the association's data, and privately put away data from the association will have its secrecy and uprightness ensured. This trustworthiness confirmation is viewed as essential for both association issued and by and by claimed cell phones; nonetheless, it is commonly less demanding to accomplish for association issued gadgets than by and by possessed gadgets. Current cell phone stages give restricted abilities to perform such honesty confirmation.

As adaptable advancement creates, agents dynamically need to use the two affiliations issued and really asserted mobile phones to get to corporate endeavour organizations, data and resources for work together related activities. Adventures are under pressure to recognize the related security risks intrinsic in the present phones due to, among various segments, saw cost save assets and agent need for increasingly unmistakable solace.

Various phones, particularly those that are eventually had, are not prepared for giving strong security affirmations to end customers and affiliations. Current mobile phones miss the mark on the hardware-based establishment of trust incorporates that are dynamically fused with workstations and diverse sorts of hosts (e.g., Trusted Platform Modules, TPMs). Mobile phones are in like manner unprotected against "jailbreaking" and "setting up," which outfit device owners with progressively unmistakable versatility and control over the contraptions, yet moreover avoid crucial security features which may exhibit new vulnerabilities.

Affiliations may wish to affirm the genuineness of a PDA before yielding it access to the affiliation's information. This affirmation gives confirmation that the affiliation's information is fittingly guaranteed—for example, the contraption's security isn't broken, the device is endorsed to get to the affiliation's information, and secretly secured information from the affiliation will have its order and decency verified. This decency check is seen as imperative for the two affiliations issued and really had mobile phones; regardless, it is generally less requesting to achieve for affiliation issued contraptions than before long guaranteed devices. Current wireless stages give obliged abilities to perform such decency check.

Revised Version Manuscript Received on 22 February, 2019

J. Caroline El Fiorenza, Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science & Technology, Chennai, India. (e-mail: caro.fiorenza@gmail.com)

Dinesh Udayakumar, Student, Department of Computer Science and Engineering, SRM Institute of Science & Technology, Chennai, India. (e-mail: dinesh.uday@outlook.com)

Chandrasekar Rajah, Student, Department of Computer Science and Engineering, SRM Institute of Science & Technology, Chennai, India. (e-mail: san341998@outlook.com)

M. Karthikeyan, Student, Department of Computer Science and Engineering, SRM Institute of Science & Technology, Chennai, India. (e-mail: karthikrider07.kr@gmail.com)

II. BACKGROUND/REALTED WORKS

At present, most cell phone hostile to robbery plots just give aloof insurance, which plans to lessen security spillage and data misfortune after cell phones being stolen. At the point when such crisis occurs, the injured individual sends control messages to the stolen telephone, so as to bolt and confine the telephone, reinforcement and erase information, remotely, which are nothing to do with diminishing the danger of telephone lost. Synchronica Plc built up a product, named Mobile Manager, to help Symbian cell phones. With Mobile Manager, organizations or specialist co-ops can promptly verify lost or stolen gadgets remotely, from Mobile Manager's online application. The gadget can be cleaned and bolted over-the-air, avoiding delicate corporate or individual information put away on the gadget from being gotten to by unapproved clients. Tencent Mobile Phone Manager, Lookout Mobile Security, Rising Phone Security Assistant and so on depend on SIM card discovery. When the SIM card is supplanted, the framework will consequently record the new SIM card number, and afterward the proprietor can use SMS to send backing up, erasing, and bolting directions remotely. Different applications, for example, 360 and Kingsoft Mobile Phone Guard, give SMS notice to SIM card substitution, telephone following, disturbing, and bolting. X. Yu et al. propose a remote cancellation instrument that enables the telephone proprietor to erase the private information remotely regardless of whether Wi-Fi is debilitated and the SIM card is unplugged. A. U. S. Khan et al. present a method to empower against burglary for android based cell phones by utilizing administrations like MMS (Multimedia Messaging Services) rather than SMS. L. Subramanian et al., propose an engineering for giving security benefits in the cloud for cell phones inside a professional workplace. In any case, those latent enemy of burglary strategies accept that the injured individual finds the loss of his or her cell phone quickly and controls the telephone remotely before the criminal shutdown the telephone or expel the insurance application administration from it. Regardless of whether the telephone has set the console lock insurance program, hoodlums can likewise evacuate the security through establishing the framework. L. Simon et al. consider the "counter robbery" components accessible to buyers to defeat unapproved access to individual information on stolen Android cell phones. They explore the usage of their "remote wipe" and "remote lock" works on 10 famous enemy of robbery applications. They found that remote locks are temperamental because of poor usage rehearses. In synopsis, current enemy of robbery devices can't keep telephones from being stolen, and can be impaired through different methodologies. It is important to plan a functioning and continuous enemy of robbery plot, which can recognize the burglary, and alarm the injured individual in any case, keeping stolen from occurring.

III. LITERATURE SURVEY

First age system Anti-robbery locks and Second age procedure ATA (Anti-Theft Alarm).

There are two fundamental determinations of latch: one resembles the one used to bolt our bikes; the other one is coded lock like the one we use to bolt our trunk. Coded lock is worked with a lot of code foreordained, taking care of the losing key issue. A wide range of strategy like above are anything but difficult to utilize and shabby. Be that as it may, their capacity is restricted. Without following strategy, we'll have nothing to do when we lost our gear.[1] The alert is planned with a 105dB amplifier, when our gear is moved illicitly, a caution will be sound. This sort of alert looks popular, however not essentially viable. It possibly works when client is adjacent.[2]

Third age Cell phone ATA and following strategy.

This strategy can be separated into two modules: hostile to robbery module and following module.[3] Hostile to robbery module is like second era item. Following module is coordinated in BIOS of hardware. At the point when it's gone, following programming will run when framework is get to. Programming will contact observing focus of programming when it interfaces Internet, conveying data, similar to IP address. [4]The proprietor can recover the hardware with the guide of police and the product organization. This sort of method can successfully follow stolen gear, yet its capacity has not been upgraded. The technique to pass judgment on whether the gear is lost is excessively straightforward and there's no appropriate answer for manage vital information.

Current anti-theft and tracking technique works on some level. But problems still remain, like low judge accuracy, complex procedure or poor tracking performance. [5] To deal with the problem, developing a new approach with clear judgment, easy operation and accurate tracking comes into our sight. In this paper, different techniques are compared with their advantages and disadvantages listed. Based on this, an innovative loop model of PC/smartphone anti-theft and tracking is introduced.

Customer on PC entire customer PC contains three databases: client characters database, usually utilized IP database and IP-area database. [6]Client characters database stores the few characters of regular client of PC; ordinarily utilized IP database stores IP tends to that are utilized as often as possible; IP-area database stores coordinating pair of IP address and genuine geographic area. In addition, there are modules on PC customer, as well. Location: this module is chiefly accountable for hostile to burglary identification. [7] In the event that they coordinate, programming will think about the PC protected, generally stolen. At the point when the PC associates Internet, IP address will be recognized to help the judgment. Alert module raises caution. In light of judgment of Detection Module, it will raise voice alert.[8] Deal with this module is in charge of sending/accepting directions from cell phone. At the point when PC is in stolen express, this module is enacted. Workstation starts to find itself with inward directions, and after that sends data to cell phone. [9] Additionally, it gets reaction from cell phone to ensure whether keep situating or not, regardless of whether drop caution. So is the situation with cell phone.

At the point when a cell phone is stolen, this module gets comparable data and sends directions to cell phone helping following. Situating and following module is intended to position current area of PC. [10] When situating order is gotten by Manage module, this module is actuated.

Customer on cell phone Combined with three modules. Considering versatile terminal's execution is limited by vitality, stockpiling and information traffic, no database is incorporated in cell phone. [11]Get module investigations the substance of data and decide if to see client the loss of his mobile or actives GPS situating module.GPS Positioning: it's accountable for cell phone situating. [12] At the point when cell phone is lost, client can send relating directions through PC and inherent programming of cell phone to dynamic this module, situating area. Send: this module is in charge of sending assortments of directions to PC.

IV. PROBLEM STATEMENT

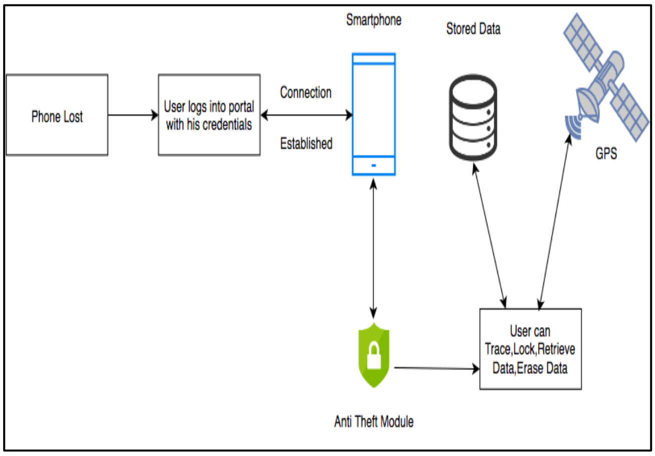
Cell phones normally need to help various security destinations. These can be cultivated through a blend of security highlights incorporated with the cell phones and extra security controls connected to the cell phones and different parts of the endeavor IT foundation. The most widely recognized security targets for cell phones are as per the following:

- Confidentiality—guarantee that transmitted and put away information can't be perused by unapproved parties
- Integrity—distinguish any purposeful or unexpected changes to transmitted and put away information
- Availability—guarantee that clients can get to assets utilizing cell phones at whatever point required.

To accomplish these destinations, cell phones ought to be verified against an assortment of dangers. Cell phones regularly need extra assurance on the grounds that their tendency by and large places them at higher introduction to dangers than other customer gadgets (e.g., work area and PC gadgets just utilized inside the association's offices and on the association's systems). Prior to structuring and conveying cell phone arrangements, associations ought to create framework danger models for the cell phones and the assets that are gotten to through the cell phones. Risk demonstrating includes recognizing assets of intrigue and the attainable dangers, vulnerabilities, and security controls identified with these assets, at that point evaluating the probability of effective assaults and their effects, lastly dissecting this data to figure out where security controls should be improved or included. Risk displaying encourages associations to distinguish security necessities and to plan the cell phone answer for fuse the controls expected to meet the security prerequisites. Significant security worries for these innovations that would be incorporated into most cell phone risk models are recorded underneath. The existing system is purely application/software based without the use of any dedicated hardware the security module, the software can be uninstalled or blocked by the person who steals the smartphone and also the phones data can be completely erased by factory resetting the device.

V. PROPOSED SYSTEM

The proposed system deals with the problems encountered in the existing system and trying to overcome the problem in an effective and fool-proof method by embedding a dedicated security module into the smartphone SoC upon manufacturing where in the device is enabled with advanced security features for anti-theft protection and remote data erase and retrieval by the user when the phone is lost. Smartphone SoC manufacturing giants like Qualcomm and Samsung with their snapdragon and Exynos processors respectively should integrate the security module which we are proposing so that the smartphone which is lost can be easily found and the data is not at stake and can be easily remote erased and data can also be retrieved from the online portal which interacts with the security module and the location of the smartphone can also be traced, which is only possible in the proposed system where in we are proposing a hardware based model whereas the existing anti-theft system for smartphones are purely app-based without the implementation of an dedicated hardware module embedded within the smartphone.


Smartphone
Stored Data
Phone Lost
User logs into portal with his credentials
Connection
Established
GPS
User can Trace,Lock,Retrieve Data,Erase Data
Anti Theft Module

Proposed Architecture diagram

VI. FUTURE SCOPE

The proposed system of hardware based anti-theft system can also be implemented in laptops with a similar concept of using an dedicated security chip which helps us to preserve our precious data without being stolen or misused because people store very important information and credentials on their laptop and these are at stake when the laptop is stolen. This make sure confidentiality of the files is maintained and no one else can access the data or misuse it and we can have a control over the laptop by communicating with the dedicated hardware. By following this we can easily retrieve the laptop from the thief who stole it and also the data is safeguarded. So the chances of getting back our laptop is high and data loss is prevented.

VII. CONCLUSION

This paper presents a robustanti-theft system for smartphones, a hardware based anti-theft system which is fool-proof and effective for smartphones.

By embedding an dedicated security module in the SoC of the smartphone we can communicate with the smartphone anytime unlike in traditional and current anti-theft system which uses a app in the smartphone which once uninstalled or factory reset is performed, the communication between the owner and the smartphone is lost and it becomes very difficult to trace and the data is also at stake. By using this system, we can estimate that the chances of getting our smartphone and the data back is high. In thefuture work, we plan to expand this implementation to laptops.

ACKNOWLEDGMENT

We would like to thank our guide Ms. J. Caroline El Fiorenza, HOD (CSE Dept) and Dean of our University.

REFERENCES

1. Xixian LIU. A Method to Realize Guard Against Theft for Laptop[J]. Technology and Applications, 2011,(09):89-90.
2. BBC news: 314 mobile phones 'stolen in London every day', http://www.bbc.com/news/uk-england-london-21018569.
3. Norton Cybercrime Report 2011, http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/.
4. Symantec, “2014 Symantec canada smartphone honey stick project”,report, 2014.
5. “Tencent Mobile Phone Manager,” http://m.qq.com/anti_theft/login.jsp.
6. “Rising Phone Security Assistant,” http://mobile.rising.com.cn/android/.
7. X. Yu, Z, Wang, L. Sun, W. Zhu, N. Gao, and J. Jing, “Remotely wipingsensitive data on stolen smartphones,” in proceedings of the 9th ACMsymposium on Information, computer and communications security,2014, pp. 537-543.
8. L. Subramanian, G Q. M. Jr., and P. Stephanow, “An architecture toprovide cloud based security services for smartphones,” in proceedingsof 27th Meeting of the Wireless World Research Forum, 2011.
9. A. U. S. Khan, M. N. Qureshi, and M. A. Qadeer, “Anti-theft applicationfor android based devices,” in proceedings of IEEE InternationalAdvance Computing Conference, 2014.
10. Simon, R. Anderson, “Security analysis of consumer-grade anti-theftsolutions provided by android mobile anti-virus apps,” in proceedings ofthe 4th Mobile Security Technologies Workshop, 2015.
11. “Software reduces identity theft risk in stolen cell phones,” http://mobiledevdesign.com/news/software-reduces-identity-theft-riskstolen-cell-phones.
12. “Lookout Mobile Security,” https://www.lookout.com.