iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4333

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Preventing the Data Over-Collection in Smart City via Secure Protection

Ms. S. Suganya[1], Mr. B. Jai Kumar[2]
[1]*PG scholar,* [2]*Assistant Professor, Department of Computer Science and Engineering, Vivekanandha College of Technology for Women Tiruchengode, India.*

Abstract: ***The smart city is meant to be the next generation of Urbanization. The most arduous challenge about the cyber security and privacy of smart city to ensure the precise data secure. The smart device not only stores users' data but also generates data. These data may consist of users' accounting numbers and passwords, emails and house addresses, photos, and other kinds of precise data. The most serious possible security hazard is that applications collect data more than enough on its original function while in permission scope, which to call it data over-collection. Cloud services are in charge of managing users' data and provide fine-grained access control and encryption/ decryption services. To solve the problem of quantifying security risk to score application mainly focusing about the data over-collection behaviors. To prove that the framework improves the security of Smartphone's significantly.***
Keyword: Smart City, Data Over-Collection, Security, Cyber-Security and privacy, cloud storage , smart phones

I. INTRODUCTION

Mobile computing is human–computer interaction by which allows for transmission of data, voice and video. The smart city is meant to be and will be the next generation of urbanization. However, it brings some new challenges to be solved, such as security and privacy. The most arduous challenge about the cyber security and privacy of smart city is to ensure sensitive data secure. People living in a smart city use all kinds of electronic devices instead of traditional manual or mechanical equipment. To make the whole smart city efficiently, almost all these electronic devices need to be smart enough to recognize different users. Consequently, they must have the ability to store and share data. Is from Go Green in the City project of Schneider Electric. The aim of Go Green in the City project is improving and integrating traditional systems into a smart city. A smart city consists of various kinds of smart things, such as smart energy, smart water, smart buildings, smart integration, smart public service, and smart mobility. In the City project of Schneider Electric, The aim of Go Green in the City project is improving and integrating traditional systems into a smart city. As shown in the smart city consists of various kinds of smart things, such as smart energy, smart water, smart buildings, smart integration, smart public service, and smart mobility. These smart systems form the backbone of the city's efficiency, livability, and sustainability. In a smart city, people need to hold a ring with many kinds of keys or to manage various kinds of cards, such as ID card, driving licensee card, and credit card. They can be recognized automatically by smart systems. To use various kinds of smart systems in a smart city, Residents must offer their personal information to these smart systems. Residents must offer the information of their bank accounting numbers and passwords to shop online. They must offer the information of their addresses to receive packages. Consequently, data are the core of a smart city, because they consist of all users' information, which is invaluable in the Big Data age. Nevertheless, users are suffering the potential privacy leakage when they are enjoying the convenience brought by the smart city. However, there may be a lot of kinds of data leakage in a smart city. In The smart city, various kinds of traditional systems transform into smart systems and integrate their functions into Smartphone's. Consequently, a Smartphone is the most widely used electronic devices in the smart city, because of its portability. Using Smartphone's, residents can access the Internet via everywhere Wi-Fi, take online courses, pay their bill online, sign a contract online, and receive medical treatment by tale-health. The Smartphone not only stores users' data but also generates data. These data may consist of users' accounting numbers and passwords, emails and house addresses, photos, and other kinds of sensitive information. As a result, the security and privacy of Smartphone data become an important issue to achieve the blueprint of the smart city.

II. RELATED WORKS

1) *W. Enck et al,* [2] today's smartphone operating systems frequently fail to provide users with adequate control over and visibility into how third-party applications use their private data. The address these shortcomings with Taint Droid, an efficient, system-wide dynamic taint tracking and analysis system capable of simultaneously tracking multiple sources of sensitive data.

Taint Droid provides real-time analysis in reach averaging Android's virtualized implementation of environment. Taint Droid incurs only 14% performance overhead on a CPU-bound micro-benchmark and imposes negligible overhead on interactive third-party applications. Taint Droid, an extension to the Android mobile-phone platform that tracks the flow of privacy-sensitive data through third-party applications. Taint Droid assumes that downloaded, third-party applications are not trusted, and monitors–in real-time–how these applications access and manipulate users' personal data. Our primary goals are to detect when sensitive data leaves the system via untrusted applications and to facilitate analysis of applications by phone users or external security services.

2) *Schneider's,* [3] The paper to start with flagging broader multidimensional larger challenges of sustainable development based on empirical findings using composite sustainable development index. To realize this is important for final negotiation towards implementation with city scale development decision makers. The second part of the study presents as well as the defined boundary for green growth. Using sector-wise database available from official sources results are derived to show which economic sector has how much green growth investment potential compared to a baseline. The potential assessment is based on effective and efficient technology deployment scope. However, case studies on behavioral response also highlight the scope of taking back effect due to behavioral response parameter of a rebound effect. Third part outline practical issues in grabbing the opportunities for green growth in a fast-growing developing country context. Utilizing distributed beam forming in relay-assisted communications to transmit information from a source to a destination has the potential to improve the performance of the wireless system on several aspects of green wireless. Relevant improvements are signal-to-noise power ratio (SNR) enhancement and reduction of power consumption. In this work, to use a distributed beam forming in a non-regenerative relay system to reduce the total power consumption. To successfully derive the optimal weights at the relay stations and the receiver using matrix/vector notation, which allows received signals to be coherently added at the receiver therefore maximizing the output SNR. The Electrical grids, gas distribution systems, water distribution systems, public and private transportation systems, commercial buildings, hospitals, homes these form the spine of the city's efficiency, livability, and sustainability. It is the improvement and integration of these critical city systems done in a step-by-step manner that become the cornerstones to making a smart city a reality.

3) *M. Egele et al,* [4] Shake Them All is a popular "Wallpaper" application exceeding millions of downloads on Google Play. At installation, this application is given permission to access the Internet for updating wallpapers and use the device microphone to change background following noise changes. With these permissions, the application could silently record user conversations and upload them remotely. These smartphones have become powerful devices that are basically miniature versions of personal computers. However, the growing popularity and sophistication of smartphones have also increased concerns about the privacy of users who operate these devices. These covers have been exacerbated by the fact that it has become increasingly easy for users to install and execute third-party applications. To protect its users from malicious applications, Apple has introduced a vetting process. To the vetting process should be ensure that all applications conform to Apple's (privacy) rules before they can be offered via the App Store. The present a novel approach and a tool, PiOS, that allow us to analyze programs for possible leaks of sensitive information from a mobile device to third parties. The PiOS uses static analysis to detect data flows in Mach-0 binaries, compiled from Objective-C code.

4) *J. Cheng et al,* [5] Mobile and web applications increasingly leverage service-oriented architectures in which developers integrate third-party services into end-user applications. This includes identity management, mapping and navigation, cloud storage, and advertising services, among others. While service reuse reduces development time, it introduces new privacy of the security risks due to data repurposing and over-collection as data is shared among multiple parties who lack transparency in third-party data practices. To address this challenge, the proposed new techniques based on Description Logic (DL) for modeling multiparty data flow requirements and verifying the purpose specification and collection and use limitation principles, which are prominent privacy properties found in international standards and guidelines. The principles reduce the risk of over-collection, which is the collection of more information than is needed, and repurposing, which is using or sharing data for purposes other than that for which data was collected the Repurposing occurs at data collectors, who collect information from the data subject, or at data processors, who process personal information on behalf of data collectors. In composable systems, these principles are challenging to verify due to the transitive nature of data storage and processing across multiple parties.

5) *A. Pathak et al,* [6] Smart object interconnected between each other and producing a large volume of information the Internet of Mobile Things (IoT) is a huge challenge. The things that expect to connect to the Internet will consist of sensors, actuators with information processing and communication capabilities that will make themselves intelligent. Sensors are collecting continuously environmental data (e.g. body area network, smart city, cars, smartphones, etc).This architecture process real-time

data and maximize the delivery of raw data to the cloud for post-processing. It also ensures efficient event-driven data collection given the buffer space and communication bandwidth limitations of each sensor. An intelligent IoMT gateway and middleware used to support different message format of sensor data and efficient decision-making system. The paper defines a data collection architecture supporting the physical dimension of sensors to the storage of data in a cloud-based service. Heterogeneous sensor data provide some services to the human being. They have sensors on a fleet of the truck of this customer and collect customer acoustic data from the engines. Any impending problem will cause the sound input change when you can get a preventive maintenance done.

III. PROPOSED WORK

The mobile-cloud framework, in which user's data is stored in a cloud. Cloud services are in charge of managing users' data and provide fine-grained access control and encryption/decryption operations which previously were implemented in smartphones. Furthermore, they evaluate the feasibility and advantages of this approach by experiments. They store the data into smartphones and use them anywhere and anytime. However, some sensitive data may be stored into the smartphones as well, such as the bank accounting number and password, some photos with commercial confidential, and some other personal information. Set of the default security level as the "normal". Assuming that applications send a request to access to a piece of data with the security level, and then the system can authorize these applications to access all the data at the security level. Due to lack of consensus about what kinds of data are highly sensitive, to assign security levels to different kinds of Smartphone data based on the security level of website data. The approach also has significant advantages for the original one. The least improvements in the experiment are the security risk of photo data and the security risk of movie data. However, the security risk of photo data in this approach is over 3.5 times less than that in the original environment.

A. Smart City Environments

To use various kinds of smart systems in a smart city, residents must offer their personal information to these smart systems. Residents must offer the information of their bank accounting numbers and passwords to shop online. They must offer the information of their addresses to receive packages. Consequently, data are the core of a smart city, because they consist of all users' information, which is invaluable in the Big Data age. Nevertheless, users are suffering the potential privacy leakage when they are enjoying the convenience brought by the smart city. However, there may be lot kinds of data leakage in the smart city.

B. Smartphone Data

With the development of electronics technology, all kinds of Smartphone’s flood into the market, and Smartphone’s are increasing usurping on peoples life with go anywhere apps offering a wide array of enterprise, social, financial, and recreational services. Apple App Store and Google Play Store provide thousands of apps with various functions. The streamlining of marketing, installation, and update creates low barriers for developers to bring apps to market, and even lower the barriers for users to obtain and use them. Besides the popularity and functionality, however, apps bring us enormous security problems.

C. Cyber Security And Privacy

At present, the most serious potential security hazard is that apps collect data more than enough on its original function while in permission scope, which we call it data over the collection. To survey current solutions to solve data over collection problem and find that almost all these approaches are passive defense measures, which are a remedy approach after being hurt. Furthermore, these solutions need to run tools or other apps to monitor and detect the data over collection a behavior, which consumes more energy of smartphones.

D. Data Over Collection

To study the data over the collection, to first analyze how these behaviors happen and the risks they bring to users. To take location, photos, International Mobile Equipment Identity IMEI and Unique Device Identifier UDID as cases and find that large parts of apps are over-collecting user's data without noticing them. Then to discuss the two main factors of data over collection in smartphones, which are operating system and permissions. They present a mobile cloud framework, in which users' data is stored in a cloud. Cloud services are in charge of managing users data and provide fine-grained access control and encryption-decryption operations which previously were implemented in smartphones. Furthermore, they evaluate the feasibility and advantages of our approach by experiments.

IV. ARCHITECTURE

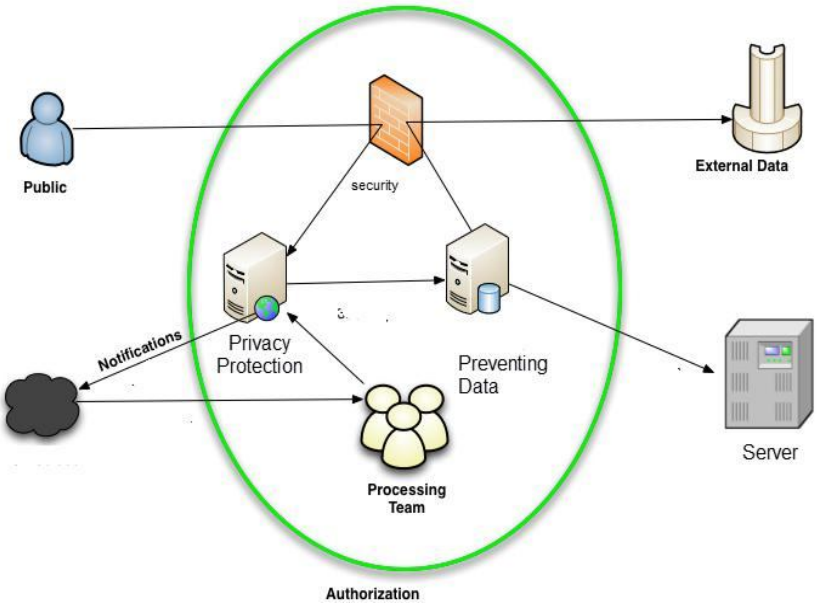


Fig-1 Architecture Diagram

V. CONCLUSION

Data over collection in smart phone becomes the most severe potential privacy hazard in the smart city. Unlike malware, data over the collection is difficult to be solved, because this kind of behaviors is within permissions authorized by users. To maximize releasing user's operation pressure and eradicating the data over collection problem, the presented an active approach. Every application that wanted to use user's data sent its request for accessing the cloud, and the cloud access control service could provide detailed permissions for every application to every block of user's data. Meanwhile, the operations of encryption and decryption were achieved by cloud encryption/decryption service that saves computation resource of smart phone for dealing with these complex calculations. Finally, experimental result verifies the feasibility and advantages of the framework.

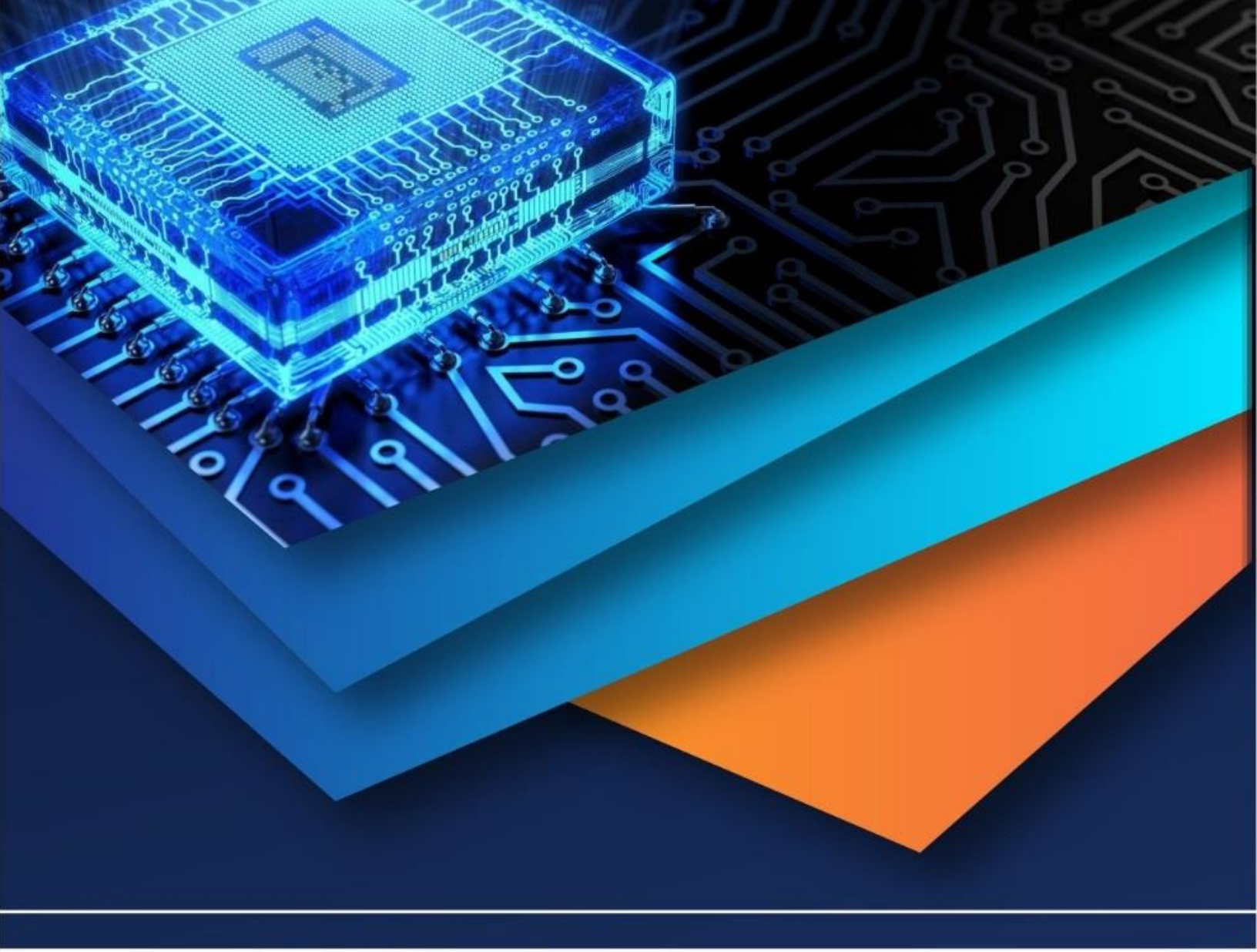
VI. FUTURE ENHANCEMENT

To set the default security level as the "normal". Assuming that an app sends a request to access to a piece of data with *s* security level, and then the system can authorize this app to access all the data with *s* security level. Due to lack of consensus about what kinds of data are highly sensitive, to assign security levels to different kinds of smartphone data based on the security level of website data. Our approach also has significant advantages for the original one. The least improvements in our experiment are the security risk of photo data in Device A and the security risk of movie data in Device D. However, the security risk of photo data in Device A in our approach is over 3.5 times less than that in the original environment. The security risk of movie data in Device D in our approach reduce is about 1.57 times less than that in the original environment. To conclude that the security risks are much lower than in the original environment. In our approach, the granularity is the unit piece of data, which directly determines the effect of our approach. The original approach has the biggest granularity and that is the reason leads to the data over-collection behaviors. Consequently, the finer granularity is the more data can be protected by our approach.

REFERENCES

[1] Yibin Li Wenyun Dai, Zhong Ming, Meikang Qiu (2016), 'Privacy Protection For Precenting Data Over Collection in Smart City'
[2] Enck .W, Gilbert .p, Chun.B.G, Cox .L.P, Jung .J, Mcdaniel ,.J, and Sheth .A.N. (2015), 'Taint droid: An Information-flow tracking system for real-team privacy Monitoring on Smartpone, in USENIX 9th Confrence on Operating System Design and Implementation.
[3] Schneider, (2014), 'Go green in the city.' http://2014.gogreeninthecity.com/smart-cities.html.
[4] Egele .M, Kruegel .C, Kirda .E, and Vigna .G. (2012), 'PiOS: Detecting privacy leaks in iOS applications,' in Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS).
[5] Cheng .J, Wong .S .H, Yang .H, and Lu .S. (2010),'Detecting Repurposing And Over - Collection In Multi-
[6] Party Privacy Requirements Specifications,' in ACM 5th International Conference on Mobile Systems Applications and Services.

[7] Pathak .A, Hu .Y.C, and Zhang .M. (2013), 'Sensors Data Collection Architecture On The Internet Of Mobile Things As A Service Platform,' in ACM 7th (Iomtaas) European Conference on Computer Systems, ser. EuroSys '12.
[8] Bose .A, X. Hu, K. G. Shin, and T. Park. (2011), 'Behavioral detection of malware on mobile handsets,' ACM 6th International Conference on in Mobile Systems, Applications, and Services.
[9] Gilbert .P. (2009), 'Participatory Sensing For Smart Cities: A Case Study On Transport Trip Quality Measurement'.Egele .M, Kruegel .C, Kirda .E, Hu .Y.C. (2012), ' Effective Collaborative Monitoring In Smart Cities: Converging MANET And WSN For Fast Data Collection,' in Proceedings of the18th Annual Network& Distributed System Security Symposium (NDSS).
[10] Enck .W, Gilbert .P, Chun .B.G, Cox .L.P, Jung .J, Mcdaniel J, And Sheth .A.N. (2011), 'Research on Multi-Source Heterogeneous Data Collection for the Smart City Public Information Platform, in USENIX Conference on Operating Systems Design and Implementation
[11] Zhang .M. (2014), 'Smart City Service Acceleration On FPGAs



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY