Location Based Encryption

Joshi Akash[1], Kamble Rutuja[2], Uthwal Harshada[3], Prof. Bharati Pandhare[4]
[1, 2, 3, 4] Department of Computer Engineering
[1, 2, 3, 4] Vidya Prasarini Sabha's College of Engineering And Technology Lonavala, Pune

Abstract- *Cloud computing is a new approach in the field of information technology and development of computer technologies based on the World Wide Web. One of the most relevant challenges in this generation is the security of cloud computing. On the other hand the security of access to critical and confidential information in banks, institutions and etc is extremely essential. Sometimes even with the enormous costs, it is not fully guaranteed and it is compromised by the attackers. By providing a novel method, we improve the security of data access in cloud computing for a company or any other specific locations using the location-based encryption.*

Keywords- Global Positioning System (GPS), Context Provider (CP), Access Controller (AC), Cellular Triangulation (Cell ID).

I. INTRODUCTION

Initially mobile phones were developed only for voice communication but now days the scenario has changed, voice communication is just one aspect of a mo-bile phone. There are other aspects which are also important. They are web browser and GPS services. Both of these are already implemented but are not in the hands of users but in the hands of manufacturers because of proprietary issues, it does not allow the user to access the mobile hardware directly. But now, after the release of android based open source mobile phone a user can access the hardware directly and design customized native applications to develop Web and GPS enabled services and can program the other hardware component like camera etc.

We are developing banking application using Location Based Encryption. As compare to current banking application which are location-independent, we are developing banking application which is location dependent.

That means Cipher-text can only be decrypted at given location in Cryptography i.e. location-dependent approach[1]. If that data is decrypted at another location, the decryption process terminates and does not acquire any information about the plaintext.

This is important in real time application[3], example in military base application, Cinema Theater. But our system is flexible enough to provide access to customer to his/her account from any location.

II. LITERATURE SURVEY

1. LDEA: Data encryption algorithm based on location of mobile users.

Authors: Hsien-Chou Liao and Yun-Hsiang Chao

A target latitude/longitude coordinate is determined firstly. The coordinate is incorporated with a random key for data encryption. The receiver can only decrypt the cipher text when the coordinate acquired from GPS receiver is matched with the target coordinate. However, current GPS receiver is inaccuracy and inconsistent. The location of a mobile user is difficult to exactly match with the target coordinate. A toleration distance(TD) is also designed in LDEA to increase its practicality. The security analysis shows that the probability to break LDEA is almost impossible since the length of the random key is adjustable. A prototype is also implemented for experimental study. The results show that the cipher text can only be decrypted under the restriction of TD. It illustrates that LDEA is effective and practical for data transmission in mobile environment.

2. On location models for ubiquitous computing

Authors: Christian Becker Æ Frank Du¨ rr

Common queries regarding information processing in ubiquitous computing are based on the location of physical objects. No matter whether it is the next printer, next restaurant, or a friend is searched for, a notion of distances between objects is required. A search for all objects in a certain geo graphic area requires the possibility to define spatial ranges and spatial inclusion of locations. In this paper, we discuss general properties of symbolic and geometric coordinates. Based on that ,we present an overview of existing location models allowing for position, range, and nearest neighbor queries. The location models are classified according to their suitability with respect to the query processing and the involved modeling effort along with other requirements .Besides an overview of existing location models and approaches, the classification of location models with respect to application requirements can assist developers in their design decisions.

3. Securing sensor networks with location-based keys

Authors: Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang

Wireless sensor networks are often deployed in unattended and hostile environments, leaving individual sensors vulnerable to security compromise. This paper proposes the novel notion of location-based keys for designing compromise tolerant security mechanisms for sensor networks. Based on location based keys, we develop a node-to-node authentication scheme, which is not only able to localize the impact of compromised nodes within their vicinity, but also to facilitate the establishment of pair wise keys between neighboring nodes. Compared with previous proposals, our scheme has perfect resilience against node compromise, low storage overhead, and good network scalability. We also demonstrate the use of location-based keys in combating a few notorious attacks against sensor network routing protocols.

4. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones

Authors: William Enck, Peter Gilbert, Byung-Gon Chun

Todays smart phone operating systems frequently fail to provide users with adequate control over and visibility into how third-party applications use their private data We address these shortcomings with TaintDroid, an efficient, system-wide dynamic taint tracking and analysis system capable of simultaneously tracking multiple sources of sensitive data. TaintDroid provides real time analysis by leveraging Androids virtualized execution environment. TaintDroid incurs only 14% performance overhead on a CPU-bound micro-benchmark and imposes negligible over-head on interactive third-party applications. Using TaintDroid to monitor the behavior of 30 popular third-party Android applications, we found68 instances of potential misuse of users private information across 20 applications. Monitoring sensitive data with TaintDroid provides informed use of third-party applications-for phone users and valuable input for smart phone security service firms seeking to identify misbehaving applications.

5. Location based services using android mobile operating system

Authors: Amit Kushwaha1, Vineet Kushwaha

The motivation for every location based information system is: To assist with the exact information, at right place in real time with personalized setup and location sensitiveness. In this era we are dealing with palmtops and iPhones, which are going to replace the bulky desktops even for computational purposes. We have vast number of applications and usage where a person sitting in a roadside caf needs to get relevant data and information. Such needs can only be catered with the help of LBS. These applications include security related jobs, general survey regarding traffic patterns, decision based on vehicular information for validity of registration and license numbers etc. A very appealing application includes surveillance where instant information is needed to decide if the people being monitored are any real threat or an erroneous target. We have been able to create a number of different applications where we provide the user with information regarding a place he or she wants to visit. But these applications are limited to desktops only. We need to import them on mobile devices. It ensures that when a person goes for a tour or any tourist place there is no need of taking the travel guides with him. All the information should be available in his mobile device and also in user specified format.

6. Location based services using android

Authors: Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta

Initially mobile phones were developed only for voice communication but now days the scenario has changed ,voice communication is just one aspect of a mobile phone There are other aspects which are major focus of interest. Two such major factors are web browser and GPS services .Both of these functionalities are already implemented but are only in the hands of manufacturers not in the hands of users because of proprietary issues, the system does not allow the user to access the mobile hardware directly. But now, after the release of android based open source mobile phone a user can access the hardware directly and design customized native applications to develop Web and GPS enabled services and can program the other hardware components like camera etc. In this paper we will discuss the facilities available in android platform for implementing LBS services (geo-services).

7. Context sensitive access control

Authors: R.J. Hulsebosch†, A.H. Salden, M.S. Bargh, P.W.G. Ebben, J. Reitsma

We investigate the practical feasibility of using context information for controlling access to services. Based solely on situational context, we show that users can be transparently provided anonymous access to services and that service providers can still impose various security levels. Thereto, we propose context-sensitive verification methods that allow checking the users claimed authenticity in various

ways and to various degrees. More precisely, conventional information management approaches are used to compare historic contextual (service usage) data of an individual user or group. The result is a relatively strong, Less intrusive and more flexible access control process that mimics our natural way of authentication and authorization in the physical world.

III. IDENTIFY, RESEARCH AND COLLECT IDEA

This technology enables individuals, companies and etc. To store their data and information on the cloud and they can access their own data at any time, from any place and using any computer through the internet. It is even possible to deploy a platform in a cloud and use it (instead of installing software on a personal computer). This technology is certainly a big advantage and always beside the advantages.
Our system uses location based encryption technique for providing security to the banking application. Our system only allows authenticated people for doing transaction. Authentication is based on location based encryption. In case of physical attack, our system creates a virtual environment with extra key in password and allows fake transactions. Our system allows access of account from any location.

IV. WRITE DOWN YOUR STUDIES AND FINDINGS

Data security in the cloud is so important. Users (individuals or companies) are concerned about the access to the information by unauthorized users.

Now suppose that data is some critical and confidential information from a bank, or a company and etc. Certainly the necessity of access control in the cloud computing is more than ever and is a very important part of data security in cloud.

In our method we use the user's location and geographical position and we will add a security layer to the existing security measures.

Our solution is more appropriate for banks, big companies, institutions and examples like this. The only thing we need is an Anti-Spoof and accurate GPS that companies can afford to buy.

Also implementing the LDEA algorithm on the cloud and the user's computer (which is connected to the GPS) is required.

A. Purpose of LDEA

The purpose of this algorithm i.e. LDEA is mainly to include the latitude/longitude coordinate in the data encryption and to restrict the location of data decryption. When a target coordinate is determined for encryption, the ciphertext can only be decrypted at the specified location. Though the GPS receiver is inaccurate and not consistent depending on how many satellite signals are received. It is difficult for receiver to decrypt the ciphertext at the same location exactly matched with the target coordinate. It is not practical to use the incorrect GPS coordinate as key for data encryption..

B. Proposed Work

We are proposing system in which when the user is under attack he/she can login to his /her account by entering the password with extra key, that is identified at server side and hence access will be prohibited. We are using Geo-Encryption Algorithm, location based cryptography, positioning tools (Anti-spoof GPS). That means our system provide solution to physical attack using virtualization, in which customer is allowed to perform fake transaction for his/her physical security purpose.

V. CONCLUSION

Location Based Encryption and LDEA algorithm were also reviewed. A new security level was adds to existing system measures using Location Based Encryption. This method can be used in several places such banks, companies, institutions and have the desired performance.

ACKNOWLEDGMENT

We thank our Principal. Prof.S.Padwal and HOD Prof.B.T.Pandhare for guiding and supporting us in this topic.

REFERENCES

[1] Hsien-Chou Liao and Yun-Hsiang Chao Department of Computer Science and Information Engineering, Chaoyang University of Technology,168 Jifong E. Rd., Wufeng Township Taichung County, 41349, Taiwan (R.O.C.)

[2] Wikipedia, (May 2013). Samsung galaxy s4 specifications. [Online]. Available: http://en.wikipedia.org/wiki/Samsung_ Galaxy_S4

[3] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, “Taintdroid: An information-flow tracking system for realtime privacy monitoring on

smartphones," in Proc. 9th USENIX Conf. Oper. Syst. Des. Implementation, 2010, pp. 1–6.

[4] J. Leyden, (Apr. 2013). Your phone may not be spying on you now—but it soon will be. [Online]. Available: http://www.theregister.co.uk/2013/04/24/kaspersky_mobile_malware_infosec

[5] R. Templeman, Z. Rahman, D. J. Crandall, and A. Kapadia, proporty.(2013).[Online] .Available: https://www.llnl.gov/about/controlleditems.html "Placeraider: Virtual theft in physical spaces with smartphones," in Proc. 20th Annual Netw. Distrib. Syst. Security Symp. (NDSS), Feb. 2013.

[6] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, "Soundcomber: A stealthy and context-aware sound Trojan for smartphones," in Proc. 18th Annu. Netw. Distrib. Syst. Security Symp., Feb. 2011, pp. 17–33. [7] L. L. N. Laboratory, Controlled items that are prohibited on llnl proporty. (2013). [Online]. Available: https://www.llnl.gov/about/controlleditems.html

[7] L. L. N. Laboratory, Controlled items that are prohibited on llnl proporty. (2013). [Online]. Available: https://www.llnl.gov/about/controlleditems.html

[8] M. Conti, V. T. N. Nguyen, and B. Crispo, "Crepe: Context-related policy enforcement for android," in Proc. 13th Int. Conf. Inf. Security, 2011, pp. 331–345.

[9] A. Kushwaha and V. Kushwaha, Location based services usinga ndroid mobile operating system, Int. J. Adv. Eng. Technol., vol. 1,no. 1, pp. 1420, 2011.

[10] E. Muller, I. Assent, S. Gunnemann, R. Krieger, and T. Seidl,"Relevant Subspace Clustering: Mining the Most Interesting Non-redundant Concepts in High Dimensional Data", in ICDM, 2009, pp. 377386.

[11] A. Gupta, M. Miettinen, N. Asokan, and M. Nagy, Intuitive securitypol-icy configuration in mobile devices using contextprofiling, in Proc. IEEE Int. Conf. Soc. Comput., 2012, pp. 471480.

[12] W. Enck, M. Ongtang, and P. McDaniel, Understanding . android securit y, IEEE Security Privacy, vol. 7, no. 1, pp. 5057, Jan. 2009

[13] H.-P. Kriegel, E. Schubert, A. Zimek, and P. Kroger, "Outlier detection in axis-parallel subspaces of high dimensional data", in PAKDD, 2009, pp. 831838.

[14] E. Trevisani and A. Vitaletti, Cell-id location technique, limits and bene-fits: An experimental study, in Proc. 6th IEEE Workshop Mobile Comput. Syst. Appl., 2004, pp. 5160.

[15] J. LaMance, J. DeSalas, and J. Jarvinen, AGPS: A low-infrastructure approach Online]. Available: http://www.gpsworld.com/innovation-assisted-gps-a-low-infrastructure-approach/.

[16] Skyhook.(2003).[Online].Available :http://www.skyhookwireless.com/.

[17] O.G.CONSORTIUM, Open gis simple features specification. forsql. revi-sion 1.1,1999