iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** II **Month of publication:** February 2017

DOI: http://doi.org/10.22214/ijraset.2017.2075

www.ijraset.com

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

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Locate Me: A Privacy Preserving Pseudonym Generation of Location Proof Updates Through Co-Located Devices

Deepan E. [1], Aaravamuthan P. [2], Kasinathan R. [3], Jagadeeshkumar R. [4], Mr. N. Gobi[5]
[1,2,3,4]*B.E., Computer Science Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi.*
[5]*Assistant Professor, Computer Science Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi.*

***Abstract:** Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. This approach allows the user to cheat by having his/her device transmit a fake location, which might enable the user to access a restricted resource erroneously or provide false identity. To address this issue, we propose a far better system, more efficient than A Privacy-Preserving LocAtion proof Updating System(APPLAUS) in which co-located Bluetooth enabled mobile devices mutually generate location proofs, and update to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server in the proposed system. Extensive experimental results show that our proposed scheme (LOCATEme), besides providing location proofs effectively, can efficiently preserve the source location privacy.*

Pseudonyms are objects that consists of Bluetooth MAC, latitudes, longitudes, timestamp, key and they don't have any specific meaning. Pseudonym objects are uploaded to the server at a particular interval of time period with a session_id that can be used to track what time the user has requested for location proofs which avoid pseudonym object clashes and mismatches. This will be helpful to identify whether the user's location is highly accurate, reliable and trustworthy.

The project is set up such that whenever it is used in the device, the bluetooth gets synced up with nearby devices, letting it get the MAC address alone of the bluetooth device just in case to give the user an identity that is totally unique. This helps in distinguishing users so that they can be used for location proof submissions. The nearby device will send proof for the user's device when the server sends an acknowledgement that their device is prone to proof submissions. The process of sensing nearby co-located devices through bluetooth allows automatic submissions of location proof updates without the need of the user to do the work manually.

I. INTRODUCTION

With the pervasiveness of smart phones, Location Based Services (LBS) have received considerable attention and become more popular and vital recently. However, the use of LBS also poses a potential threat to user's location privacy. In this project, we present an efficient and privacy-preserving location-based query solution, called APPLAUS and LOCATEme. Specifically, to achieve privacy-preserving spatial range query, we propose the first predicate-only encryption scheme for inner product range (Pseudonym object PO), which can be used to detect whether a position is within a given circular area in a privacy-preserving way. To reduce query latency, we further design a privacy-preserving index structure in LOCATEme. Detailed security analysis confirms the security properties of LOCATEme. In particular, for a mobile LBS user using an Android phone, around 1.9 s is needed to generate a query, and it also only requires a commodity workstation.

Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. This approach allows the user to cheat by having his device transmit a fake location, which might enable the user to access a restricted resource erroneously or provide bogus alibis. To address this issue, we propose a privacy preserving location proof updating system (APPLAUS) in which co-located Bluetooth enabled mobile devices mutually generate location proofs, and update to a location proof server.

To develop periodically changed pseudonyms that can be used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. We also develop user-centric location privacy model in which individual users generate their location privacy preserving pseudonym objects in real-time and decide whether and when to accept a location proof exchange request based on their location privacy levels. The main objective is to provide privacy preserving location proof updates for all Location Based Services (LBS), existing and new ones. LOCATEme can be implemented with the existing network

©IJRASET: All Rights are Reserved

infrastructure and the current mobile devices, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost.

II. EXISTING SYSTEM

Mobile devices, such as smartphones and PDAs, are playing an increasingly important role in people's lives. Location based services take advantage of user location information and provide mobile users with a unique style of resource and services. Nowadays more and more location-based applications and services require users to prove their locations at a particular time. Location data are in the form of latitudes and longitudes generated through the GPS available in the mobile device. This data is sensitive and requires privacy[3]. To ensure this privacy of user's location data, we design LOCATEme, a privacy preserving location proof updates through co-located bluetooth devices. Each device generates the location and a corresponding pseudonym object. A pseudonym object comprises of MAC identity of that device, latitude, longitude, timestamp and a key. Initially, the device submits a dummy proof to the server as an acknowledgement. Every time a dummy proof is submitted, a new session gets started with a fresh set of proof counts for each pseudonym object. These are tracked dynamically with real time updates to ensure the accuracy of location data and also preserving the privacy of the location data enclosed within the pseudonym object. When the location proof counts exceeds the threshold value, the user is granted permission and the location is verified as a trusted one. This prevents any sort of false identity and preserves the privacy of the data, that the user entrusts it with the server.

Co-located bluetooth devices are used to generate proofs in the form of pseudonym objects for N nearby devices[4]. Hence, N number of proofs from N number of devices will be generated for N number of other devices simultaneously. Pn number of pseudonym objects will be generated for each nearby device and the same for every other device present within a device's reach. Proximity analysis is not required because, bluetooth is put into use which has a constraint of sensing devices only upto a few hundred metres. We can infer from this that, any proof from one device to another device suggests that those two devices are definitely nearby.

III. SYSTEM METHODOLOGY

A. Dummy proof generation

The prover broadcasts a location proof request to its neighboring nodes through Bluetooth interface according to its update scheduling. The request should contain the prover's current pseudonym Pprov, and a random number Rprov. Dummy proofs acts as an acknowledgement for the server so that it starts to wait for proofs submitted by co-located devices before the session ends and a new one starts.

Figure I Dummy proof generation



B. Pseudonym object generation

Suppose a mobile node i has a set of pseudonyms P1,P2,⋯ ,PM which change periodically, and distinct parameters λ1,λ2,⋯ ,λM for each pseudonym are predetermined. If each pseudonym Pj updates its location proofs (including dummy proofs) such that the inter-update interval follows Poisson distribution with parameter λj, as in Figure 3, then the entire inter-update intervals for node i follow Poisson distribution with a parameter of $\lambda = \lambda 1 + \lambda 2 + \cdots + \lambda M$. It has the properties of pseudonym unlinkability and statistically strong source location unobservability. The pre-defined updating parameter λ determines how frequently location proofs are updated.

©IJRASET: All Rights are Reserved

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

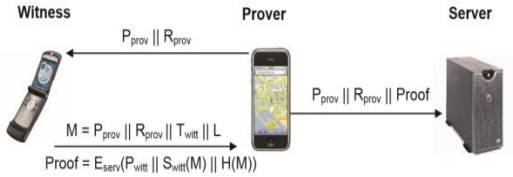
Figure II Proof generation



C. Bluetooth module with location proof generation

Bluetooth is a ubiquitous short-range, low-power communication technology that also provides a robust device discovery mechanism, making it a logical choice for implementing our prototype. As observed in evaluation, limited range and discovery latency due to underlying Bluetooth technology exerts another negative impact on performance of our protocol, especially in high mobility scenarios. **Bluetooth** Smart advertising packets also contain a **MAC address** to identify the device. This helps distinguishing the various users available in the region and also to generate unique per device pseudonym objects. This might help us understand the importance of bluetooth module in the proposed system[14].

Figure III Pseudonym generation through co-located devices



D. Implementing automatic location updates generator

Location will be updated for every 2 seconds. Location manager manages the time interval and accuracy of location data generated by the user's device. Location manager checks for user's permission to allow generate location data, explicitly and it allows the user to decide. Location listener decides what to do with the data based on the location manager's status. It overrides several functionalities like what to do when the location gets changed or disabled. Location provider method will be called every two seconds to generate location data.

Bluetooth module is implemented to get the nearby device synced up with our device automatically in order to get the MAC address of each device and send proofs for them automatically in the background to the server every two seconds letting the user not to do much work but just switching on the option given. Location manager can be used to get high accurate location coordinates from the server.

Bluetooth shouldn't always be switched on which drains the battery of the device. Hence, a time period is provided stating when bluetooth should be active. Once it senses nearby devices, the device list should be stored in a temporary list and the bluetooth must be switched off. This must be done automatically every time, the user sends a dummy proof to the server. Bluetooth discoverability mode should be turned on so that it is visible to all nearby devices. If we fail to do this, none of the nearby device can send proofs for our device and the main purpose for the system fails. Hence, this should be automated to. The default discoverability mode extends up to 300 seconds. After 300 seconds, visibility is turned off and no nearby device can sense the device.

E. Influence of proposed system over LBS

Our proposed system consists of implementation of our modified existing system with privacy preserving location proof updates through co-located devices in all Location Based Services (LBS). We have chosen two location based services, LBS authentication and campus LBS. We ought to implement location proof updates through bluetooth module and we ought to set a threshold value so as to ensure, when the estimated location proofs cross this threshold, the location based services should be enabled. LBS authentication is proposed because username and passwords have become too mainstream and prone to hacking. To avoid this, LBS

©IJRASET: All Rights are Reserved

Volume 5 Issue II, February 2017
ISSN: 2321-9653

authentication provides authentication questions based on user's location. To preserve this location data, we can implement LOCATEme over LBS authentication[1]. The device's dummy proof along with nearby devices' proofs, allows the system to calculate the score whether or not to trust the user's location data.

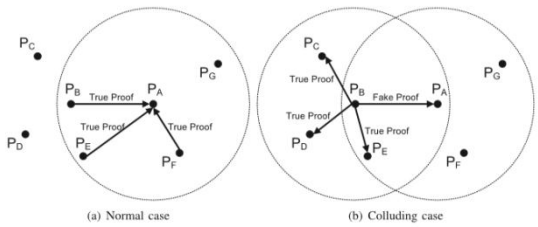
Campus LBS can be used in organizations that requires job tracking and employee tracking. It can be used to track user's activities inside the organization and to provide location data privacy, LOCATEme is implemented over campus LBS. Each time the user accesses the device, new session starts enabling the server to identify the incoming proofs as new set of proofs. This enables the user to have real time updates over their locations and can be established anywhere anytime. Implementation of LOCATEme over LBS can be done by checking whether the proof count is greater than the threshold value or not[2]. If proof count is greater than the threshold value, location data is valid and it enables the LBS. If proof count is not greater than the threshold value, a new session gets started and it waits for new sets of proofs from nearby devices. The bluetooth sense module has been implemented in the existing system itself and it can be used for the proposed system too. It allows the device to sense nearby devices and generate location proof updates for those devices. Automatic generation of data is encouraged in proposed system too as it makes the job of the user easy and it is user friendly.

F.Implementation in LBS authentication system

A location-based authentication system is where authentication questions are generated based on users' locations tracked by smartphones. More specifically, the system builds a location profile for a user based on periodically loggedWi-Fi access point beacons overtime, and leverages this location profile to generate authentication questions. locateme can be used in this system for providing privacy for user's location. If there exists colliding locations, questions may arise based on both the locations.

None the less, location based scheme can be used in addition to password based mechanisms to prevent attacks launched by stolen or lost devices, or attacks launched from remote locations using stolen passwords. For example, location based questions may be asked only if a service provider is in doubt. In such cases, even if the password gets compromised, someone from a remote location cannot access the accounts/services due to failure to answer the location based questions correctly. Hence, based on our findings, we strongly believe that the proposed location-based authentication system can be easily incorporated with existing techniques and significantly improve the overall system security by adding another level of easy to use security mechanism.

Figure IV LBS authentication



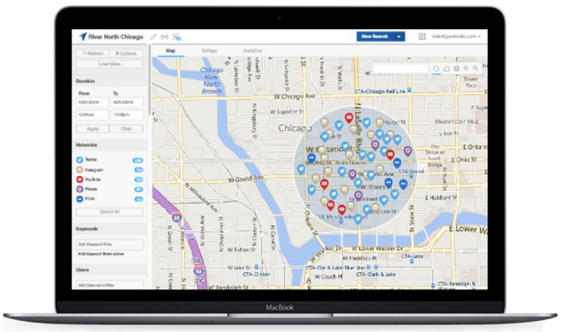
G. Implementation in campus LBS

It can be used in Campus LBS, a system that checks whether the user is present in the required location or not. This system may be used for job tracking and employee tracking. Any campus environment, can gain a lot of value from the emerging location-based services (LBS). There are a few characteristics that render campuses as prime hotspots that enable richer Bluetooth-based LBS experiences. Firstly, there is a captive audience, students, staff, employees spend a lot of time within the campus, with a proportion even living on campus during this period. Secondly, the growing trend is pervasive WiFi – indoor and outdoor always available. Lastly, due to widely available free WiFi, the proportion of people walking around with their mobile devices with WiFi switched "on" is very high relative to other industries, not surprising since students are happy to use campus WiFi rather than pay for their mobile data service and with the help of bluetooth enabled devices, we can manage the activities of each students/employees by implementing LOCATEme over campus LBS to provide locatio data privacy. We can use proximity analysis for tracking location data of the user within the campus and we can manage activities according to that location data.

©IJRASET: All Rights are Reserved

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Figure V Campus LBS



IV. RESULTS

A. Dataset

The referred dataset consisted of raw latitude and longitude data mapped with real time environment and relative location dataset. This wasn't efficient enough to deal with privacy preserving location updates. Pseudonym objects are one among the entities of the table that deals with proximity analysis as well as privacy preservation.

Figure VI Dataset

Entry	Time	Relative location data extracted from beacon processing	Location Estimate from Terminal			Location Estimate at Infrastructure			Location Accuracy Estimate		
			Lat	Long	Elev	Lat	Long	Elev	Lat	Long	Elev
Infrastructure Computation	3/5/2010 10:45 AM	<Terminal beacon data set 6>	na	na	na	40.7936445	-73.415234	162	4.9	5.9	39.6
Infrastructure Computation	3/5/2010 10:30 AM	<Terminal beacon data set 5>	na	na	na	40.7934334	-73.415133	217	5.3	6.1	47.0
Terminal data 4	3/5/2010 10:29 AM	<Terminal beacon data set 4>	40.7933961	-73.4150283	124	40.7933961	-73.4150283	124	12.6	6.2	54.2
Terminal data 3	3/5/2010 10:03 AM	<Terminal beacon data set 3>	40.7934421	-73.4150002	101	40.7934421	-73.4150002	101	14.8	8.2	12.0
Terminal data 2	3/5/2010 9:42 AM	<Terminal beacon data set 2>	40.7934992	-73.4153872	319	40.7934992	-73.4153972	319	2.8	9.9	27.3
Terminal data 1	3/5/2010 9:27 AM	<Terminal beacon data set 1>	40.7939991	-73.4151119	86	40.7939991	-73.4151119	86	7.1	19.2	14.0

The dataset that we intend to create should consist of pseudonym objects instead of latitudes and longitudes in order to provide location data privacy to the users. The device will generate the pseudonym and send it to the server automatically every two seconds. The dataset consists of hits and session to keep track of number of proofs and time of the location data updates.

Figure VII Dataset generated by locate me system

id	pseudonym	hits	session
C0:EE:FB:D5:7F:BA	F5oyp2ubNBSo9/+5yX/Mag== LATLONI99Amtzuj1vqZJNqOYa...	2	1
C0:EE:FB:D5:7F:BA	EQltt41uDBtq7ppnBxEYHw== LATLONTlo5/t+XzJ55k1qT7c1...	2	1
24:DA:9B:7E:F9:69	F5oyp2ubNBSo9/+5yX/Mag== LATLONI99Amtzuj1vqZJNqOYa...	3	1
C0:EE:FB:D5:7F:BA	EQltt41uDBtq7ppnBxEYHw== LATLONTlo5/t+XzJ55k1qT7c1...	2	1
24:DA:9B:7E:F9:69	Ood1jrKosGgt0kqQIXTdWw== LATLONV4/GB/a+JKICFICA7P5...	3	1
24:DA:9B:7E:F9:69	F5oyp2ubNBSo9/+5yX/Mag== LATLONI99Amtzuj1vqZJNqOYa...	1	2

B. Evaluation Metric

During our evaluation, we use three metrics: message overhead ratio, proof delivery ratio, and average delay. The message overhead ratio is defined as the ratio of dummy traffic and real proof traffic. The proof delivery ratio is the percentage of location proof message that is successfully uploaded to the location proof server. The average delay is the time difference between the time when a location proof update is needed and when the location proof message has reached the location proof server. We compare our LOCATEme scheme with a baseline scheme in terms of all metrics. In the baseline scheme, each node does not alter pseudonyms based on Automatic generation system. Rather, it uses a constant rate to upload location proofs. Unlike LOCATEme where two nodes mutually exchange location proofs, the baseline scheme only uploads its own location proof if there is a proof available. A dummy message is uploaded instead when there is no proof available.

©IJRASET: All Rights are Reserved

The performance comparison between LOCATEme and the baseline scheme is shown under different ratio of Interval proof and Interval contact. Here, Interval proof is the required interval between two location proof updates, while Interval contact is the mean real contact interval. Let ω = Interval proof/Interval contact. LOCATEme outperforms baseline on overhead ratio when ω is larger than 0.75. When ω > 1.5, the overhead ratio of LOCATEme decreases to as low as 0.2. The proof delivery ratio also reaches 93% when ω > 1.5. LOCATEme and baseline have similar average delay when ω > 1, in which the delay is measured as the unit of Interval proof. When ω > 1.5, the delay becomes lower than 0.15 of Interval proof. We can conclude that when ω > 1.5, that is, when the location proof update interval is at least 1.5 of the contact interval, the performance of LOCATEme reaches an adequate level. The performance is not improving significantly after ω = 2. Therefore, an appropriate ratio ω between Intervalproof and Intervalcontact should be carefully chosen between 1.5 and 2. LOCATEme assures the ω value of 2 and hence the accuracy level is around 93% and it is a constant one. In Figure 11, the x-axis deals with Intercal proof/ Interval contact ratio and the y-axis deals with the delay. It compares the baseline scheme with LOCATEme and portrays the advantages of LOCATEme over baseline scheme.

V. FUTURE ENHANCEMENT

Thus, Location data in LBS systems can be preserved so that the users will have the assurance of location data privacy as well as efficient transition of location data with promising speed and accuracy. LOCATEme can solve any LBS related problem regarding privacy issues. LOCATEme provides top level accuracy and privacy for user's location data in the form pseudonym objects that can be transferred to any anonymous server without hesitation of losing privacy. This enables the application to develop any kind of LBS based on LOCATEme so as to ensure privacy.

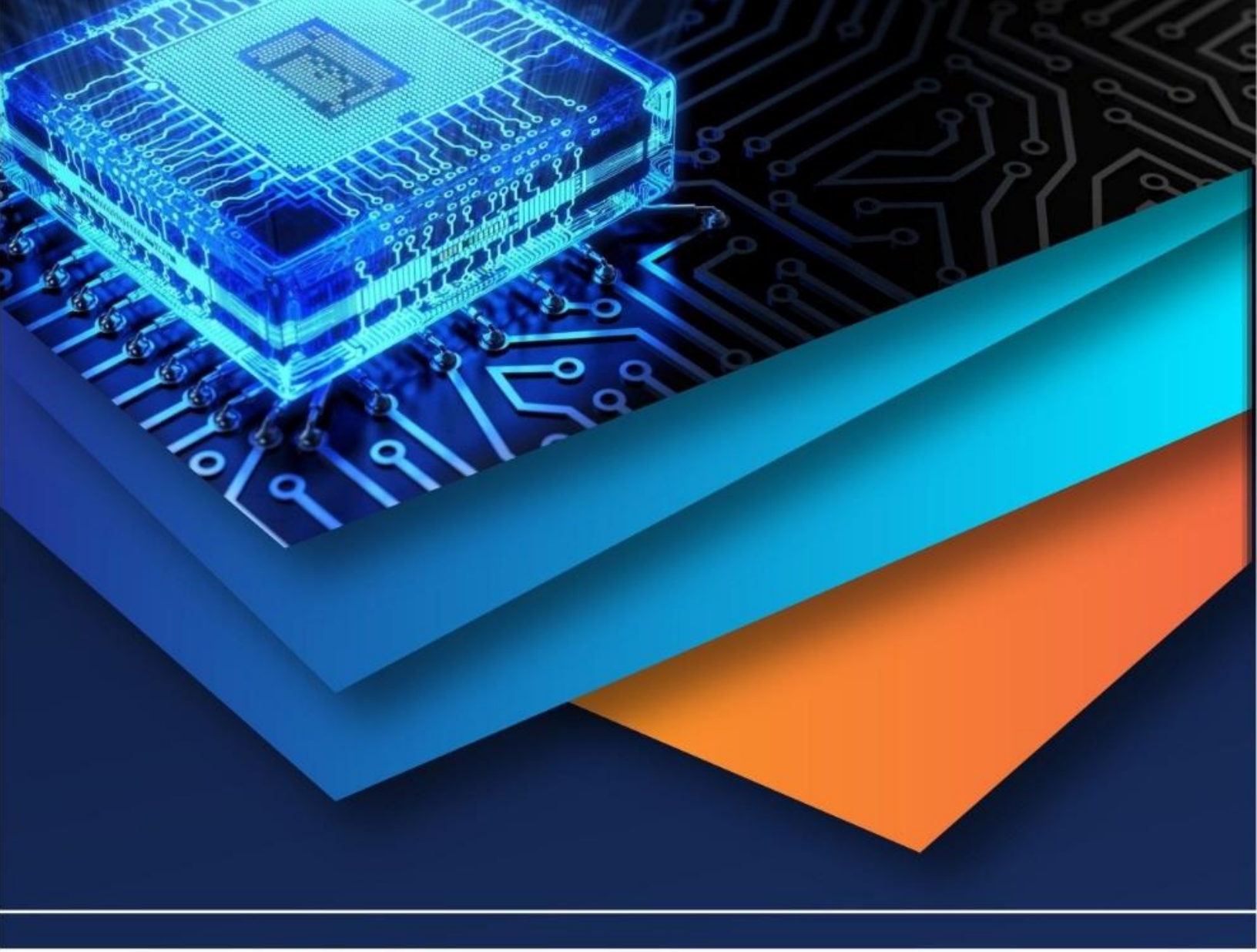
Many emerging applications such as the recent games, Pokemon Go and Mini Militia, constantly shares the user's location data to the server. The user has no location data privacy. It is studied that our system can provide privacy to all the user's location data simultaneously and enable them use these applications in a safer environment.

Many campuses these days have LBS (Location Based Services) with no location data privacy. LOCATEme solves that problem by enabling the user to choose between different privacy levels. LBS authentication is a major interest for many companies now but the huge problem of maintaining the user's location data preserved has been solved by LOCATEme. We ought to give promising results and a better future for all location based services which will be a base factor for all new emerging applications in the market.

REFERENCES

[1] Albayram, Y., Khan, M. M., Bamis, A., Kentros, S., Nguyen, N., & Jiang, R. (2014). A Location-Based Authentication System Leveraging Smartphones. IEEE 15th International Conference on Mobile Data Management
[2] Das, S., & Sadhukhan, P. (2014). Performance evaluation of a LBS system delivering Location-Based Services using wireless local area network. Applications and Innovations in Mobile Computing (AIMoC
[3] Gambs, S., Killijian, M.-O., Roy, M., & Traore, M. (2014). PROPS: A PRivacy-preserving Location Proof System. IEEE International Conference on Reliable Distributed Systems
[4] Gruteser, M., & Grunwald, D. (2013). Anonymous usage of location-based services through spatial and temporal cloaking. ACM MobiSys
[5] Hua, L., & Dai, J. (2014). A location authentication scheme based on adjacent users. Progress in Informatics and Computing (PIC)
[6] Kaur, G., & Sachdeva, M. (2013). Implementation of Secure Authentication Mechanism for LBS using best Encryption Technique on the Bases of performance Analysis of cryptographic Algorithms. International Journal of Security, Privacy and Trust Management (IJSPTM)
[7] Li, M., Sampigethaya, K., Huang, L., & Poovendran, R. (2012). Swing & swap: user-centric approaches towards maximizing location privacy. 5th ACM workshop on Privacy in electronic society
[8] Luo, W., & Hengartner, U. (2013). Proving your location without giving up your privacy. ACM HotMobile
[9] Mengjun, L., Shubo, L., Rui, Z., Yongkai, L., Jun, W., & Hui, C. (2014). Privacy-Preserving Distributed Location Proog Generating System. Security Schemes and Solutions Conference
[10] Niu, B., Zhu, X., Chi, H., & Li, H. (2013). 3PLUS: Privacy-Preserving Pseudo-Location Updating System in Location-Based Services. IEEE Wireless Communications and Networking Conference
[11] Wang, X., Pande, A., Zhu, J., & Mohapatra, P. (2011). STAMP: Enabling Privacy-Preserving Location Proofs for Mobile users. IEEE ACM TRANSACTIONS ON NETWORKING
[12] Zhichao, Z., & Guohong, C. (2015). APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-based Services. IEEE INFOCOM

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)