iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3129

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 III, March 2018- Available at www.ijraset.com

STAMP: Enabling Location Privacy for Mobile Users While Using Public Wi-Fi

Navya Davis[1], Afeefa M .U[2], Aruna T .S[3], Clincy Jose[4], Radhika V .M[5]
[2,3,4,5] *Assistant Professor, University of Calicut, Computer Science Department, I E S College of Engineering, Chittilappilly, Thrissur, Kerala*
[1]*University of Calicut, Computer Science Department, I E S College of Engineering, Chittilappilly, Thrissur, Kerala*

Abstract: Today location based services are becoming more popular. Majority of the applications are based on user's current location. So there may be some malicious users rely on that application. The malicious can access our location. In this paper we propose a Spatial Temporal Provenance Assurance with Mutual Proofs (STAMP). It is used for ad-hoc mobile users generating location proofs in distributed settings. It is accommodating wireless access points and trusted mobile users. It ensures integrity and non-transferability as well as protecting user's privacy. A semi trusted CA is used for cryptographic key distribution as well as guard uses against collusion by a light-entropy based trust model. It's implementation on IoS platform shows that it requires low cost in terms of computational and storage resources.
Keywords: Spatial temporal provenance, cryptographic key, collusion detection, entropy based trust model, privacy.

I. INTRODUCTION

Nowadays location based services are received more attention and popularity. Most of the location based services become sensitive due to sharing of user's current locations. The users share their location with the server and the server performs processing based on the location given by the user and returns back the information or the data or the service to the user. According to the user's current location, there must want to validate the users past location. So here we introduce a location proof scheme for the mobile users at particular time sequences as spatial temporal provenance (STP) of the specified user and digital proof of the user's current location is generated as STP proof. In this paper the introduced scheme is Spatial Temporal Provenance Assurance with mutual proofs (STAMP) [1]. This aims to achieve integrity and non-transferability of location with potential of securing user's location privacy. Most of the location based services relies on wireless infrastructure (e.g.: Wi-Fi APs, GPS) to create STP proof. However it allows spiteful users to fake their location. So we have to use a semi-trusted third party to validate user's location in order to achieve the integrity of the location.

STAMP is based on the distributed architecture. The co-located mobile devices mutually generate STP proofs for each other. In STAMP a distributed system introduce STP proof generation and verification of the protocol to achieve the integrity and non-transferability of the location. So here no additional third parties are needed except a semi-trusted third party CA. It is designed for protecting user's location privacy and anonymity. STAMP is collusion resistant, in which it is implemented prevent the user from collecting proofs on behalf of another user. Here we implement a new additional feature into this scheme as manual timestamp, such as we can manually set up the location where no one can access or get the actual location of the user. For example we can set up location manually such as in classroom or an office instead of public meeting place or a park if the user is in same network.

II. LITERATURE SURVEY

In Zhu et al.'s APPLAUS [2], A Privacy Preserving Location proof Updating System in which the co-located Bluetooth enabled mobile devices will generate the location proofs and upload to the untrusted location proof server. There is a statistically changed pseudonym to protect the location privacy from each other and from untrusted location proof server. By using a user-centric model each users can evaluate their location privacy levels and decide when to accept the location proof requests. The experimental results show that, besides providing location proof, which can preserve the source location privacy.

In Sebastien Gambs et al.'s PROPS [3], a Privacy-preserving location Proof System which allows users to generate location proofs in a private and distributed manner by using witnesses. It provides unforgeability and non-transferability of location proofs and resistance to several attacks. It is purely based on LPS (Location Proof Share) which denotes a timestamped digital signature of the location of a user generated by a nearby user. These LPSs are collected to generate LP (Location Proof) that can exhibit users' current location at particular granularity to a service.

©IJRASET (UGC Approved Journal): All Rights are Reserved

In Davis et al.'s [4], Privacy-Preserving Alibi systems, where a user can hide his or her identity during alibi (location proofs) creation. There are two alibi schemes. In first one, a public entity called alibi corroborator that doesn't need any privacy protection. In second one, protect the privacy of corroborator using cryptographic schemes and which doesn't consider the multi-level location granularity.

Hasan et al.'s [5] proposed system which depends on the location proofs from wireless APs and witness agreements from co-located Bluetooth enabled devices. Users can cast proofs without colluding with wireless APs and other witnesses. It eliminates multiple CAs. To ensure the integrity, it provides Hash chain and Bloom filters.

Veriplace [6] proposed system provides collusion recovery and privacy protection. To avoid collusion, Veriplace requires three types of trusted entities run by different parties. A TTPL (Trusted Third Party for managing Location information), TTPU (Trusted Third Party for managing User information) and CDA (Cheating Detection Authority). Each trusted entity knows user's identity or his or her location. This technique works only if users request their location proofs frequently.

In our paper we propose STAMP (Spatial Temporal Provenance Assurance with Mutual Proofs). It ensures the integrity and non-transferability of the STP Proofs and also protecting users' privacy. It is purely based on distributed architecture. Here we use a semi-trusted CA (Certification Authority) for cryptographic key distribution. It requires low cost of computational and storage resources while implements on iOS platform. We also preferred [7] [8] [9] [10] papers for the reference and getting good conclusion.

III.PROPOSED SYSTEM

We propose an STP proof scheme such as Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP). It ensures the integrity and non-transferability of the location with location proofs for each user. And the proposed scheme also implements a manual timestamp setup feature to provide privacy of user's current location. The existing system may not feasible to all kind of application. Here all users should be within the same network (LAN or MAN or WAN). Our system contributes several advantages such as integrity and non-transferability of STP proofs, high balanced accuracy with appropriate system parameters, which requires only a single semi trusted third party (CA), low computational and storage resources and also achieves security and privacy objectives.

A. Requirements

Security aspects of STP proofs includes integrity and non-transferability. Integrity means no prover can create fake STP proofs by himself/herself/by untrusted third parties. The non-transferability means no prover can assert the ownership of another provers authorized STP proofs. The privacy includes anonymity, pseudonyms and location granularity. An STP proof system needs to be adaptable to enforce location privacy and accommodate localization error. Threat model includes Prover, Witness, Verifier, and Certificate Authority (CA). Prover is a mobile device which tries to obtains location proofs. A witness is a device which is closed with the prover and willing to create STP proofs for the prover. Witness can be trusted or untrusted. CA is a semi trusted server which manages cryptographic credentials for other parties. Two different collusions are there. W-P collusion and P-P collusion.

B. Architecture

Fig.1 illustrates the architecture of our system. A prover and witness communicate each other in ad-hoc mode. Our protocol consists of two primary phases STP proof generation and STP claim and verification. When a prover collects STP proofs from his/her peer mobile devices so we can say that STP proof collection process started by the prover. During first phase, prover getting an STP proof from each witness. Therefore an STP proof collection process may consists of multiple STP proof generations and gives it to the verifier for authentication purpose. Second phase takes place between the prover and verifier. A part of the verification is done by CA.

C. The STAMP Scheme

STAMP protocol includes some preliminaries such as location granularity levels, cryptographic building blocks, Distance bounding etc. Upon receiving the verifier response, verifier performs two additional operations such as zero-knowledge proof and STPR opening. Suppose there are n granularity levels for each location (e.g. an exact geo coordinates). The semantic representation of the location level is standardized throughout the system. It uses the concept of commitments to ensure the privacy of the provers. That means it allows one to commit to a message while keeping it hidden to others. One way hash functions are used for commitment scheme. Since these hash functions are vulnerable to dictionary attacks, we do not use it for privacy protection purposes. A location proof system needs a prover to be securely localized by the witnesses. A distance bounding protocol will serve this purpose. We

©IJRASET (UGC Approved Journal): All Rights are Reserved

have two factors to which determine a user u's collusion like diversity and fairness. Diversity means that the number of different users who have STP proof transaction with u. Fairness means randomness in the distribution of STP proof transactions among all users who have STP proof transactions with user u.

D. Security Policy

We find out the security policies of STAMP protocol which includes the facts that a prover can't create a legitimate Endorsed Proof (EP) without a witness and a prover can't use an EP created for another prover. A prover can't change the spatial or temporal information in an EP. Without colluding with a witness, a prover can't create a legitimate EP without being present at the claimed location at the claimed time. Another fact that a prover and a witness can't find out each other's identity. The lowest location level a verifier learns about a prover is the level that the prover intends to reveal to him/her. CA can't learn any location information about a prover or witness from verifier request. Most interesting fact that trusted users increase the overall trust of the system. And nobody can fake himself/herself as a trusted user.

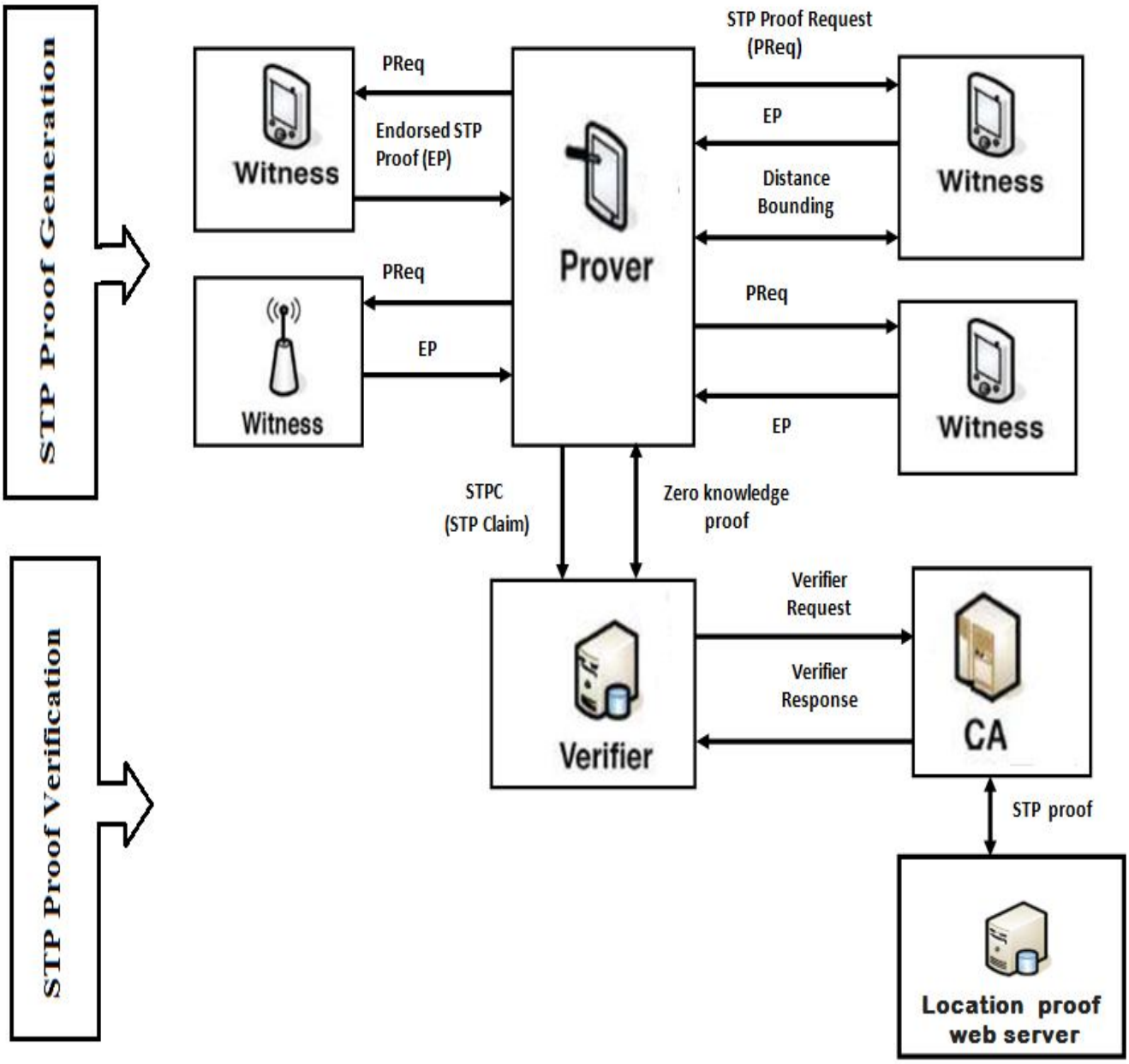


Fig. 1 Proposed architecture.

©IJRASET (UGC Approved Journal): All Rights are Reserved

IV. IMPLEMENTATION

Implementation of software refers to the final installation of the package in its real environment, to the satisfactions intended users and the operation of the system. The people are not sure that the software is meant to make their job easier. We implemented a prototype client application on iOS with swift 3 using the tool kit XCODE 8.2.1. Our experiments are carried out on to iphone 5s later devices equipped with chipset apple A9, CPU 1.85 GHz dual-core 64 bit, RAM 4GB, battery 3.82 V 6.55 W –h Li-Po 150 min charge time, running macOS 10.13. We use cyphertext policy attribute based encryption algorithm and blowfish algorithm for key generation. We implemented the web services using JAVA/J2EE, the software NetBeans 7.2.1 and the database using MYSQL 5.7. And we also host the web services on cloud. We model each location with six levels: exact location, neighborhood, town/city, region/county, state and country, where each level is represented by a name string except that the lowest level also has the geo co-ordinates.

Fig. 2 shows the implementation workflow of the proposed system. Our proposed system consists of five modules such as Login, Registration, Validation, Verification and Analysis. In Login process, the user can be verified according to the existing users or new users or the admin login process. In Registration process the data can be processed related to the user privileges and then the server can be provided and data transmission can be accessed according to the user's authentication. In Validation criteria, data can be analysed by the admin and then the data can be validate according to user authentication. In Verification process, the data can be verified in order to the user's duplication process and then server can be verified related to the user's usage and the data can be transmitted to the process. Finally during analysis phase data can be processed and then the server log files can be removed and past log will be generated related to the usage.

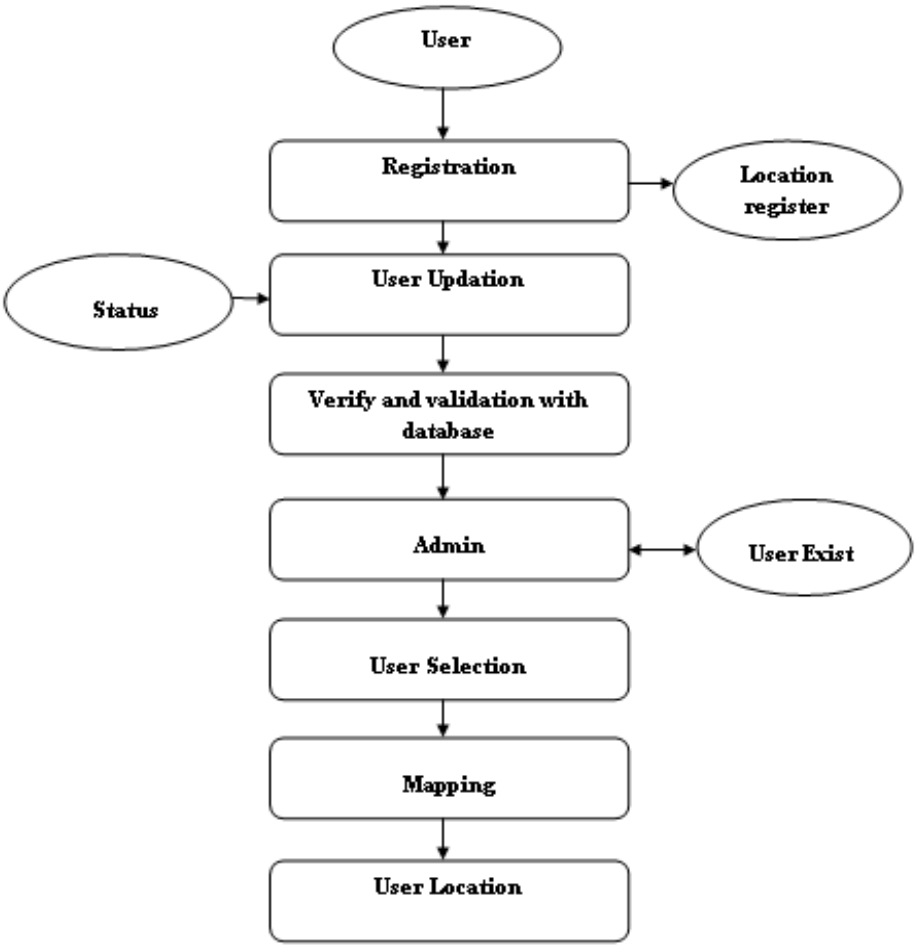


Fig. 2 Implementation Work Flow.

©IJRASET (UGC Approved Journal): All Rights are Reserved

V. CONCLUSIONS

In this paper we proposed STAMP, which assures the privacy and security for mobile users' proofs for their past locations while using public Wi-Fi. The major goals of this paper is integrity and non-transferability location proofs. It maximizes users' anonymity and we can manually set up the time stamp value in order to protect our location privacy from malicious access. For example we can set up location manually such as in classroom or an office instead of public meeting place or a park if the user is in same network. Our implementation on iOS platform shows that STAMP requires low cost of computational and storage resources. The experimental results show that our trust model is able to achieve a high balanced accuracy.

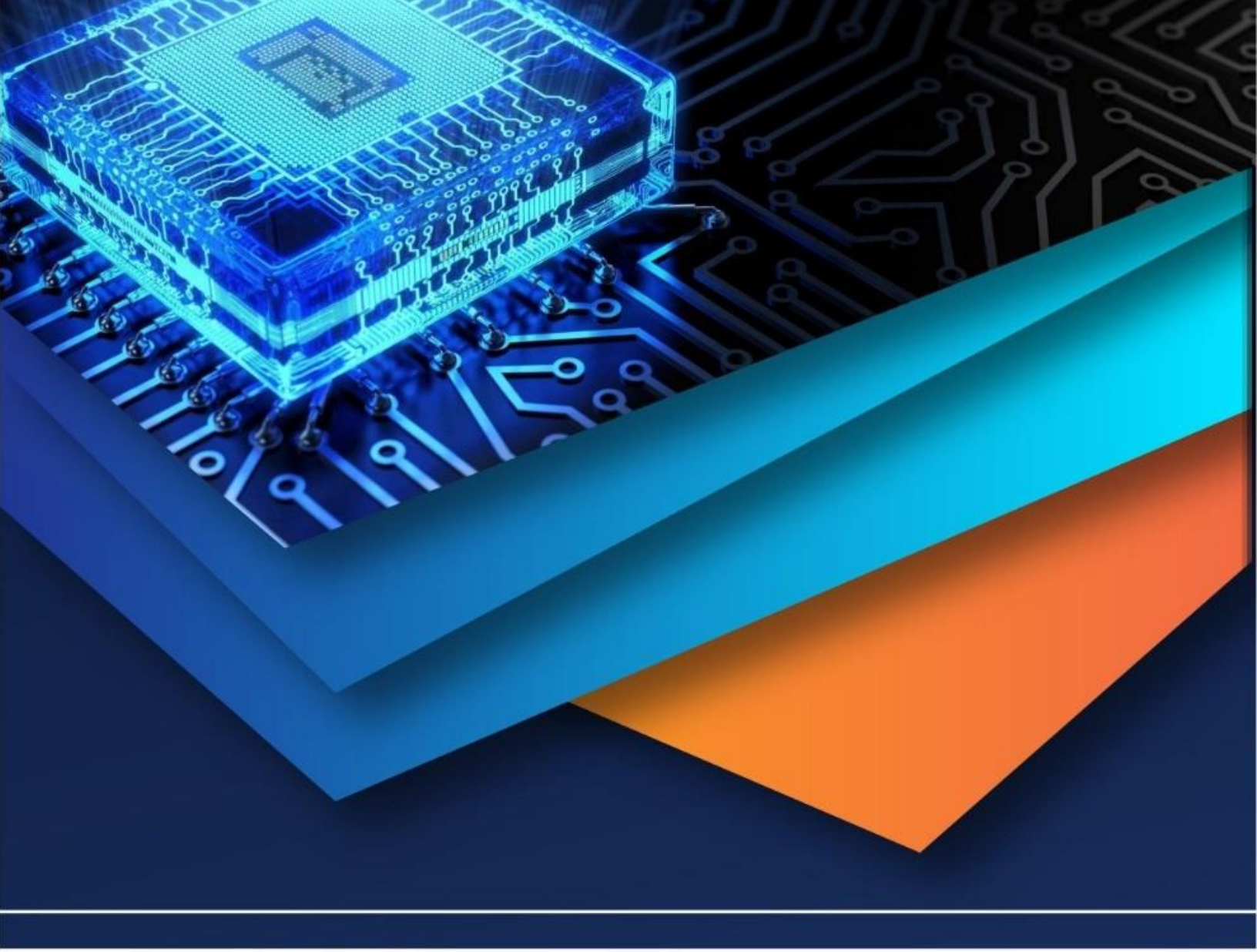
VI. ACKNOWLEDGMENT

We are grateful to Dr.Brilly Sangeetha Head of Computer Science and Department for her timely suggestions, kind guidance and valuable support during this project. We also show our sincere thanks to Ms.Navya Davis who has been guiding us in molding this project into a successful one.
Above all, we are very much thankful to the Lord almighty, the foundation of all wisdom who has been wonderfully guiding us step by step.

REFERENCES

[1] Xinlei Wang, Amit Pande, Jindan Zhu, Prasant Mohpatra, "STAMP: Enabling Location Privacy-preserving Location proofs for Mobile Users.", Dept. Of Computer Science University of California IEEE 2016.
[2] Zhichao Zhu, Guohong Cao, "APPLAUS : Aprivacy –preserving Location proof Updating System for Location –Based Services", Dept. of Computer Science and Engineering, Pennsylvania State University PA 16802.
[3] Sebastien Gambs, Marc-Oliver killijian, Matthieu Roy, Moussa Traore, "PROPS: A PRivacy-preserving Location Proof System", hal-01242266.
[4] B.Davis, H.Chen, M.Franklin, "Privacy preserving alibi Systems", in ACM ASIACCS,2012.
[5] R.Hasan and R.Burns, "Where have you been? Secure Location Provenance for Mobile devices", CORR2011.
[6] W.Luo and U.Hengartner, "VeriPlace: a privacy – aware location proof architecture.", in ACM GIS 2010.
[7] Chen Lyu, "CLIP: Continuous Location Integrity And Provenance For Mobile Phones", IEEE 2015.
[8] Anh Pham, "Secure And Private Proofs For Location Based Activity Summaries In Urban Area".
[9] N.Roy, H.Wang, Chowdary R R, "I am a Smart Phone and I Can Tell My Users Walking Direction",2014.
[10] S.Saroiu and A.Wolman, "Enabling New Multiplications With Location Proofs ",ACM HotMobile,2009.

©IJRASET (UGC Approved Journal): 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)