VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JNANA SANGAMA" BELAGAUM – 590 018

THE PROJECT REPORT ON

" Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System"

Submitted in the partial fulfillment of the requirements for the award of degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

PROJECT ASSOCIATES

ASHRITHA S	4GM10CS002
KAVITHA A	4GM11CS404
NADIYA R	4GM11CS406
RAGHAVI K	4GM11CS412

GUIDE

Prof. KOTRESHI S.N

B.E., M.Tech., M.I.S.T.E.,

COORDINATOR

Prof. KOTRESHI S.N

B.E., M.Tech., M.I.S.T.E.,

HEAD OF DEPARTMENT

Prof. SUNIL KUMAR B.S

B.E., M.Tech., M.I.S.T.E.,

Srishyla Educational Trust ®, Bheemasamudra

G M INSTITUTE OF TECHNOLOGY

#4, P B Road, Davangere –06

2013-14

ABSTRACT

Today's location-sensitive service relies on user's mobile device to determine the current location. This allows malicious users to access a restricted resource or provide bogus alibis by cheating on their locations. 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 send updates 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.An authorized verifier can query and retrieve location proofs from the server.

We also develop user-centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept the location proof requests. In order to defend against colluding attacks, we also present between's ranking-based and correlation clustering-based approaches for outlier detection.

APPLAUS can be implemented with existing network infrastructure, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost. Extensive experimental results show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks.