

# SAPTHAGIRI COLLEGE OF ENGINEERING

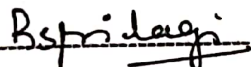
14/5, Chikkasandra, Hesaraghatta Main Road, Bangalore-560057

Department of Computer Science and Engineering

## Certificate



Certified that the project work entitled "A SECURE ID BASED SIGNATURE SCHEME FOR WSNs USING IoT" carried out by BHAGYASHREE.M (1SG13CS026), CHAITHRASHREE.B (1SG13CS030), CHITRA.K (1SG13CS032), DEEPASHREE.G (1SG13CS035), bonafide students of this institute, in partial fulfillment for the award of Bachelor of Engineering in Computer Science and Engineering of Visvesvaraya Technological University, Belgaum during the academic year 2016-17. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the department library. The project report has been approved as it satisfies the academic requirements in respect of Project work [10CS85] prescribed for the said degree.

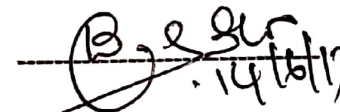


13.06.2017

Signature of the Guide

Mr. Rajeev Bilagi

Associate Professor



Signature of the HOD

Dr. C.M. Prashanth

Professor and Head



Signature of the Principal

Dr. Ashwatha Kumar M

Principal

Name of the Examiners

1.....

2.....

Signature with date

.....

.....

## ABSTRACT

The wireless sensor network is one of the highly anticipated key contributors of the big data in the future networks. Wireless sensor networks (WSNs), with a large number of cheap, small and highly constrained sensor nodes sense the physical world, has very broad application prospects both in military and civilian usage, including military target tracking and surveillance, animal habitats monitoring, biomedical health monitoring, critical facilities tracking. However, the technique still has the inherent security problems, such as eavesdropping, reply attacks, data forge and data tampering, etc. Hence, designing a secure data aggregation method is very significant for WSNs. The security proof indicates that our ID based aggregate signature scheme for wireless sensor networks can ensure the integrity of the data and reduce the communication and storage cost. The detailed security proof is given based on the computational Diffie-Hellman assumption in random oracle mode