

SAPTHAGIRI COLLEGE OF ENGINEERING

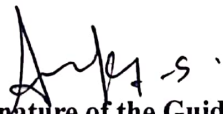
14/5, Chikkasandra, Hesaraghatta Main Road, Bengaluru - 560057.

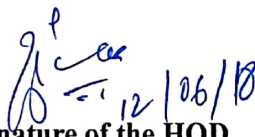
Department of Computer Science and Engineering

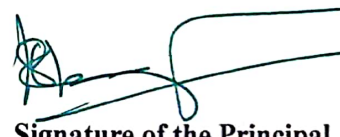


Certificate

Certified that the Project Work entitled **"ANALYSIS OF NETWORK TRAFFIC AND SECURITY THROUGH LOG AGGREGATION"** carried out by **BHOOMIKA.H (ISG14CS019)**, **ANANYA BANDYOPADHYAY (ISG14CS012)**, **ISHAN SINGHANIA (ISG14CS034)**, **KRUPAL SHAH (ISG14CS045)**, bonafide students of Sapthagiri College of Engineering, in partial fulfillment for the award of Bachelor of Engineering in Computer Science and Engineering of Visvesvaraya Technological University, Belagavi during the academic year 2017-2018. 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.


Signature of the Guide
Arun Kumar S
Asst. Professor


Signature of the HOD
Dr. Yogish H K
Professor & Head of the Department
Computer Science Engineering
Sapthagiri College of Engineering
Bangalore-57


Signature of the Principal
Dr. K L Shivabasappa
Principal

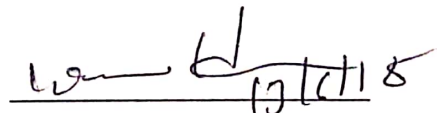
EXTERNAL EXAMINATION:

Name of the Examiners

1. K. Ramakrishna

2. Ramanagouda S. Patil

Signature with Date


12/6/18


12/6/18

ABSTRACT

With the tremendous growth in Internet-based applications, there has been a steady elevation in the cyber world based accommodations such as websites, email, web portals, portlets, API etc. With the increase in growth of Internet-based applications, the threat landscape has incremented manifolds. The number of attacks on IT infrastructure has also increased spontaneously. The increase in the infrastructure has posted the assessment of maleficent invasion as a major challenge. To amend the security ecosystem it is desirable to have a complete security solution that covers all verticals and horizontals of the threat landscape. This paper proposes to have a wholesome security ecosystem for the huge amount of websites from malignant attacks and threats, to increase knowledge about traffic patterns and trends and also to perform authentic time decision on maleficent traffic. Log analysis is the art of making sense out of computer-generated records (i.e. logs). A technique is evolved for log aggregation and analysis in authentic time through a dashboard and terminal exhibit. It is performed with the help of user interactive displays, real-time alerts are generated based on conditions, and preventive actions can be taken based on those alerts.