

SAPTHAGIRI COLLEGE OF ENGINEERING

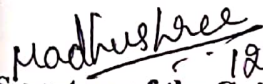
14/5, Chikkasandra, Hesaraghatta Main Road, Bengaluru - 560057.

Department of Computer Science and Engineering




Certificate

Certified that the Project Work entitled **"PROVIDING SECURITY TO CLOUD DATA USING KEY EXPOSURE"** carried out by **DINESH KUMAR (ISG14CS027), DIVESH KUMAR (ISG14CS043), KAWALJEET SINGH (ISG14CS043), KUMAR PIYUSH (ISG14CS047)**, 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
Madhu Shree
Assistant Professor


Signature of the HOD
Dr. Yogish H K
Professor & Head
Department of Computer Science & Engg.
Sapthagiri College of Engineering
14/5, Chikkasandra, Hesaraghatta Main Road,
Bengaluru-560 057.


Signature of the Principal
Dr. K L Shivabasappa
Principal


EXTERNAL EXAMINATION:


Name of the Examiners

1. balasim cob...

2. Ramanagouda. S. pahl

Signature with Date

 13/6/18

 13/6/18

ABSTRACT

Attackers break data confidentiality by acquiring cryptographic keys, by means of coercion or backdoors in cryptographic software. If the encryption key is exposed, data confidentiality is tough to preserve. The only way is to limit the attacker's access to the cipher text. The cipher text can be spread across servers in multiple administrative domains, assuming the adversary cannot compromise all of them. But if the existing schemes are used for data encryption, an adversary equipped with the encryption key can still compromise a single server and decrypt the cipher text blocks stored therein. In our paper we propose Bastion , a novel and efficient scheme that guarantees data confidentiality even if the encryption key is leaked and the adversary has access to almost all the cipher text blocks .We analyze the security of Bastion and evaluate its performance by means of a prototype implementation . Our evaluation results suggest that Bastion is well-suited for integration in existing systems.