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 **"Identity Based Two Server Password Authenticated Key Exchange Protocol"** carried out by **R SUSHMA (1SG13CS077), VYSHAK M.V (1SG13CS127), BHARATH R (1SG14CS406), VEDA KUMAR B.H (1SG13CS421),** 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 progress 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	Signature of the HOD	Signature of the Principal
Prof. Chethan M	Dr. Prashanth C.M	Dr. Aswatha Kumar M
Assistant Professor	Professor and Head	Principal

Dr. Aswatha Kumar. M
Principal
Sapthagiri College of Engineering
No. 14/5, Chikkasandra,
Hesaraghtta Main Road,
Bangalore-560 057

Name of the Examiners	Signature with date
1.....	.....
2.....	.....

ABSTRACT

In two-server password-authenticated key exchange (PAKE) protocol, a client splits its password and stores two shares of its password in the two servers, respectively, and the two servers then cooperate to authenticate the client without knowing the password of the client. In case one server is compromised by an adversary, the password of the client is required to remain secure. In the proposed application, we present two systems that transform any two-party PAKE protocol to a two-server PAKE protocol on the basis of the identity-based cryptography, called ID2S PAKE protocol. We construct ID2S PAKE protocols which achieve implicit authentication. As long as the underlying two-party PAKE protocol and identity-based encryption or signature scheme have provable security without random oracles, the ID2S PAKE protocols constructed by the compilers can be proven to be secure without random oracles. Compared with the existing two-server PAKE protocol with provable security without random oracles, our ID2S PAKE protocol can save from 22% to 66% of computation in each server.