Apr - Jun © 2016 Transactions; 3(10): 427-433

International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

Research Article

A Security Protocol for mobile-banking and payment using SMS and USSD in Ethiopia

[1] Ramesh Gadde, [2] Kifle Berhane. N and [3] Fthi Arefayne Abadi

Corresponding Author:
gadde.padma22@gmail.com

DOI:
http://dx.doi.org/10.17812/IJRA.3.10(72)2016

Manuscript:
Received: 9th Apr, 2016
Accepted: 15th May, 2016
Published: 28th June, 2016

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

Short message service (SMS) and Unstructured Supplementary Services Data (USSD) are a very popular and easy to use communications technology for mobile phone devices. Originally, these services were not designed to transmit secured data, so the security was not an important issue during its design. Yet today, it is widely used to exchange sensitive information between communicating parties i.e. HelloCash, Ethio Gebeta, Lehulu, CBE M-banking, 8100, 8400 and so much more. Due to the vulnerable nature of SMS and USSD this paper proposes an alternative solution that provides a client-server SMS and USSD security protocol that guarantees provision of confidentiality, authentication, integrity, non-repudiation, and file compression security services. A hybrid cryptographic scheme is used which combines the Identity Based Encryption (IBE) and AES-Rijndael algorithms without key distribution servers and certificate authorities to achieve more robust functionality. HMAC-SHA256 hashing algorithm will be used to generate a message digest. IBE will be used to digitally sign the message and to encrypt the encryption key used on AES. LZW compression will be used to compress the SMS. Unlike any previous works that involve certificate authority and key management, this protocol is proposed to be used in mobile banking and payment once a user successfully subscribes to the service.

Keywords: USSD, HelloCash, IBE, HMAC-SHA256.

[1 2 3] Department of CSE, Mekelle Institute of Technology, Mekelle University, Tigray, Ethiopia.

IJRA - Year of 2016 Transactions:
Month: April - June
Volume – 3, Issue – 10, Page No's: 427-433
Subject Stream: Computers

Paper Communication: Author Direct

Paper Reference Id: IJRA-2016: 3(10)427-433