Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Implementation of Secure Anonymous Key for Bank System Processes

P. Annapurnamma[1], Sk. Javed Akthar[2], T. Alekhya[3], S. Surendra[4], P. V. S. Sherma[5]
[1, 2, 3, 4] Pursuing B.Tech (CSE) from St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh, India
[5] Working as Associate Professor (CSE) in St. Ann's College of Engg. & Technology, Chirala, Andhra Pradesh, India

Abstract: ***Establishment of secure communication sessions has become an important issue for smart grid environments. In order to support secure communications between smart meters and service providers, key management for authentication becomes a crucial security topic. Recently, several key distribution schemes have been proposed to provide secure communications for smart grid. However, these schemes do not support smart meter anonymity and possess security weaknesses. This project utilizes an identity-based signature scheme and an identity-based encryption scheme to propose a new anonymous key distribution scheme for smart grid environments. In the proposed scheme, a smart meter can anonymously access services provided by service providers using one private key without the help of the trusted anchor during authentication. In addition, the proposed scheme requires only a few of computation operations at the smart meter side. Security analysis is conducted to prove the proposed scheme is secure under random oracle model.***

Keywords: Identity-based encryption, identity-based signature, key distribution, privacy, smart grid.

I. INTRODUCTION

AN IMPLEMENTATION OF SECURITY ANONYMOUS KEY FOR BANK SYSTEM PROCESSES is support and manage information among various stake holders in smart grid domains. To establish secure communication session has become an important issue for smart grid environments. So we utilize an identity-based signature schemes and an identity –based encryption scheme to propose a new anonymous key distribution scheme for smart grid environments. So the smart grid is an advanced metering infrastructure for automatically gathering and utilizing information. This new infrastructure makes more efficient, secure and reliable through bidirectional transmission flows and data communication.

A smart gird usually contains four components 1) sensing 2) communication 3) control and 4) actual systems. This way we are going to implement key Distribution scheme for smart grid. Usually, end users devices for smart grid such as smart meter are composed of sensing and communication, control, and actuation modules. Key management schemes generally are divided in to two categories 1) public key infrastructure for key management and 2) symmetric key management.

II. RELATED WORK

II.I Existing System with Drawbacks

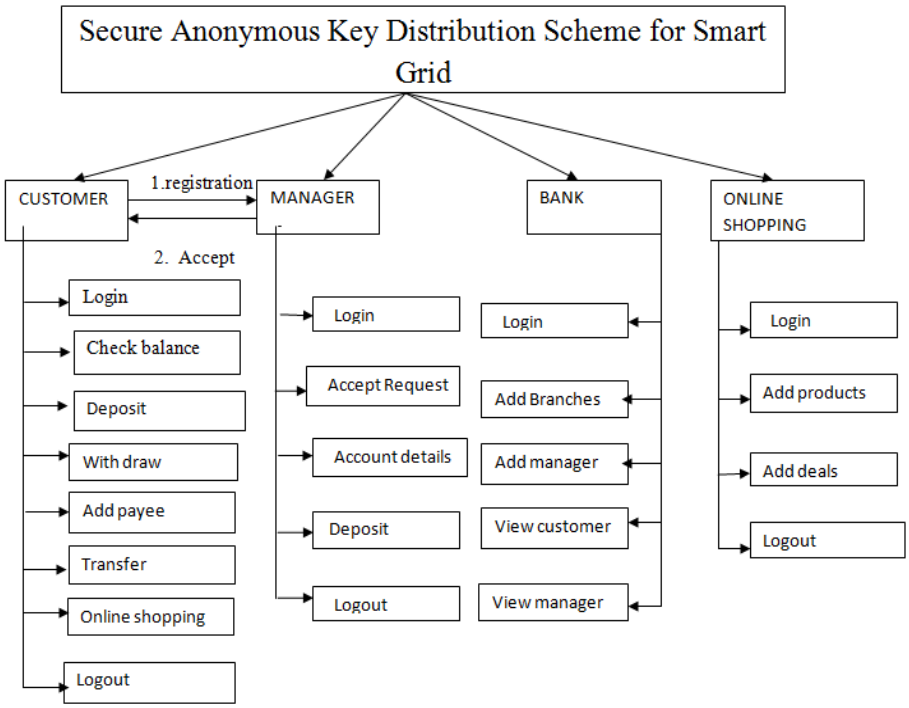
Comparisons on security and efficiency among the proposed scheme and other existing ones indicate that the proposed scheme is secure without sacrificing performance efficiency. To fully support information management among various stakeholders in smart grid domains, how to establish secure communication sessions has become an important issue for smart grid environments. A smart grid consists of a power network composed of intelligent nodes that can operate, communicate and interact autonomously, in order to efficiently deliver electricity to the customers. This heterogeneity in architecture of a smart grid motivates the use of advanced technology for overcoming various technical challenges at different levels. The drawbacks of database with the tuple data does not be maintained confidentially.The existing systems another person to easily access database.

II.II Proposed System with Features

Provide secure communications for smart grid. However, these schemes do not support smart meter anonymity and possess security weaknesses. This paper utilizes an identity-based signature scheme and an identity-based encryption scheme to propose a new anonymous key distribution scheme for smart grid environments. In the proposed scheme, a smart meter can anonymously access services provided by service providers using one private key without the help of the trusted anchor during authentication. In addition, the proposed scheme requires only a few of computation operations at the smart meter side. Security analysis is conducted to prove the proposed scheme is secure under random oracle model. The proposed key distribution scheme utilizes identity-based cryptosystems to fulfill anonymous secure communication between two communicating parties. In recent years, several identity-based authenticated key agreement protocols have been proposed. These protocols allow two parties to authenticate each other and share a session key after authentication.

The advantages of anonymity of DB are not affected by inserting the records. We provide security proofs and experimental results for both protocols.

III. SYSTEM ARCHITECTURE



IV. MODULE WISE FUNCTIONAL REQUIREMENTS

The following are the module wise functional requirements of our project. They are:

1. Bank Module:

The main role of BANK is to add products in the site and if any products are not sold by anyone that are removed from site and update the new products, view the customer sales. Provide security for user account and transactions.

2. Manager Module:

It Accept user registration request and maintain transaction

3. Customer Module:

Manual sever blocks the user who has been casted their vote through online otherwise permits the user to cast the vote. Comparison shopping and product selection on various attributes in terms of price and placement of order and authorization of payment.

4. Online Module:

In this module shop owner can add the products and daily deals with offers and manage the purchase and delivery

V. RESULTS

Index Page:

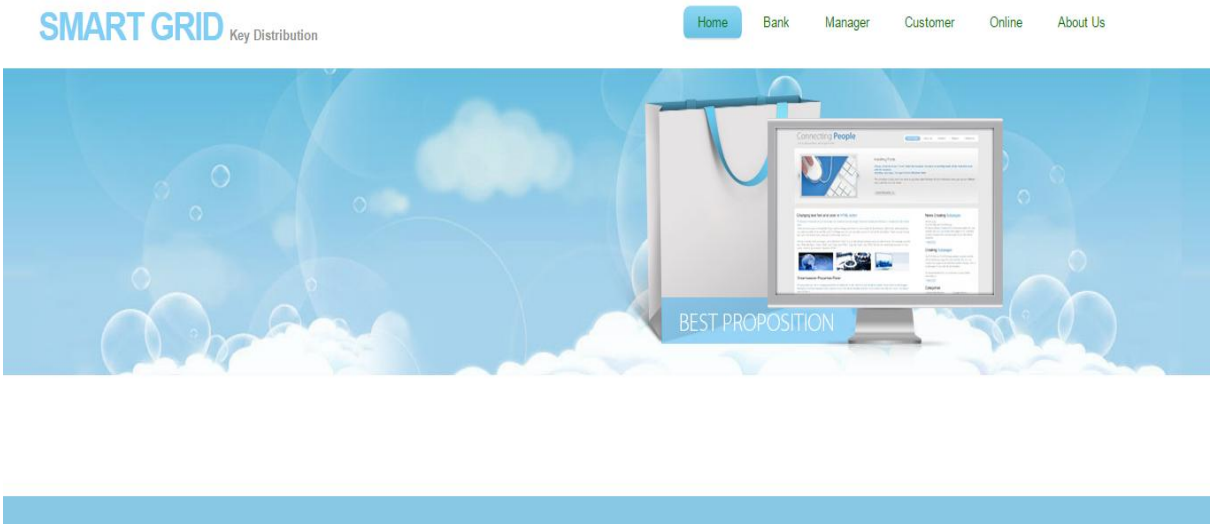


Fig. Index Page

Customer Registration Page

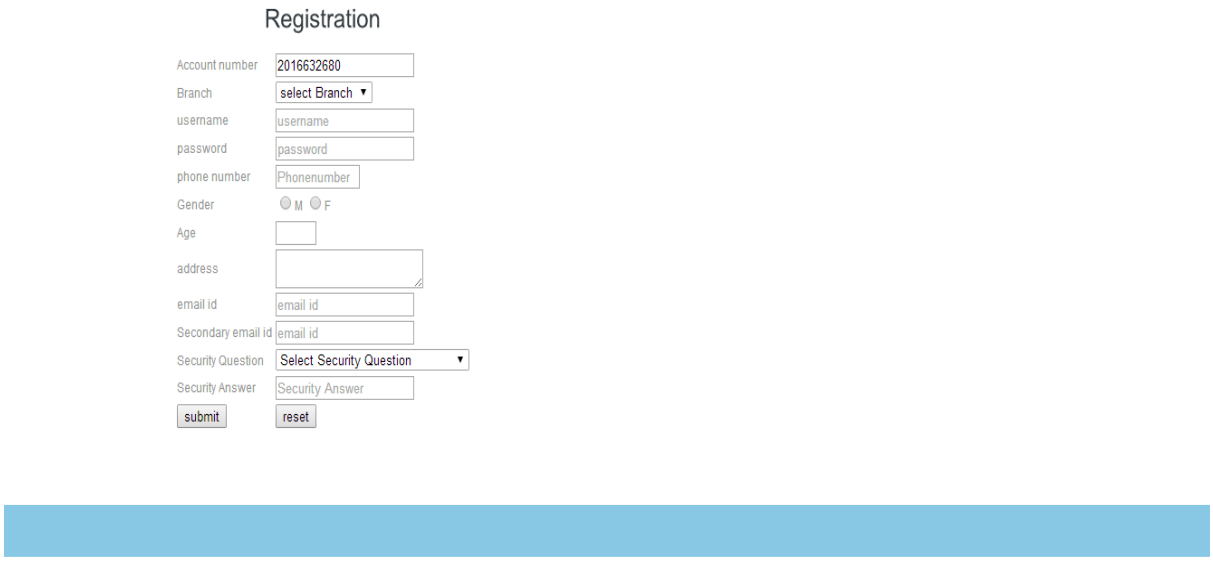


Fig. Registration Page

Add Manager Page

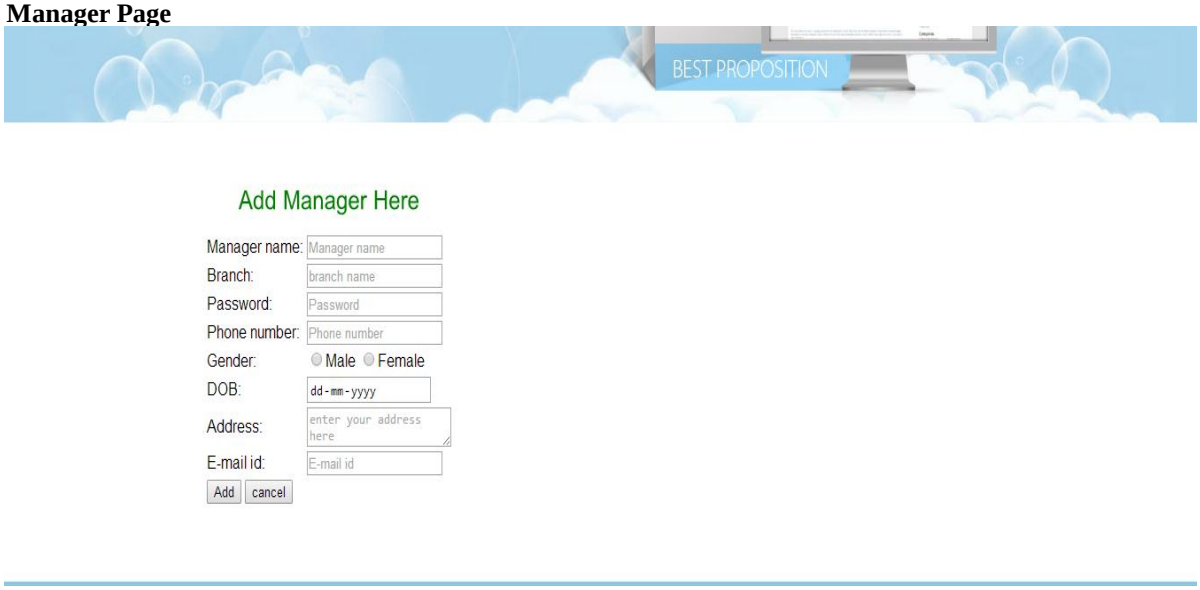


Fig. Add Manager Page

Online Product Page

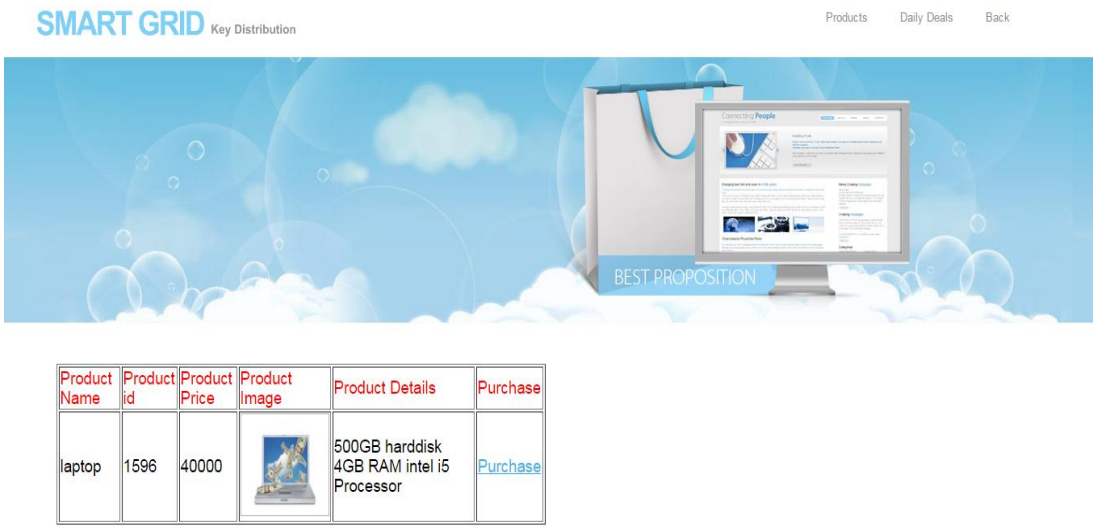


Fig. Online Product Page

VI. PROCEDURE

1) Registration

This module provides the user to register/create an account himself/herself on the website by providing proper details it will provide the common and unique ACCOUNT NUMBER.

2) Bank Login

After registration the banker can login using the Username and password .In this module banker can add manager and branches. In this banker maintain transactions.

3) Manager Login

After registration the banker can login using the Username and password .In this module banker can add manager and branches. In this banker maintain transactions.

4) Online Shopping Login

In this module shop owner can add the products and daily deals with offers.

VII. CONCLUSION & FUTURE SCOPE

This project introduced a new secure key distribution scheme for smart grid environments. The proposed scheme allows a smart meter to anonymously access services from service providers with one private key. The advantage of the proposed scheme is that a smart meter can be quickly authenticated by responding service providers without involving the trusted anchor, because two identity-based cryptosystems are adopted in our scheme. Unlike other existing schemes, the proposed scheme supports mutual authentication and smart meter anonymity. We also conduct security analysis to prove the proposed scheme is secure under random oracle model. The next generation of metering and data exchange technologies, known as advanced meter infrastructure (AMI) technologies is a cornerstone and one of the most visible element of the smart grid.

REFERENCES

[1] H. Krawczyk, "HMQV: A high-performance secure Diffie–Hellman protocol," in Proc. CRYPTO, Santa Barbara, CA, USA, 2005, pp. 546–566.

[2] R. Sakai and M. Kasahara, "ID based cryptosystems with pairing on elliptic curve," Cryptol. EPrint Archive, Report 2003/054, 2003. [Online]. Available: http://eprint.iacr.org/2003/054.pdf [3] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in Advances in Cryptology—ASIACRYPT. Berlin, Germany: Springer-Verlag, 2005, pp. 515–532.

