IJRRECS/August 2014/Volume-2/Issue-8/2903-2907 **ISSN 2321-5461**

**INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE**

# MANAGING OF TRUST DELEGATION FOR ACCESSING AGENTS

**Revathi Thota[1], A.Ugendhar[2]**

**[1]M.Tech Student, Dept of CSE, Aurora's Scientific And Technological Institute, Aushapur(V), Ghatkesar(M), R.R Dist, T.S, India**

**[2]Associate Professor, Dept of CSE, Aurora's Scientific And Technological Institute, Aushapur(V), Ghatkesar(M), R.R Dist, T.S, India**

## ABSTRACT:

In the latest advanced technology privacy plays a crucial role and plays a one of the challenging task under the environment of the smart grid. Here many of the several previous existing methods are facing the problems of the privacy and unable to rectify the complete problem and this is a major concern from the user based perspective. Here in order to overcome the problems of the several previous methods here a new technique based on the phenomena of the novel approach where the performance of the system is improved by the proper design of the challenging task in a well efficient manner respectively. Here the proposed technique is designed by the name of the novel scheme related to the key management by the integration of the technique oriented with respect to the elliptic curve followed by the technique related to the symmetric key in a well efficient manner respectively. Here there is a problem after the privacy that there may be a chance that the system may gets effected by the threats and some of them includes attack of the mid man followed by the replay. Therefore the main aim of the proposed designed scheme is initially to provide the security that is the maintenance of the privacy based user followed by the effective detection of the attacks is a major concern respectively. Some of the merits of the present designed technique includes the efficiency, accessibility and fault tolerance respectively. Experiments have been conducted on the present method where in order to improve the performance for the system in terms of the outcome of the entire system a test bed consisting of the large number of the datasets in a well oriented fashion respectively.

***KEYWORDS: Smart grid, Smart meter, Data infrastructure, Fault tolerance, Security, Privacy, Data authentication, Scalability, Accessibility, Efficiency, Shelf oriented commercial (SOC), Design security and management scheme respectively.***

## 1. INTRODUCTION:

In the rapid advancement related to the field of the science and technology plays a crucial role in its applicability the Information technology and its convergence takes place by the help of the design of the well effective semantic of the power grid. Engineering related to the communication followed by the strategy of the power system plays a crucial role for the provision of the power system under the electrical phenomena related to the robust and the flexible scenario respectively [1]. The specification of the concept related to the smart grid implies that the communication under the bi directional strategy followed by the intelligence metering real time power grid facilitation for the users for the purpose of the applications or the appliances of the home. Therefore due to the advancement in the technology of the smart grid it plays a crucial role in the society that is many of the customers are getting attracted to it by which its design oriented strategy includes the reduction of the complexity followed by the well effective utilization of the system in an accurate manner respectively [2][3]. Here the power grid oriented power transformation takes place in the system from the scenario of the bi directional strategy. Here there is a design of the well effective system where the grid plays a crucial role for the transmission and the receiving of the power through the customer based perspective respectively [4]. The major role of the smart grid includes the structural scenario of the control and the communication followed by the sensing etc.

**BLOCK DIAGRAM**

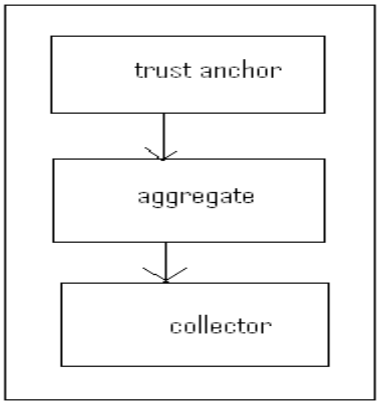


**Fig 1: Shows the block diagram of the present method respectively**

## 2. METHODOLOGY:

In this paper a design of the well effective technique related to the smart grid is a major concern which involves the reduction of the complexity and the efficient utilization of the services or even its accessibility for the sake of the home appliances for the customers respectively. Here the implementation of the present method is shown in the above block diagram and is explained in an brief theoretical fashion respectively [5][6]. Here in the design of the present system oriented strategy a scheme of the authentication is proposed where the advancement in the data encryption strategy involves the scenario of the technique of the cryptography under the public key elliptic for the implementation of the protocol of the Needham Schroeder phenomena is a major concern. Here the implementation of the protocol takes place by the help of the anchor trust under the employment of the public key and its establishment in the symmetric strategy respectively. Here the mechanism of the sensors are involved by the help of the trust oriented sensor for the agents based local grid access [7][8]. Here the delegation base on the public key are verified by the collector in a fast manner by which there is an efficient filtering of the data under the attackers of the DOS is a major concern respectively. Here the private key is issued by the help of the sensors and the key based on the private basis plays a crucial role under the certification of the anchors trust for the design of the setup under the initial strategy respectively [9].

## 3. EXPECTED RESULTS:

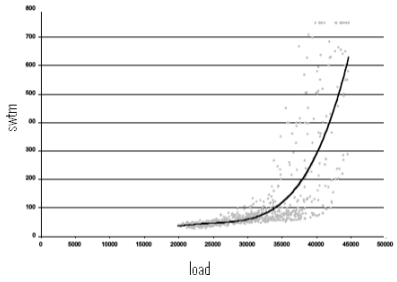


**Fig 2: Shows the graphical representation of the present method respectively**

A comparative analysis is made between the present method to that of the several previous methods are shown in the above graphical representation [10]. Here the present method completely overcomes the drawbacks of the several previous methods in a well oriented fashion by which it completely analyzes the problems of the several previous methods and in a sequential manner so that the same faults can't be repeated in the present method by which the performance of the present method is

improved in a significant manner respectively. Here the implementation of the present method is effective in terms of the following illustrations and includes the scenario of the conditions of the scalability is a major concern respectively. Here the sensors oriented with the strategy of the low power of the single transmission followed by the reception plays a crucial role for the basis of the authentication mutually in between the scenario of the aggregator and the sensor respectively. Secondly the design of the authenticated protocol of the Needham Schroeder plays a crucial role for the purpose of the anchor based trust redirection under the scenario of the cross realm respectively. And the system up to which is somewhat ineffective by which it is got effected by the attacks under the service is a major concern respectively. Here the certificates are design based on the independent strategy for the purpose of the key related to the private and the public is a major concern respectively. Here we finally conclude that the present method is effective and efficient in terms of the performance followed by the outcome of the entire system in a well oriented fashion respectively.

## 4. CONCLUSION:

In this paper an effective advanced technique is implemented where the key challenge is the privacy followed by the preservance of the data from the attacks is a major concern. Therefore many of the several previous methods are unsatisfactory in the above implementation of the couple of tasks in a well oriented fashion for the design of the smart grid respectively. Here the design of the management scheme related to the key in which it is proposed for the smart grid and its utilization in a well effective manner. Here the proposed method is designed under the scenario of the infrastructure of the public key and the secured protocol of the Needham Schroeder plays a crucial role in its privacy based implication respectively. Here there is an analysis of the several advancement in the system based strategy of the keys under the session of the vulnerabilities followed by the communication is a major concern. Here the advancement in the techniques includes the scenario of the utilization of the rule on time followed by the generation of the key based fly respectively. There are a lot of merits for the proposed present method in which it includes the scenario of the scalability, security followed by the strategy of the

tolerance of the faults in terms of the efficiency and accessibility respectively.

## REFERENCES

[1] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols," in 43rd Hawaii Intl. Conf. on System Sciences, Jan. 2010.

[2] B. C. Neuman and T. Ts'o, "Kerberos: an authentication service for computer networks," IEEE Communications Mag., vol. 32, no. 9, pp. 33–38, 1994.

[3] S. M. Bellovin and M. Merritt, "Limitations of the Kerberos Authentication System," ACM Computer Communication Review, vol. 20, no. 5, pp. 119–132, Oct. 1990.

[4] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," Communications ACM, vol. 21, no. 12, pp. 993–999, Dec. 1978.

[5] D. E. Denning and G. M. Sacco, "Timestamps in key distribution protocols," Communications ACM, vol. 24, no. 8, pp. 533–536, Aug. 1981.

[6] C. Tang and D. O. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks," IEEE Trans. Wireless Comm., vol. 7, no. 4, pp. 1408–1416, April 2008.

[7] I. Cervesato, A.D. Jaggard, A. Scedrov, J.-K. Tsay, C. Walstad, "Breaking and Fixing Public-Key Kerberos," Information and Computation, vol. 206, no. 2-4, pp. 402–424, Feb.-April 2008.

[8] D. Dolev and A. C. Yao, "On the security of public key protocols," IEEE Trans. Inform. Theory, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[9] M. Mambo and K. Usuda and E. Okamoto, "Proxy signatures for delegating signing operation," in 3rd ACM CCS, 1996, pp. 48–57.

[10] R. Molva, D. Samfat and G. Tsudik, "Authentication of mobile users," IEEE Network, Special Issue on Mobile Communications, vol. 8, no. 2, pp. 26–34, 1994.