ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Key Management Mechanism and Authentication Impact on Network Layers

Jadhav Neelkanthrao, Dhiren kumar Dalai

PG Scholar, Dept of CSE, Turbomachinery Institute of Technology& Sciences, Hyderabad, India

Assistant Professor, Dept of CSE, Turbomachinery Institute of Technology& Sciences, Hyderabad, India

ABSTRACT**:** A smart grid is a generic label of integrated networks that consists of many subsystems for the application of computer intelligence and networking abilities, all working together as a system of systems, which can be attacked remotely. Hence security has been identified as the most challenging issues in SG development, and designing a smart grid server that consist of gridlets, machines and resources with the impact of network attack on the it is the first important step. Later it is followed by attack identification and mutual authentication scheme of PKI. The existing system provides security to the authentication server using PKI infrastructure mechanism by utilizing an initial password to the registered users in SG. PKI uses identity based scheme (public key distribution scheme) for generation of complex values of every users after validation. We propose an efficient key management protocol based on enhanced identity-based cryptography with multicast key mechanism and enhanced its security via EAP based unified key management function across multiple protocols within the same communication layer. The proposed mechanisms are capable of preventing various attacks. The improved efficiency for key management and EAP is carried by refreshing all public/private key pairs as well as multicast keys using encryption/decryption by the key generator entity. Finally security achieved and performance analyses are calculated to demonstrate the beneficial impact of proposed system against existing one.

KEYWORDS: Sgkm- smart grid key management, enhanced identity based cryptography, public key infrastructure, source multicast key.

I. INTRODUCTION

Providing a high level of security is one of the most important and challenging topics in the smart grid (SG) design. SG is a combination of different systems and subsystems and is vulnerable to various attacks that may cause different levels of harms to the devices. A reasonable level of the data communication security and privacy is one of the most important area in the smart grid (SG) design that needs enough attention.

Information technology (IT) security and data communication security to be more precise, has different aspects, for instance Authentication, Authorization, Integrity and Confidentiality. The first step of designing and implementing a reasonable security is providing an scheme for the authentication. Parties/Nodes should be able to authenticate each other prior to any other data communication. Secure communications generally employ cryptographic keys for encrypting/decrypting data messages. Public Key Infrastructure is preferred for securing data exchanges over SG. Based upon the identity-based signature scheme proposed ID-based cryptography (IBC) for encryption–decryption and key management which extends PKI by replacing the public key of an entity with a function of the entity’s ID to reduce the over-head of public key distribution.

Smart grid key management provides an efficient key management protocol for SG communications using PKI. It employs enhanced IBC (EIBC) scheme to substantially reduce the overhead of key renewals. The security analysis shows that these schemes are capable of preventing various well-known attacks such as brute-force, replay, MITM and DoS.

Unified key management function (UKMF) across multiple protocols within the same communication layer or across different communication layers which refers to application-layer and link-layer protocols, this concept is generally

DOI: 10.15680/ijircce.2015.0306141

applicable to any protocol requiring a cryptographic operation at any communication layer. Ideally, there should be only one UKMF across all protocols with ciphering mechanisms. This is referred to as the fully unified model. EAP based key management framework supports bootstrap ciphering of multiple protocols which focus on the use of the EAP key management framework because it is being used for existing access technologies such as Ethernet, Wi-Fi and WI-MAX networks.

Detection System (IDS), Secure Group Communication and clustering along with trust computation but while focusing on developing such a system for MANET, energy of the particular node has to be considered as an important factor along with the packet delivery ratio, total number of packets sent divisible by total number of packets received by the receiver. Since MANET is energy constrained environment.

The remainder of this paper is organized as follows: Section 2 gives an overview of work that are related Section 3 describes the system architecture. Section 4 presents the experiments and evaluation. Conclusion and future work are given in the final section.

II. RELATED WORK

Wu and Zhou [1] proposed a new key management scheme for the smart grid. In their scheme, they combine both of PKI and a third trusted anchor, which will essentially increase the complication for the smart grid because their protocol at least needs two different kinds of servers for PKI and the trust anchor respectively. Wu and Zhou’s key management scheme for the smart grid and shows that the scheme they claimed to be secure against the man-in-the-middle attack is vulnerable to this attack. Like an authentication scheme in a Kerberos system, a trusted third party (e.g., trust anchor) is involved in the process of authentication as well.

Bartoli, Hernandez-Serrano, Soriano, Dohler, Kountouris, and Barthel [2] worked on a communication protocol for Smart Meters. These networks are typically composed of resource-constrained devices. The authors use data aggregation in the network to efficiently deliver the data to a gateway. The contribution of the work is a lossless data aggregation protocol that has a security-to-communication trade-off.

Khurana, Bobba, Yardley, Agarwal, and Heine [3] proposed a set of design principles to use when designing Smart Grid authentication protocols. The motivation for their work was to propose a set of guidelines that could be used by protocol designers to develop authentication protocols with less vulnerability. The contribution of the work is a set of design principles that can be used when creating authentication protocols in the Smart Grid. The design principles are based off of principles used when designing Internet-based authentication protocols.

F. Zhao and Y. Hanatani provided [4] an authentication schema for the MANET communication that is an Identity-Based. They used node IP address as the node ID to sign the OLSR routing protocol header excluding Time-To-Live (TTL) and Hope Count (HC), in order to provide a source authentication. Each intermediate node, first checks packet origin aiming the source public key, then verifies TTL and HC and then updates them accordingly. Finally, TTL and HC are signed with the node private key and packets are forwarded to the next hop. They also proposed the system secret key generation process and updating.

X. He, M. Pun, and C. Kuo [5] worked on simulating network communications and power systems. The motivation for this work was to perform an analysis on the impact of communication failures in the Smart Grid. This was accomplished by integrating Open DSS.

A network communication simulator. The contribution of is a co-simulation model that can be used to analyze communication failure impacts on the Smart Grid. The simulator was run on power configuration with a solar power source that had several small-scale storage batteries. The storage batteries are used to offset the variable voltage output of the solar power source. The simulator was used to analyze the power system impacts caused by communication failures. The benefit of this work is that it is using two exiting simulation models and combining them to predict Smart Grid behaviours.

H.K. Oh and S.H. Jin [6] discusses Open ID standard and how enterprise style SSO concept can be copied to open Internet where several identity providers are working and managing their own users and identities. It also discusses about extendibility and suitability of Open ID, issues it may raise and if it can meet the future requirements and is it sufficient in general to act as a SSO protocol for Internet.

S. Das, Y. Ohba, M. Kanda, D. Famolari, and S. Das [7] proposed environments in which current electric grids operate as well as the requirements for the emerging smart grid differ substantially from those of today's Internet and telecommunication networks. we present a smart grid key management framework with application to AMI networks. Specifically, we describe how this key management model can be realized in such a resource-constrained environment using existing standard protocols and provide preliminary performance results.

III. SCOPE OF RESEARCH

Different viruses or attacks such as brute-force and dictionary attacks can target the data security and confidentiality. The Stauxnet worm is another example that can cause a significant impact even on national security. Once an entry point is found, an intruder or a malicious node may perform different actions to compromise the whole system. Since millions of homes are connected to an SG, the impact of such attacks can cause a significant loss or harm on society.

This work is focused on authentication and key management over the Smart grid Users. The Smart Grid Users will likely to employ Internet Protocol version 6 (IPv6) technology in a mesh-based topology.

An attacker can counterfeit network failures by modifying users data, like resource size and bandwidth, to trigger inappropriate protection operations Even worse, an incorrect operation may spread quickly to neighbor users due to interconnections between substations, thereby deriving cascading failures in a large area . Thus, how to protect the integrity and authenticity of SAS messages between interconnected users is a crucial challenge not only for the reliability of the smart grid, but for the national security and public safety.

We reduce the network overhead caused by the control packets for key management. The improved efficiency results from our key refreshment protocol in periodically broadcasts a new key generation to refresh the public/private key pairs of all the nodes as well as any required multicast security keys. The performance analysis at last verifies the overhead reduction.

We propose a secure and efficient SG mutual authentication (SGMA) scheme and an SG key management (SGKM) protocol. SGMA provides efficient mutual authentication between Smart Grid users and authentication server in the SG using passwords; it reduces the number of steps in Secure Remote Password from five to three and the number of exchanged packets from four to three.

DOI: 10.15680/ijircce.2015.0306141

IV. SYSTEM ARCHITECTURE

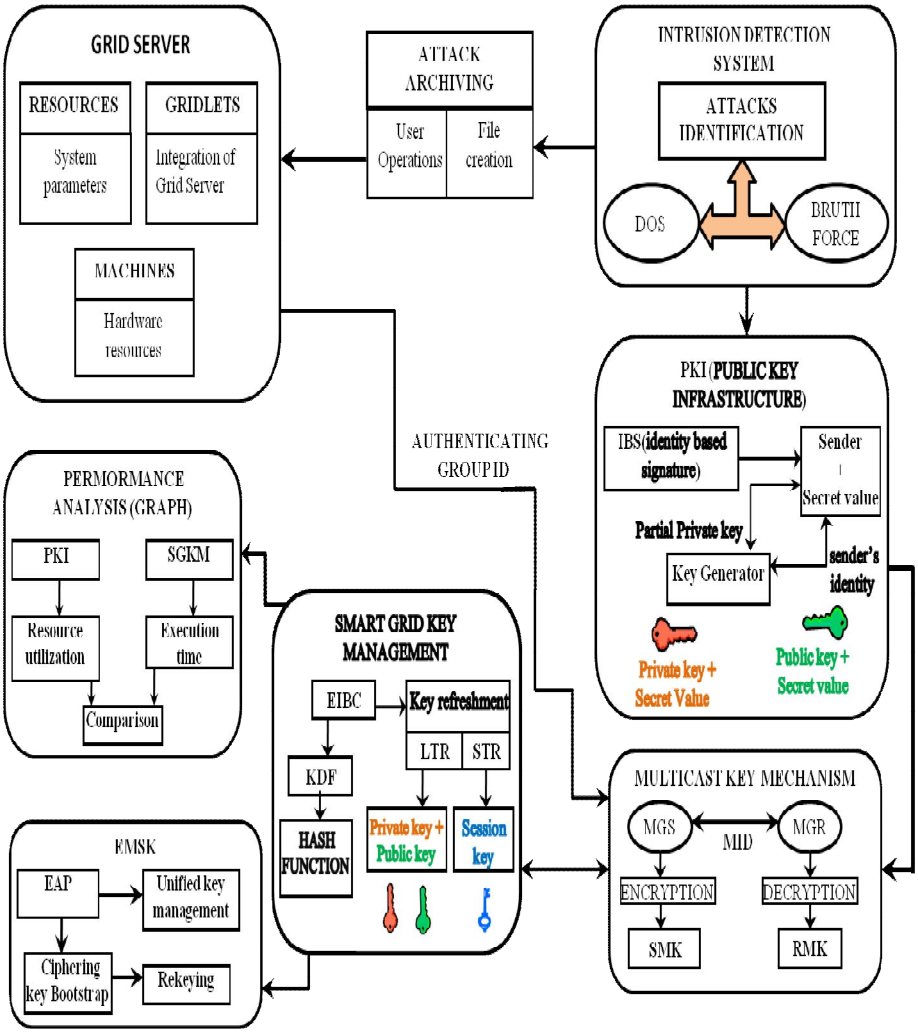


Fig 1. System Architecture

To support secure multicasting, EIBC incorporates two mechanisms to manage the multicast group source (MGS)/receiver key pair. Each multicast group is identified by a multicast group ID (MID), which is used similar to the ID of an entity, to obtain the source multicast key (SMK). At the same time, each group has a receiver multicast key (RMK) managed by SAS .Each MGS entity receives the group's SMK and RMK and grants membership to a multicast group receiver (MGR) entity by sending RMK to the new MGR.

Therefore, MGS encrypts the messages by SMK, and an MGR uses RMK to decrypt the messages. In order to authenticate the source of a multicast packet and because an SMK can be compromised. MGS signs the messages using its own entity (original) private key ($PrvK_i$ ID). Furthermore, EIBC generates m_i, similar to s_i, using a multicast group PRNG with its own setup values c and d and initial value mo. Receivers use m_i to refresh RMK.

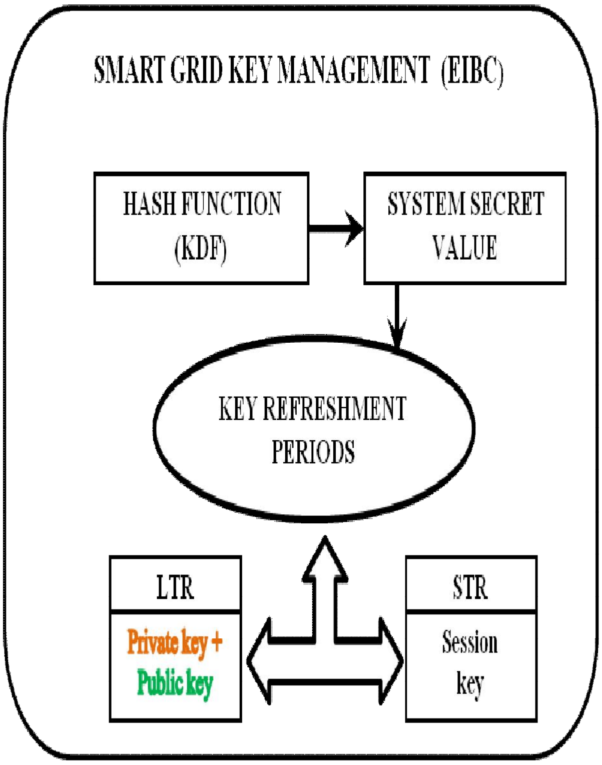


Fig. 2 Smart grid key management mechanism

EIBC enhances IBC by making the private key refreshment more efficient and by accommodating distribution and refreshment of any multicast key needed in the network. The modifications to IBC are described as follows:

1) One-Way/Hash Function F(.) : The static function F(.) in IBC is made dynamic in EIBC as function $F_i(.)$. Precisely, PKG periodically generates and broadcasts function $f_i(.)$ that is applied to F_i (.) to obtain F1+ $_i$ (.), which is the new one-way function of the system. In this case, all of the public keys and private keys are being updated. Each party updates the public key of any other party by applying $f_i(.)$ to the current public key of that party. Also each party uses $f_i(.)$ in the private key refreshment algorithm that will be explained shortly. The index i represents the current state (called live in this paper) of the system.

$F_i +1(.) = f_i +1 (F_i (.))$

PubKi(ID) = F_i (ID)

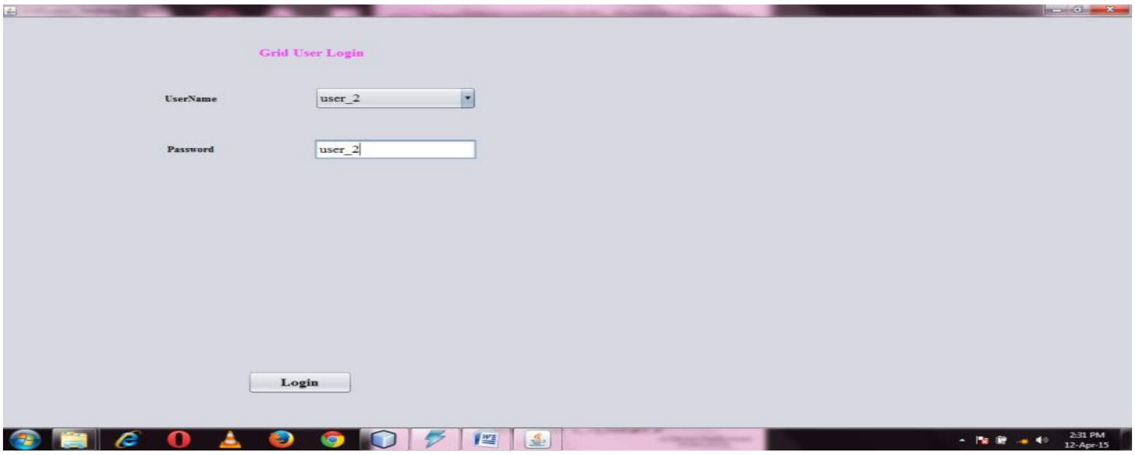
2) Key refreshment periods : The key refreshment will be carried out by Diffie-Hellman Module which consist of private key pair and public key pair of owner & user .Each owner & user consist of key value & message that is going to be modified. The system secret value is the key value chosen by owner in order to convert the message into cipher text using electronic codebook ECB/PKCS5 padding. The chiper text so formed using the above padding scheme is in encrypted form that consist of every private key and public key pair of owner & user in **UTF (Universal Character Set + Transformation Format—8-bit)** message encoded form.

EIBC Algorithm for Key refreshment

1. Generates key Pairs form KPG **(key pair generator)**
KeyPair kp1 ; KeyPair kp2;
Key pair generator
Get the instance of key (password) during run time

```
kpg = KeyPairGenerator.getInstance ("DH");
initialize KPG (no. of combination);
2. Gets the public key
PublicKey=pbk1   PublicKey=pbk2;
3.  Gets the private key
PrivateKey prk1 = kp1      PrivateKey prk2 = kp2
4. Computes secret keys
SecretKey key1:
if agreeSecretKey(prk1, pbk2) is True then
goto
ka.init(prk_self) (initialize the key agreement)
5. Computes the KeyAgreement
ka.doPhase(pbk_peer, lastPhase)
6. generate shared secret key
byte[] secret = ka.generateSecret();
7. Initialise  the cipher mode
Cipher c = Cipher.getInstance(ECB/PKCS5Padding")
c.init(Cipher.ENCRYPT_MODE, key1);
8. Compute the cipher text
byte[] ciphertext = user0 .getBytes();
9. Start the encryption Mode using UTF
Encrypted:  new String(ciphertext, "utf-8");
```

IV. **RESULTS**



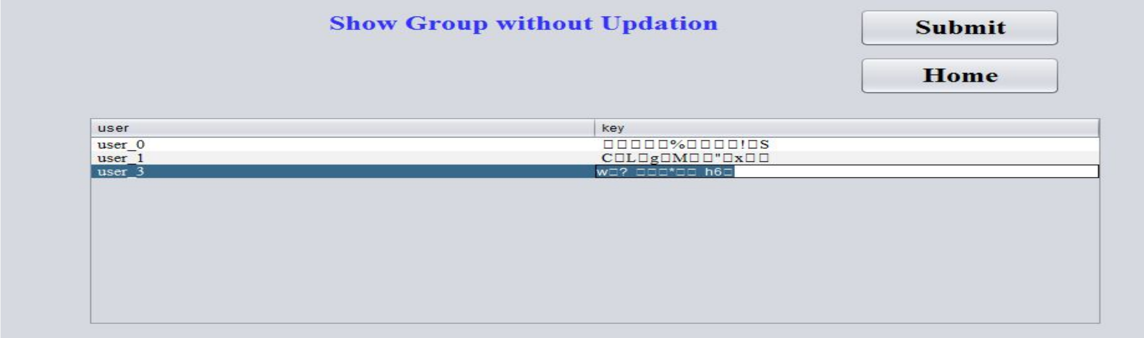
Grid User Login

UserName user_2

Password user_2

Fig 3.1 Host user login in server

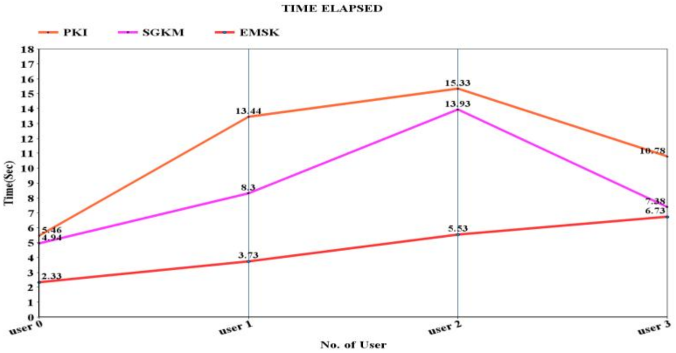
Fig 3. Shows the host user login details inside the grid server for multicasting and Fig 3.2 shows the keys generated for group of guest users that act as source multi-cast key and receiver multicast key.

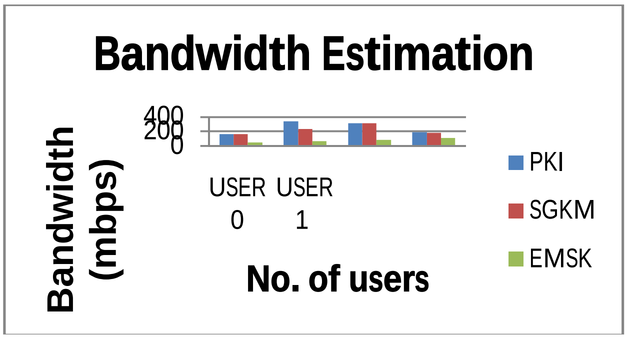


user	key
user_0	□□□□□%□□□□!□S
user_1	C□L□g□M□□"□x□□
user_3	w□? □□□*□□ h6□

Fig.3.2Guest user key generation for multicasting

No. of Users	INPUT	Avg. BDW (mbps)	Avg. TIME (Sec)
USER 0	Min val: 8 Max val: 15	168	5.46
USER 1	Min val: 8 Max val: 15	338	13.44
USER 2	Min val: 8 Max val: 15	316	15.33
USER 3	Min val: 8 Max val: 15	187	10.78





V. CONCLUSION AND FUTURE WORKS

The design of grid server in a dynamic environment to shows the activity and list of operations on process & how allocations of users are initiated by grid Server on demand. Secondly we have implemented SGKM in the GS in order to show the key refreshment when multiple users are trying to access the resources in a GS. Third we have shown the

DOI: 10.15680/ijircce.2015.0306141

EAP based UKMF and the impact on the server that generate token in a specific time interval for accessibility of others users. We proposed a new secure key distribution scheme for the smart grid with high efficiency as well as high security. In order to enjoy the security benefits of SGKM has endured the inefficient resource utilization due to the large key sizes as well as the large key distribution overhead. In SGKM Scheme we have implemented a new cryptography concept named EIBC that uses Salt and Iteration of plain text and an encrypted text and converted them into UTP-8 format and byte-64 coded machine readable format to generate a complex string. The proposed enhanced mechanism EAP based UKMF is flexible in peer entity authentication can be treated as either network access authentication or application-level authentication. EAP-based unified key management mechanism and show that it is important to consider re-key efficiency of the ciphering keys bootstrapped from EMSK.

The module established that information discovery for bootstrap application ciphering is an important and as yet missing piece to realizing the unified key management framework vision. This area requires additional investigation and is part of our future work and also included in the security enhancements that may be needed to support new demands of the smart grid. Key management has been an area of considerable attention, particularly in browser-based web applications.

References

[1]. Dapeng Wu, Chi Zhou,"Fault-Tolerant and Scalable Key Management for Smart Grid," in Smart Grid, IEEE Transactions on (Volume:2 , Issue: 2),pp. 1949-3053,June 2011.
[2]. A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, D. Barthel "Secure Lossless Aggregation for Smart Grid M2M Networks", First IEEE International conference on Smart Grid Communications, pp 333-338, Oct 2010, doi: 10.1109/SMARTGRID.2010.5622063
[3]. H. Khurana, R. Bobba, T. Yardley, P. Agarwal, E. Heine, Design principles for power grid cyber-infrastructure authentication protocols, Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS'10) 2010.
[4]. F. Zhao, Y. Hanatani, Y. Komano, B. Smyth, S. Ito, and T. Kambayashi, "Secure authenticated key exchange with revocation for smart grid," in Proc. IEEE PES ISGT, 2012, pp. 1–8.
[5]. X. He, M. Pun, and C. Kuo, "Secure and efficient cryptosystem for smart grid using homomorphic encryption," in Proc. IEEE PES ISGT, 2012, pp. 1–8.
[6]. H.-K. Oh and S.-H. Jin, "The Security Limitations of SSO in OpenID," ICACT, 2008.
[7]. S. Das, Y. Ohba, M. Kanda, D. Famolari, and S. Das, "A key management framework for AMI networks in smart grid," IEEE Commun. Mag., vol. 50, no. 8, pp. 30–37, Aug. 2012.
[8]. AVISPA-Automated Validation of Internet Security Protocols. [Online]. Available: http://www.avispa-project.org
[9]. D. Dolev and A. Yao, "On the security of public-key protocols," IEEETrans. Inf. Theory, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[10]. J. Xia and Y. Wang, "Secure key distribution for the smart grid," IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 1437–1443, Sep. 2012.

BIOGRAPHY

[1]**Jadhav Neelkanthrao.** B.Tech (CSE) degree from JNTU-Hyderabad India in 2012. He is pursuing M.Tech. in the Computer Science Turbo machinery Institute of tech.& Sciences(JNTU)Hyderabad. Mail id- nilkant.inform@gmail.com

[2]**Dhiren Kumar Dalai** received his M.Tech (CSE) degree from Anna University, India in 2015. He is presently working as Assistant professor in the Computer Science and Engineering Dept, Turbo machinery Institute of tech.& Sciences (JNTU)Hyderabad. His research interest is in the area of Network Security.