ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Threshold Cryptography-based Group Authentication Scheme for the Smart Home Environments

Geetha A V[1], Rajesh Kumar PM[2]

PG Scholar, Computer Science, LBS College of Engineering, Kasaragod, India[1]

Assistant Professor, Computer Science, LBS College of Engineering, Kasaragod, India[2]

Abstract: The rapid increase of current wireless communications and information technologies have been altering human's lifestyle and social interactions; the next achievement is the smart home environments or spaces. A smart home consists of low capacity devices and wireless networks, and therefore, all working together as a secure system that needs an adequate level of security. Here a lightweight and secure session key establishment scheme for smart home environments is introduced. To establish trust among the network, every sensor and control unit uses a short authentication token and establishes a secure session key. This scheme provides important security attributes including prevention of various popular attacks, such as denial-of-service and eavesdropping attacks. In this smart home environment only the outside devices can be authenticated. To establish group authentication of devices in smart home new scheme is introduced that is threshold cryptography based group authentication. Secure, and efficient group authentication scheme is used that authenticates a group of devices at once. Here presents novel Threshold Cryptography-based Group Authentication scheme for the smart homes which verifies authenticity of all the devices taking part in the group communication. The proposed scheme is implemented for WIFI environment.

Keywords: Public key Searchable Encryption, Semantic Security, Public key Encryption ,Keyword Search, security, Authentication, Threshold cryptography.

I. INTRODUCTION

Generally, a smart home network consists of a number of heterogeneous smart devices, such as, low-cost sensor, actuator, smart light, smart window shutter, smart thermostat and surveillance camera or other type of smart devices that are integrated with intelligence, as shown in Fig.1. The home environments and networks are used interchangeably. Most of the devices are having resource-limitations .However, in such home networks, the SDs communicate over the wireless channels through the local home gateway. The home gateway acts as a bridge between the SDs and the users, and provides interoperability and control for the SDs, connect to the outer world via the Internet . Thus the qualities of SDs are enabling users to operate homes remotely/directly using the smart phones, tablets, or through designated web apps, anywhere and anytime.

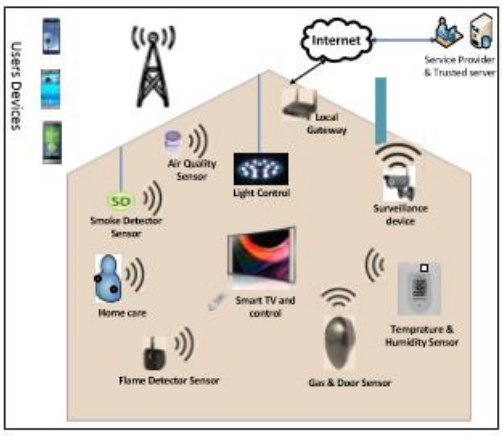


Fig. 1. Smart home environment.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

A smart homes open up an attack surface as the SDs data collected and communicated over insecure wireless networks, leaving them vulnerable to security attacks. To obtain a satisfactory level of security, here presents a lightweight and secure session key establishment scheme. It allows each entity should be performed a light- weight mutual authentication prior participation in the home network and establish a session key in a secure manner. To verify the device authentication and message integrity, utilize the smart device's unique and immutable identifier, after denoted as its Silicon ID (a silicon serial chip number). This scheme uses the symmetric key cryptography and a hash function to compliment other techniques in order to provide more security in the smart homes. In addition, a new device can be easily entered arbitrarily and securely into the scheme to extend the smart home services.

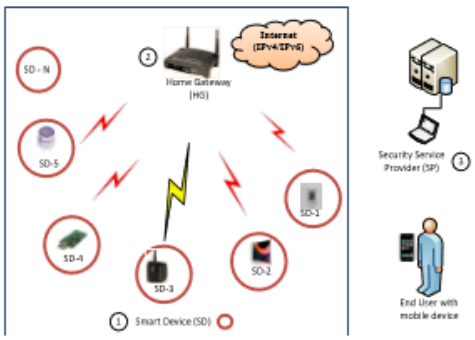


Fig. 2. SD-to-HG communication pattern in smart home.

As shown in Fig. 2, three entities are mainly involved in a smart home environment, as follows. 1) The SD forwards home data to the home gateway using a single-hop link. Similarly, the home gateway can perform queries to the SDs, whenever needed. 2) The home gateway is a special node that takes re- sponsibility of controlling the network data, device and network interoperability, and security management . In addition, the gateway works as a router between the SDs and the end users. It has two wireless interfaces: (i) a short-range wireless interface (e.g., 802.15.4) main- tains the connection within the internal (smart) devices, and (ii) a long-range communication interface (e.g., Wi- Fi/GPRS) maintains a connection with the outer world 3) Security service provider is a trusted server, and is responsible for generating and assigning the keying material to the smart home entities.

II. RELATED WORK

Gomez and Paradells discussed a different types of wireless home automation network architectures and technologies, including security obstacles of the ZigBee, INSTEON, Wavenis and Z-wave, and for the IP-based technologies. Similar to [1], Ayday-Rajagopal has also noticed that the existing home area network (HAN) protocols (ZigBee, Z-wave, and INSTEON) support security only up to a certain level . They introduced three different secure device authentication mechanisms for smart grid-enabled HAN. For example, (1) authentication mechanism between the gateway and the smart meter; (2) authentication between the smart appliances and the HAN; and (3) authentication between the transient devices and the HAN. However, to perform the authentication, the schemes presented in are (heavily) depending on 3rd party (such as, the Internet service provider, or telecommunication companies), and then it providing security to the HAN.

The security scheme in aimed a secure smart household appliances framework, named S2A. The authors conceptually focused on the usability, controlling electricity prices, and operational safety for the smart devices (i.e., appliances). By employing a machine learning method, the S2A framework provides an effective and reliable security protection. However, it (S2A) does not consider the fundamental security properties (i.e., device authentication, data confidentiality, and integrity), which means the framework may not withstand under a collaborative adversary model (e.g., the Dolev-Yao model).

Guillet et al. developed a correct by construction security approach to design a fault tolerant smart home for the disabled people. The proposed scheme exploits a formal technique named discrete controller synthesis (DCS) to automatically control the devices. To control a device, authors presented two types of security constraints expressed as boolean expressions: (i) hypothesis (supposed to remain true for all execution); and (ii) guarantee (enforced to remain

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

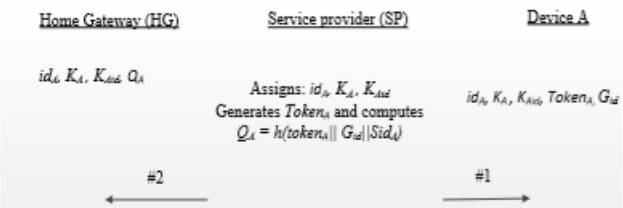
true using DCS if and only if the hypothesis stays true). Though, the scheme employing formal techniques and boolean expressions to control the devices states (e.g., on/off), the authenticity of boolean expressions are not being verified. Therefore the scheme may not work under active attacks.

Kim et al. presented a seamless integration of heterogeneous devices and access control in smart home. Authors observed that there is a lack of the de facto communication standard in the interoperability of device from different vendors in the smart homes. Therefore, based on the open services gateway initiative they proposed a smart home architecture that integrates heterogeneous protocols in the HAN. In their architecture, an access control model manages authentication and authorization for different users' requests. In addition, the remote access is available only through the Restful web services. However, this scheme did not consider a device authentication at the time of home network deployment

III.PROPOSED WORK

Earlier work of smart home not focus the security. Here for security purpose light weight and secure session key can be using. This proposed scheme provides important security attributes including prevention of various popular attacks, such as denial-of-service and eavesdropping attack .In addition to this security attacks group authentication can also focus in this proposed work.
For security purpose includes three phases: the system setup; authentication and key establishment; and ease of addition of a new smart device.

A. System Setup
First of all, each home device should be registered off-line to the security service provider (SP) and obtained security parameters. Prior to the network deployment, for every smart device A, firstly, SP assigns identity (idA), and stores a unique secret key (KA) along with key identifier (KAid) to the device memory . SP generates a unique short authentication token (tokenA) and computes QA = h(tokenA||Gid||SidA). Note that, SidA is a Silicon-ID (a silicon serial number) that presented on the devices . Then, SP stores TokenA and idA to device A. In addition, SP also stores the HG identity (Gid) to device A. Secondly, SP stores each A's assigned identity (idA), QA and key (KA) along with its key identifier (KAid) to the home gateway (HG). Finally, SP maintains a database that keeps record of the deployed devices. For the smart home security purposes, it is practical to assume that all the stored keys have their life-time (e.g., 6 to 12 months), which depends on the SP.



B. Authentication and Key Establishment
To maintain an initial trust among the smart devices, this sub-section presents an authentication and key establishment mechanism. Assume the HG wants to start bootstrapping with the device A, as follows. S1: HG generates a random nonce r and computes C = MAC[QA,Gid||idA||T1||r] and sends a request {Gid, C,T1,r} message to the device A. Here T1 is the current timestamp of HG. S2: Upon receiving request message from HG, device A checks (T2− T1) ≤ T, if yes then proceeds to the next step. Compute QA= h(tokenA||Gid||SidA) and C∗ = MAC [QA, Gid||idA||T1||r]. Verifies C = C∗, if not, then it generates a false message and terminates the system. Otherwise, the device A generates a random secret s and computes NA= EKA[idA,s,r,T2] and tag = HMAC [QA,idA||Gid||s||r||T2], and sends a response message (i.e., {KidA, NA,tag,T2}) to the HG. Here T2 is the current timestamp of device A. S3: HG checks (T3 − T2) ≤ T, if hold then retrieves the corresponding key (KA) of KidA from own data- base and decrypts NA to obtain idA∗,s,r∗,T2∗. Now it verifies the following, T2∗ = T2, idA∗ = idA and r∗ = r, if not then aborts the system. Else it verifies (HMAC[QA, idA∗||Gid||s||r||T2])=tag∗. It generates the session key σ = h(idA||Gid||s||T3||T2||QA) and computes NHG = EKA[σ,s,T3], and then it sends a notify message {NHG,T3} to the device A. Here, T3 is a current timestamp of the HG. S4: Upon receiving notify from the HG, device A checks (T4 − T3) ≤ T, if it holds then decrypts NHG using KA and obtains σ∗, s∗ and T3∗. Verifies T3∗ = T3, s∗ = s, if yes then the session key (i.e.,σ = (h(idA||Gid||s||T3∗||T2||QA∗))) will be securely established between the two legal entities. Here, T4 is the current timestamp of device A. Fig. 4 depicts the flowchart of session key establishment scheme.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

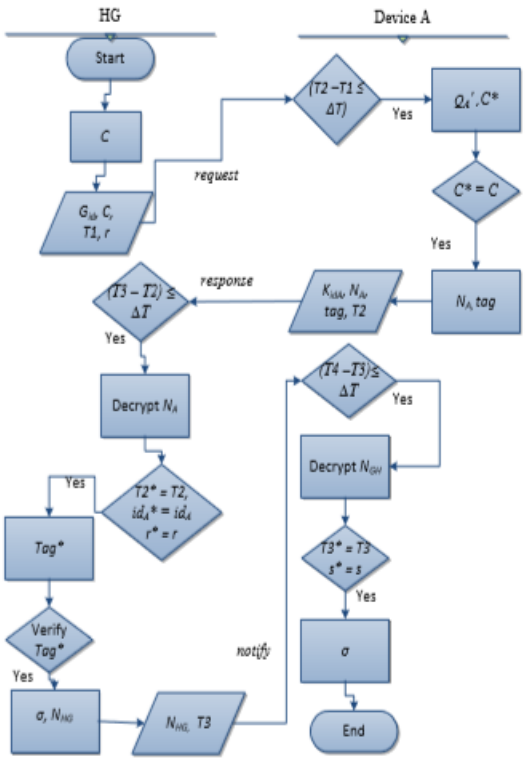
International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016



C. Ease of Addition a New Smart Device

It is practical that a new wireless smart device can join the smart home arbitrarily. The proposed scheme provides an ease of addition a new device (e.g., J) in the smart homes. To do this, the SP will initiate the followings. First, the SP will assign identities (idJ,Gid) and embed required security- related (KJ, Kjid,TokenJ) credential to the new device (J). Then, the SP securely passes J's information to the home gate- way (i.e.,idJ, KJ, Kjid, and QJ(= h(tokenJ||Gid||SidJ)) and deploys the new device. Then, the HG and the new device will perform the same above mentioned procedure.

To achieve group authentication in smart home environment this paper extends this work using Paillier Threshold Cryptography. This scheme establishes a secret session key at the end of each group authentication which can be use.

If a device of the group B, wants to communicate with any device in the group A, then device will initiate the handshake, thereby authenticating itself with the group A. Eventually, only authenticated devices from the group B will have the secret of the group A. Now it can communicate with all the members of the group A since it is group authenticated. On the other hand, all the devices of the group B except the authenticated one cannot communicate with the group A devices. The head of the group is required to generate, and distribute the new key pairs every time a new member enters the group to maintain group key leakage, and it is referred as Group Authority (GA). For group authentication following five modules are needed:

1. Key Distribution.
2. Key Update.
3. Group Credits Generation.
4. Authentication Listener.
5. Message Decryptor

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Algorithm 1 TCGA – *Key Distribution*

```
1: GA <-- Key Distributor
2: NewM <-- New Member
3: Gcurr <-- The Group member wants to join
4: START
5:    if (REQUEST == JOIN)
6:    if (groupListContains(Gcurr) &&
      Pssword= = Gcurr.Password)
7:    updateMemberList(IP[NewM])
8:    updateThreshold(n)
9:    keys [] = KeyGen. PaillierThresholdKey (128, n, threshold,
10:   randomNum( ))
11:   for (k: Gcurr.groupMembers )
12:   Connect (Gcurr.groupMembers.i)
13:   Send (Gcurr, key [k++])
14:         else
15:               Display ("ERROR")
16: END
```

Time Analysis: n = Number of devices

Recurrence relation can be written as:

$$T(n) = T(n-1) + T(1)$$
$$= T(n-2) + 2*T(1)$$
$$= T(n-3) + 3*T(1)$$
$$\ldots$$
$$= T(n-k) + k*T(1), \text{ let's put } k = n-1$$
$$T(n) = T(1) + n-1(T(1))$$
$$T(n) = 2 + n*2 - 2, \quad \text{Hence } T(n) = O(n)$$

Time analysis of key distribution shows that, in the proposed TCGA scheme, it takes O (n) time to distribute key amongst n devices. This shows that, even for large number of devices, the time required for key distribution is linear and more appropriate for all devices.

Algorithm 2 TCGA – *Key Update*

```
1: Gcurr <-- Current Group
2: START
3:    if (REQUEST == "UPDATE_KEY")
4:    Update (Gcurr.set(PrivatePartKey) ,
      Gcurr.set (GroupMemberList))
5: END
```

Algorithm 3 TCGA – *Group Credits Generation*

```
1: Gcurr <-- Current Group
2: START
3:    secret = Random (r)
4     hash = MessageDigest ["SHA-512", secret]
5:    GroupCred = Encrpyt ([secret, hash]_KPublicKey )
6:    for (i: Gcurr.groupMembers)
7:    Send (GroupCred,i )
8:    //After Group Cred sent to all the members,
      GAuthentication starts
9:    for (i: Gcurr.groupMembers)
      Send ("Start Distribution")
10: END
```

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Algorithm 4 TCGA – *Authentication Listener*

```
1: GroupCred <- [Secret, H (Secret)]
2: Gcurr <-- Current Group
3: PDM <-- Partially Decrypted Message
4: START
5:     if (REQUEST == "START DISTRIBUTION")

6:     myPDM = DECRYPT (GroupCred, Gcurr.
       PrivatePartKey)
7:     START [ PDMMessageDecryptor ]
8:     for (i: Gcurr. GroupMembers)
9:     Send (myPDM)
10: END
```

Time Analysis: Group Authentication

Recurrence relation can be written as:

$$
\begin{aligned}
&T(n) = T(n-1) + O(n) \\
&= T(n-2) + O(n-1)) + O(n) \\
&= T(n-2) + O(n-1) + O(n) \\
&= T(n-3) + O(n-2) + O(n-1) + O(n) \\
&\quad \ldots \\
&= T(1) + O(2) + \ldots + O(n-1) + O(n) \\
&= O(1 + 2 + \ldots + n-1 + n) \\
&= O(n^2)
\end{aligned}
$$

A. Pre-Authentication Phase

In this phase, the GA of the group, who creates the group, is responsible for generating a public key KPu (G) and multiple private keys KPr1 (G)…..KPrn (G) using Paillier Threshold Cryptosystem depending upon the number of members (n) in the group, and the threshold value t. Private keys K Pr1(G)…..K Prn(G) are then distributed by the GA among all the members of the group. When a new member joins the group, the threshold value is changed appropriately, and keys are generated, and distributed again. This threshold value changes dynamically as new members join so that the high level of security is maintained.

B. Group Authentication Phase

If a group activity needs to be started, group authentication needs to be performed as a pre-requisite to check if all the members M1…Mm (where m<=n) are part of the group. The GA chooses a pseudo-random number as a session secret [SS] key which is going to be shared with all the members of the group once the group authentication is done. This is encrypted using the public key [KPu] of the group, and sent to all the members of the group. The hash of the session secret H [SS] is also sent along with it. Message = {[SS] KPu, H [SS]} Each of the members, upon reception of this message, applies their private key part to decrypt it, giving them a PDM. Each device has a unique PDM corresponding to a different part key. PDM = Decrypt (Message, PrivatePartKey) Each device then sends this PDM to every member including the GA. All the devices wait to combine all the PDMs until n-1 PDMs are received. Each device combines all the PDMs so as to get the decrypted session key. Session Key = Combine (PDM1, PDM2… PDMm) when any particular member wants to start a group activity, it send a request to the current GA. On reception of the request, the GA generates a session secret which is going to be shared by all the members of that group. This session secret is then encrypted with the public key of the group. This provides the required security as it can only be decrypted by the complete private key. A Hash map function is applied to the session secret which is going to be used in further steps to prove the integrity of this message. It is sent along with the encrypted session secret in a single message. This message is sent to all the members of the group. All the devices then use their own part private keys to decrypt this message which gives them a PDM which is not the final session secret. Now it sends this PDM to each member in the group. Until n-1 PDMs are received each of the devices waits. All the devices then try to combine all of the shares which will

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

ultimately give them the final session secret. If successful, means that all the PDMs received are by the legitimate group members only, and, hence the group authentication succeeds. The group activity can then be started using the session secret for further communication. If unsuccessful, means that there is at least one device which is using a fake part private key and hence the partial decryption generated by him is not genuine. Therefore, upon trying to combine all the shares it was result in failure. This means that group authentication fails, and there is a need to restart the process.

When the devices belonging to different groups communicate to each other through Internet, This scheme performs key distribution, key update, message decryption and finally group authentication in order to authenticate each other

IV.DISCUSSION

Smart home environment as "a small world where different kinds of smart devices are continuously working to make inhabitants' lives more comfortable." Smart environments aim to satisfy the experience of individuals from every environment, by replacing the hazardous work, physical and repetitive tasks with automated agents.For differentiates three different kinds of smart environments for systems, services and devices: virtual (or distributed) computing environments, physical environments and human environments, or a hybrid combination of these: Virtual computing environments enable smart devices to access pertinent services anywhere and anytime. Physical environments may be embedded with a variety of smart devices of different types including tags, sensors and controllers and have different form factors ranging from nano- to micro- to macro-sized. Human environments: humans, either individually or collectively, inherently form a smart environment for devices. However, humans may themselves be accompanied by smart devices such as mobile phones, use surface-mounted devices (wearable computing) and contain embedded devices (e.g., pacemakers to maintain a healthy heart operation).

A light weight and secure session key can be establishing for the smart home environment for authenticating the outside devices. This can be make secure against denial-of-service and eavesdropping attacks. Also here make group authentication of the devices in the smart home environment. For this group authentication threshold cryptography based group authentication (paillier cryptosystem) can be used. The paillier cryptosystem, named after and invented by by Pascal Paillier in 1999, is probabilistic symmetric algorithm for public key cryptography. The problem of computing n-th residue classes is very difficult. The scheme is an additive homomorphic cryptosystem, ie given only the public key and the encryption of m1and m2,one can compute the encryption of m1 and m2.

V.CONCLUSION

Here proposed a lightweight and secure session- key establishment scheme focusing on the smart homes. The proof of concept demonstrated that a session key is established in a lightweight way, which is a paramount security requirement for the smart home environments; there are unbounded numbers of heterogeneous devices talking to each other. Each device should not be able to authenticate during the short time. Due to the scale of economics, more than hundreds of devices may request authentication approval at the same time. To this purpose, here presented threshold cryptography based group authentication scheme. This scheme established a group authentication scheme also which ensures the simultaneous authentication of all the members of a group using paillier threshold cryptography but also established a secret session key which can be used for communication that might occur in group oriented applications

REFERENCES

[1] C. Gomez and J. Paradells, “Wireless home automation networks: A survey of architectures and technologies,” IEEE Commun. Mag., vol. 48, no. 6,pp.92-101,jun.2010.
[2] J. E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, and D. Mosse, “Seamless integration of heterogeneous devices and access control in smart homes,” in Proc. 8th Int. Conf. Intell. Environ. (IE), Jun. 2012, pp. 206–213
[3] G. Mantas, D. Lymberopoulos, and N. Komninos, “Security in smart home environment,” in Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications. Hershey, PA, USA: IGI Global, 2006.
[4] D. Pishva and K. Takeda, “A product based security model for smart home appliances,” in Proc. 40th Annu. IEEE Int. Carnahan Conf. Secur. Technol., Oct. 2006, pp. 234–242.
[5] N. K. Suryadevara, S. C. Mukhopadhyay, R. Wang, and R. K. Rayudu, “Forecasting the behavior of an elderly using wireless sensors data in a smart home,” Eng. Appl. Artif. Intell., vol. 26, no. 10, pp. 2641–2652, Nov. 2013.
[6] S. Bhardwaj, T. Ozcelebi, J. Lukkien, and C. Uysal, “Resource and service management architecture of a low capacity network for smart spaces,” IEEE Trans. Consum. Electron., vol. 58, no. 2, pp. 389–396, May 2012.
[7] H. Tschofenig, J. Arkko, and D. McPherson, “Architectural consider- ations in smart object networking,” Internet Engineering Task Force, Fremont, CA, USA, Tech. Rep. RFC-7452, Jul. 2014
[8] D. G. Korzun, S. I. Balandin, and A. V. Gurtov, Deployment of Smart Spaces in Internet of Things: Overview of the Design Challenges (Lecture Notes in Computer Science), vol. 8121. New York, NY, USA: Springer, 2013.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

[9] M. Burrough and J. Gill. Smart Thermostat Security: Turning up the Heat. [Online]. Available: http://www.burrough.org/Documents/Thermostat-final-paper.pdf, accessed Apr. 10, 2015.
[10] Y. Chen and B. Luo, "S2A: Secure smart household appliances," in Proc. 2nd ACM Conf. Data Appl. Secur. Privacy (CODASPY), 2012, pp. 217–228.
[11] Maarten Botterman, "Internet of Things: an Early Reality of the Future Internet," Workshop Report, European Commission Information Society and Media, May 2009.
[12] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad, "Identity Authentication and Capability based Access (IACAC) Control for the Internet of Things," In Journal of Cyber Security and Mobility", River Publishers, Volume: 1, Issue: 4, pp: 309-348, March 2013
[13] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad, "Identity Establishment and Capability Based Access Control (IECAC) Scheme for Internet of Things," In proceedings of IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012), pp: 184-188, Taipei - Taiwan, September 24-27 2012.
[14] Sachin D. Babar, Parikshit N Mahalle, Neeli R. Prasad and Ramjee Prasad, "Proposed on Device Capability based Authentication using AES-GCM for Internet of Things (IoT)," In proceedings of 3rd International ICST Conference on Security and Privacy in Mobile Information, and Communication Systems (Mobisec 2011), Aalborg – Denmark, May 17-19, 2011.
[15] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," In Proceedings of the 17th International Conference on Theory, and Application of Cryptographic Techniques (EUROCRYPT), pp: 223-238, 1999
[16] Miao Pan, Jinyuan Sun, and Yuguang Fang, "Purging the Back- Room Dealing: Secure Spectrum Auction Leveraging Paillier Cryptosystem," In IEEE Journal on Selected Areas in Communications, Volume: 29, no.4, pp: 866-876, April 2011.
[17] Rongxing Lu, Xiaohui Liang, Xu Li, Xiaodong Lin, and Xuemin Shen, "EPPA: An Efficient, and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," In IEEE Transactions on Parallel and Distributed Systems, Volume: 23, no.9, pp: 1621-1631, September 2012.
[18] E. Goh, "Encryption Schemes from Bilinear Maps," Ph.D. Thesis, Stanford University, USA, September 2007
[19] Lein Harn, "Group Authentication," In IEEE Transactions on Computers, IEEE computer Society Digital Library, IEEE Computer Society, 16 October 2012
[20] Lei Zhang, Qianhong Wu, Solanas A., and Domingo-Ferrer J., "A Scalable Robust Authentication Protocol for Secure Vehicular Communications," In IEEE Transactions on Vehicular Technology, Volume: 59, no. 4, pp:1606-1617, May 2010.