Novel and efficient Authentication Scheme for IoE in Smart Home Environment

Ajay Nadargi, Mythili Thirugnanam

Abstract: ***Nowadays, the smart home combines the information technology and communication in which connected things and systems communicate with one another and controlled to communicate with family members and standard of their life. In any case, the nature of Smart Home environments is always associated with the computer network and the open privacy indirect accesses by family members increase privacy issues. This scenario must absolutely respect the confidentiality and privacy of household member's information. Therefore, this paper attempts to review of security challenges of various authentication schemes for ensuring security in Smart home environment. Also, this work analyzed the solution of various security issues presented in the exiting works. The review revealed that the solution of device level security issues is desirable, at the same time existing authentication schemes is very expensive process for smart objects communication inside the Smart Home IoE. Based on these analyses, this paper proposed a novel authentication scheme to resolve security issues in Smart Home Environment. Also, the paper concludes the performance of evaluation of existing authentication schemes based on the past work.***

Index Terms**: *Authentication, ECC, Internet of Everything's (IoE), Smart Homes.***

I. INTRODUCTION

The Internet of Everything's (IoE) is a rising worldview concentrating on the between association of things to one another and to the clients. After some time, the many associates are moving from 'Human to Objects' to 'Objects to Objects'. This innovation turns into a fundamental achievement for smart homes IoE to carry accommodation and productivity inside our lives and homes. The IoE innovation into our homes there will be significant results for security in these technologies. Due to connected things within smart home to one another on the web outcomes in new protection issues, e.g., authenticity, privacy and information integrity. These innovations are especially susceptible against various security assaults for smart home IoE unbound to live in and in this way, it's important to assess the privacy threats to pass judgment on smart homes. In smart home IoE to be effective and accomplish broad use, it desires to pick up the faith of clients by giving enough privacy confirmation. In IoE [20] keeping up privacy is the basic test to survive. The smart home is progressively computerized and loaded up with smart objects, potential system security assaults and their effect on inhabitants should be explored [3].

II. RELATED WORKS

There is an enormous research done for securing Smart Home Environment. Many researchers have studied various aspects of security issues in Smart Home IoT. The most researches in this field are discussed in the following section. There is a related work done in the Smart home IoE [4,5] where the authentication and communication cost are remains unaddressed.

The various authors presented security solutions, yet attack resistance is not discovered and the central point of impacts are the device connectivity, power consumption, security, geographical issues, installation cost, and execution cost [1, 2]. Based on these impacts different authentication schemes are necessary for security against the different attacker models.

ANALYSIS OF EXISTING AUTHENTICATION SCHEMES IN SMART HOME

In this paper we discovered the security issues in smart home networks and conduct existing authentication schemes analysis.

The result analysis are helps to find outs necessary requirements for secure communication in smart homes. Analyses of various issues in existing authentication scheme are carried out and same is discussed in Table I.

From Table I, overall review on security IoE concludes that, existing authentication scheme have security issues such as wireless attack and electromagnetic interference. DOS attack, radio attack, MIM attack, device cloning issue, authentication issues, unauthorized traffic monitoring, and massage tampering issues are commonly occurred in Smart Home environment. Mostly [22], third party intrusion and reply attack issues are found on smart home gateway device. In Table II, shows the comparison of different authentication schemes based on security parameters. From Table II, the existing authentication schemes not fulfill all requirements for authentication in smart home IoE. The 'X' sign in Table II indicates the respective feature absence in the corresponding schemes. The literature analysis shows that all existing solutions in smart home IoE not fulfill all the requirements like lightweight solution, mutual authentication, attack resistant and access control.

Revised Manuscript Received on June 05, 2019.

Ajay Nadargi, Research Scholar, School of Computer Science and Engineering, VIT University, Vellore, Tamilnadu, India.

Mythili Thirugnanam, Associate Professor, School of Computer Science and Engineering, VIT University, Vellore, Tamilnadu, India

Table I: Review of various security issues in existing authentication scheme

Sr No	Authentication Schemes	Observation	Issues Identified
1	ECC based Authentication [6] [7]	Secure, mutual authentication protocol, which is based on ECC, Lightweight Solution, Identity authentication by key itself and not by the third-party, avoid Communication Overhead	DoS, MIM Attack, Electromagnetic Interference, Access Control
2	Peer-to-Peer Authentication [8]	The peer-to-peer authentication provides security, integrity and authentication. Avoid Central Point of failure	Limited Computational resources, and cannot be used for a wide area, More Computation time and memory, Requires prior knowledge about the network setup and structure
3	Mutual Authentication schemes using hash functions [9]	Authentication among the system and node, less computation, inexpensive communication	Authentication, integrity and privacy issues, MIM, Replay Attack
4	Distributed User Authentication scheme [10]	Distributed user authentication scheme for WSN	User entity authenticated, and not lightweight solution for IoE
5	Progressive Authentication [11]	Parameter passing during the handshake based on symmetric key cryptography, Lightweight Solution	Time consuming, Prime numbers required large memory
6	Peer Identification [12]	For node authentication, Direction of the signal is considered	Required more computations and memory to find signal path
7	Cluster based [13]	Cluster based authentication, large-scale, low cost	More Computation time and memory, Attacker hold system key pairs and cluster key
8	Directed path-based authentication scheme (DPAS) [12]	Mapping and verification for the sensor nodes, Reduce Communication overhead and computation load, Symmetric Key generation	Reply Attack, key distribution Problem
9	Aggregated-Proof Based Hierarchical Authentication	Symmetric Key Generation [18]	Replay attack, Message tampering issue
10	IACAC Authentication [2]	Diffie-Hellman exchange	DoS, Replay, MIM, Message tampering issue
11	Improved Identity Authentication	Based on Public Key cryptography [19]	Time consuming, Privacy issues
12	Device Authentication Scheme (AK) [15]	ECC, Public Key	MIM, Device cloning issue
13	Key Establishment (KE) Scheme	Key Generation for secure communication [17]	Replay attack, Masquerade
14	Threshold Cryptography-Based Group Authentication (TCGA)	Based on Asymmetric cryptography [2]	MIM, Replay Attack, Unauthorized Traffic Monitoring

From Table II, the solutions of common security issues in smart home network are compared and which is bringing the closure to categorize the level of existing solutions as a resolved (√) and not resolved (X). Solutions are classified as a not resolved category in security issues are proposed security mechanism techniques with many constrained. The solution with this intention, a novel authentication scheme is proposed to improve the partially resolved security solution in Smart Home IoE.

In [14,16,21], discovered some weakness in existing solutions proposed such as secure session key, message exchange and access control.

Based on the literature survey the existing schemes are costly for secure communication in smart home IoE. Therefore, it is necessary to propose improvements to existing schemes in terms of low communication cost and privacy and the relative performance analysis with existing solutions to evaluate our proposed scheme

Table II: Comparison of different authentication schemes based on security parameters

Authentication Schemes	Security Solution Observed						
	Mutual Authentication	Lightweight Solution	Attack Resistant			Distributed Nature	Access Control
			DoS	Man in Middle	Reply		
ECC based Authentication	√	√	X	X	X	√	X
Progressive Authentication	√	√	X	√	√	X	X
Mutual Authentication schemes using hash functions	√	√	X	√	√	√	X
Peer Identification schemes	√	X	X	X	X	√	X
Peer to Peer	X	X	√	√	√	X	X
Cluster-based authentication	√	X	X	X	X	√	X
Distributed User Authentication scheme	X	X	X	X	X	√	X

III. PROPOSED AUTHENTICATION SCHEME

This provides a novel authentication scheme which can be applied in Smart home IoE steadily and securely. LFSR and PUF function are basic principles used in this scheme and thereby proposing authentication scheme minimizes hardware requirement, which establishes light computation and communication cost.

As shown in Fig. 1, proposed scheme comprises of two phases registration and verification.

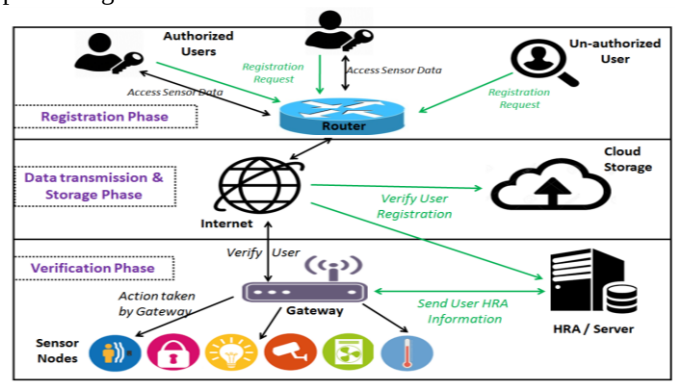

Fig. 1: Proposed Authentication Scheme

In proposed schemes, few conventions are considered and not to be violated during schema implementation. In Table III shows the signs and notations. The below assumptions are listed out.

Table III. Notations [21]

Notations	Description
H (.)	One-way hash function
RA	Registration authority
HRA	Home registration authority
P	Point on E
EK[m]	Encrypted data
DK[m]	Decrypted data
⊕	Bitwise XOR
||	Concatenation
MAC	Device Identity Code
PW	IDu Password
ID(u/t)	User / Thing Identity
Fp	Finite field
E	Elliptic curve
Nra	Gateway Nonce
G	Group of elliptic curves
Nu	HRA create nonce for User
S	Gateways (*RA*) private key
IDra	Gateway User ID
LSFR	Linear Feedback Shift Register
PUF	Physical unclonable function

1. In the registration phase smart home IoE, service providers and all the clients (user, things, Gateway) are to be authentic.
2. After that, not single client (user, things, Gateway) and HRA is authenticated. To use environment and services by the client's needs to authenticate themselves in login phase by submitting exact identification data.
3. HRA always trusted if mutual authentication is completed. So, it is considered that the server not ever negotiations with the attackers.
4. User interacts with gateway to save the communication cost of smart objects.
5. Secret key (S) considered to allocated before gateway interact in Smart Home.

A.Registration Phase

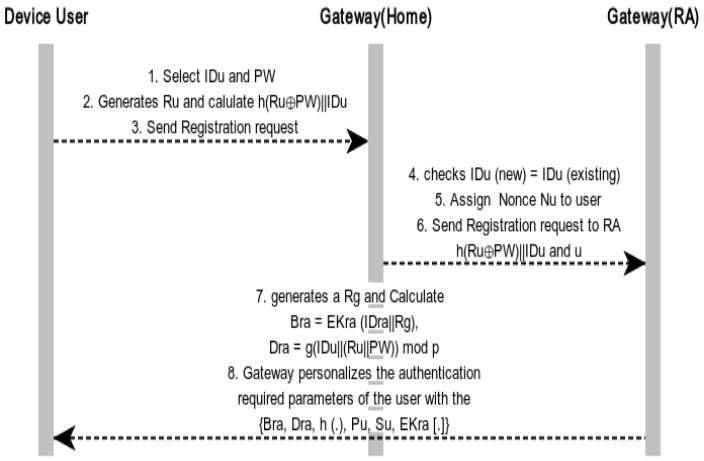

Fig. 2: Registration Process

The purpose of registration process is to authenticate user and

gateway by exchange of common secret key. The Fig. 2 shows the smart object communication in registration process.

B. Authentication Phase

Authentication phase is to perform the mutual authentication when user needs to use the smart home network. In Fig.3. Smart device performs the mutual authentication operations.

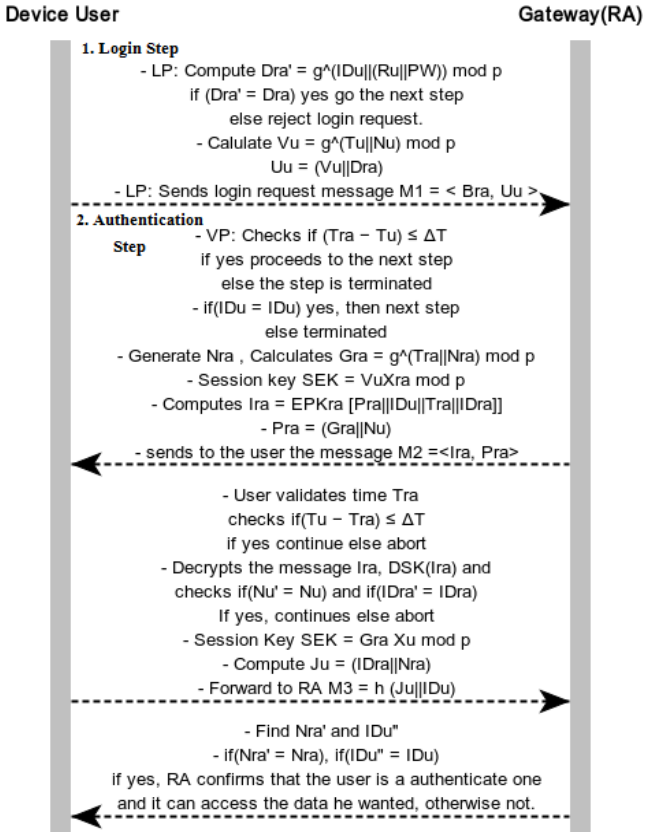

Fig. 3: Login and verification stage process

IV. PERFORMANCE EVALUATION

Proposed authentication scheme is feasible to implement LFSR and PUFs with less hardware (which requires thousands of gates) [23].

Table IV: Comparison of Encrypt Operations

Encrypt Operations	Total Gates Required
SHA 256	10,868
SHA 1	8120
MD5	8400
MD4	7350
AES	3400

As per review Table IV shows Comparison of Hash Function which needs from approximately more than 3,400 gates to implement [24] and the main problem is computation cost and consume more power for encrypt operations.

The Table V shows, the proposed scheme for 64-bit input requires only about 784 gates, considerably fewer than alternative schemes. Similarly, for 96-bits key it requires 1168 gates approx.

Table V: Gates required for 64-bit Key length

Key Length (64-Bit)	Functions	
	LSFR	PUF
Required Gates	256	512
XOR Gate	3	4
Total	**259**	**516**
ALU Gates	775	
Control Gates	9	
Total Gates	**784**	

Table VI: Proposed Authentication features

Key Size (bits)		8	16	32	64	96	160
Number of Gates	ALU + Control	103 +9	199 +9	391 +9	775 +9	1159 +9	1927 +9
	Total	**112**	**208**	**400**	**784**	**1168**	**1936**

In Table VI shows that, it requires less number of operations / gates to reduce communication and storage cost and also it requires less power requirement for performing encrypt operations.

Table VII: Comparable key sizes [23]

Key Size	RSA / DSA	Proposed
8	512	112
16	768	208
32	1024	400
64	1536	784
96	2043	1168
128	3024	1552
256	7680	3088

In Table VII demonstrates the measurable estimation of the computational and communication expense from the correlation execution. In table VII demonstrates that, for 128 bits key likewise requires 1552 logic gates entryways which is not as much as edge esteem different schemes.

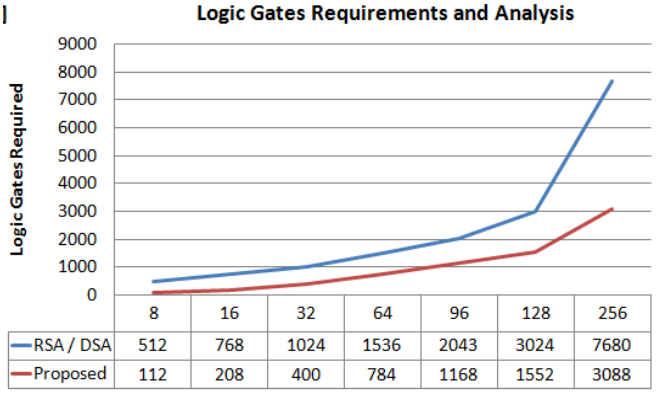

Fig. 4: Logic Gates Requirements and Analysis

In Fig 4, shows the performance of existing work and proposed scheme grounded on communication and computation cost.

V.CONCLUSION

The review focuses mainly around different security imperfections in smart home, impacts and proposing countermeasures to the recognized issues fulfilling a large portion of security necessities. The paper is condensed dependent on the parameters like mutual validation, lightweight schemes, impervious to assaults, distributed nature, trust and access control arrangement. Considering the real difficulties of security in the Smart home IoE the novel authentication proposed which are lightweight and assault safe for circulated nature of Smart Home IoE and it can securely be executed even in low cost objects with thought of calculation overhead, storage overhead and correspondence overhead for the performance analysis.

REFERENCES

1. Freddy K Santoso, and Nicholas C H Vun, "Securing IoT for Smart Home System", 978-1-4673-7365-4/15/$31.00 ©2015 IEEE
2. Parikshit N. Mahalle, Sachin Babar, Neeli R Prasad, and Ramjee Prasad, "Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges," In proceedings of 3rd International Conference CNSA 2010, Book titled Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010, Springer Berlin Heidelberg, pp: 430 - 439, Volume:89, Chennai- India, July 23-25 2010.
3. Antonietta Stango, Parikshit N. Mahalle, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)," In proceedings of 3rd International Conference CNSA 2010, Book titled: Recent Trends in Network Security and Applications - Communications in Computer and Information Science 2010 Springer Berlin Heidelberg, pp: 420 - 429 Volume: 89, July 23-25, 2010
4. Ramjee Prasad, "My personal Adaptive Global NET (MAGNET)," Signals and Communication Technology Book, Springer Netherlands, Pages: 435, 2010.
5. Kyriazanos Dimitris M., Stassinopoulos George I., and Neeli R Prasad, "Ubiquitous Access Control and Policy Management in Personal Networks," In Third Annual IEEE International Conference on Mobile and Ubiquitous Systems: Networking & Services, Volume: Issue: pp:1-6, San Jose-CA July 17-21, 2012.
6. Michael Braun, Erwin Hess, and Bernd Meyer, "Using Elliptic Curves on RFID Tags," In IJCSNS International Journal of Computer Science and Network Security, Volume: 8, Issue: 2, pp: 1-9 2008.
7. Sheikh Iqbal Ahamed, Farzana Rahman, and Endadul Hoque, "ERAP: ECC based RFID Authentication Protocol," In 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, pp: 219-225. Kunming, October 21-23, 2008.
8. Balfanz, D., Smetters D. K., Stewart P., and Wong H. C., "Talking to Strangers: Authentication in Ad-hoc Wireless Networks," In Network and Distributed System Security Symposium; pp: 6-8, San Diego CA- USA, February 2015.
9. Guanglei Zhao, Xianping Si, Jingcheng Wang, Xiao Long, and Ting Hu, "A Novel Mutual Authentication Scheme for Internet of Things," In Proceedings of 2011 IEEE International Conference on Modeling, Identification and Control (ICMIC), Volume: Issue: pp:563- 566, Shanghai – China, June 26-29, 2011.
10. C. Jiang, B. Li and H. Xu, "An Efficient Scheme for User Authentication in WirelessSensor Networks," In 21st International Conference on Advanced InformationNetworking and Applications Workshops, pp: 438-442, Niagara Falls – Ont, May21-23 2015.
11. R.R.S. Verma, D.O'Mahony, and H.Tewari , "Progressive Authentication in Ad-hocNetworks," In Proceedings of the Fifth European Wireless Conference, Barcelona –Spain, February 24-27 2014.
12. Suen, T., and Yasinsac A. "Ad-hoc Network Security: Peer Identification and Authentication using Signal Properties," In Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, IAW '05, pp: 432- 433, NYUSA, June 15-17, 2013.
13. Venkatraman L., and Agrawal, D.P., "A Novel Authentication Scheme for Ad-hoc Networks," In IEEE Wireless Communications and Networking Conference, WCNC-2013, Volume: 3, no., pp:1268-1273, Chicago-IL, 2013.
14. Ravi S. Sandhu, "The Typed Access Matrix Model," In Proceedings of the IEEE Symposium on Security and Privacy 2013, IEEE CS Press, USA, pp: 122-136.
15. T. Close, "ACLs don't," HP Laboratories Technical Report, February 2010
16. Gong L., "A Secure Identity-based Capability System," In Proceedings of 2011 IEEE Symposium on Security and Privacy (Oakland, Calif., May), IEEE Computer Society Press, Los Alamitos.
17. K. Hasebe, M. Mabuchi, and A. Matsushita, "Capability-based Delegation Model in RBAC," In Proceeding of the 15th ACM symposium on Access control models and technologies (SACMAT '10), pp: 109-118, Pittsburgh –USA, ACM, 2015.
18. David Barnard-Wills, "Threat Landscape and Good Practice Guide for Smart Home and Converged Media", http://www.shutterstock.com - Image ID: 162180008 - Copyright: Macrovector, Dec 2016
19. S. Radomirovic, "Towards a Model for Security and Privacy in the Internet of Things," In Procedings of 1st International Workshop Security of the Internet of Things (SecIoT 10), Network Information and Computer Security Laboratory, 2016.
20. R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," In IEEE Computer Journal, Volume: 44, Issue: 9, pp: 51-58, September 2014.
21. B. Ndibanje, H. Lee, and S.Lee, "Security Analysis and Improvements of Authentication and Access Control in the Internet of Things",Sensors 2014, 14, 14786-14805
22. Blaze, M.; Kannan, S.; Lee, I.; Sokolsky, O.; Smith, J.M.; Keromytis, A.D.; Lee, W.; "Dynamic Trust Management," Computer, vol.42, no.2, pp.44-52, Feb. 2014
23. Feldhofer, Martin, and Recberger, "A Case Against Currently Used Hash Functions in RFID Protocols", in RFIDSec, 2006.
24. G. E. Suh, S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation", in DAC, 2007.

AUTHORS PROFILE

Ajay Nadargi, Pursuing PhD, is a research scholar in the School of Computer Science and Engineering at VIT University, Vellore, India. He received his Master's in Computer Engineering from SIT, Pune University. He has 8 years of teaching experience. His area of specialization includes Network security and Internet of things (IoT). He has 2 years of research experience for the sponsored projects funded by BCUD Pune University.

Dr. Mythili Thirugnanam is an Associate Professor in the School of Computer Science and Engineering at VIT University, Vellore, India. She received her Master's in Software Engineering from VIT University. She has been awarded doctorate in Computer Science and Engineering at VIT University in 2014. She has 8 years of teaching experience. She has 3 years of research experience in handling sponsored projects funded by Government of India. Her area of specialization includes image processing, software engineering and knowledge engineering. She has published 15 papers in international journals and presented around 7 papers in various national and international conferences.