International Journal of Research in Advent Technology, Vol.6, No.6, June 2018
E-ISSN: 2321-9637
Available online at www.ijrat.org

Securing Real time data in IoT Environment

Miss. Nikita Chaudhari[1], Prof. Amit Palve [2]

Student, M.E.(Computer), SITRC, Nashik[1]
Assistant Professor, Computer Department, SITRC, Nashik[2]
Email: nikitachaudhari0394@gmail.com[1], amit.palve@sitrc.org[2]

Abstract- IoT (Internet of Things), future internet where everything is interlink with other via wire or wireless network, building ubiquitous computing era. Security is concern as IoT application area is evolving vastly long with attacks on devices. Interconnected devices has many application in smart grid, health, military, computing area, daily day-today life like smart vehicle, home, security application etc. Intelligent nodes, platform are working together without human interference in them. Enormous security and privacy threads of IoT applications arise due to ubiquitous and dynamic nature of IoT. Protocols like 6LoWPAN, providing security on communication level that is machine-to-machine communication security through authentication and authorization to void the security attacks on network. To provide the security as communication level, to nullify the security breaches on network, proposed system provides the mutual authentication between M2M devices. Registration, authentication, and key establishment can be done for communication of M2M devices in 6LoWPAN.

Index Terms- Security, 6LoWPAN, M2M, Sensor, Communication, Authentication, IoT.

1. INTRODUCTION

The time of IoT is starting with fast growth of network infrastructure and sensor. IoT is called collaborative ecosystem of context-aware, sensible and automatic program linked net-work, don’t consider security being an running requirement to ensure that security considerations joined down in matter list. Thus, corporations are reluctant to utilize security completely to the products and services. Consequence of the poor fashion, competitors can use a lot of susceptibility which causes security attack and enormous monetary damage. We know why security is crucial, and what competitors may do with security vulnerability [26].

IoT is the next massive boom inside the networking area. The imaginative and prescient of IoT is to attach day by day used gadgets (which have the potential of sensing and actuation) to the internet. This may or may not additionally involve human. IoT discipline continues to be maturing and has many open troubles, build up on the safety issues. Devices have low computational energy and memory the present security mechanisms, need to additionally be optimized thus or an easy slate technique wishes to be followed [27].

Today, the IoT has become one of the very most encouraging communication paradigms, and one in which all the smart objects within our lifestyle become the main Internet owing to their interaction and processing capabilities. That possibility delivers with it new safety issues for IoT applications. That is, each intelligent object might develop into a vulnerable entry point for any malicious attack. Two security issues, i.e. physical protection for smart objects, and how to maintain data confidentiality, integrity and privacy during data collection among smart objects, have thus emerged. This is because traditional security protection mechanisms might not be ideal for smart objects. For example, firewalls containing network management control protocols are able to manage high-level traffic through the Internet. However, this application-level solution is not suitable for endpoint devices in IoT applications because these devices usually possess a specific, defined mission with finite resources present to usage of it. Therefore, the refinement of traditional security solutions to fit the specific security requirements of IoT-based smart objects is one of the most promising ways of securing IoT-based application systems [4],[19].

The machine-to-machine connection, allowing instant and sent methods to change numerous data without specific involvement, is extremely encouraging methods of Internet of Things (IoT). As time goes on, the M2M connection is likely to make a few applications, such as e-health, intelligent grids, automata in industry and surrounding monitoring, to produce a significant industry with a lot of possibilities, create a great deal more advantages to humans. Machine-to-Machine (M2M) transmission, one or more entities, do not necessarily require human interaction or intervention in the process of communication [9],[13].

Generally, protection is resolved throughout the system living pattern, including protected booting, access control and authentication of products, system management, fire wall, IDS/IPS and improvements and patches. Among these, unit authentication (with protected device-to-device communication) has been revealed to supply significant advantages to the protection paradigm of IoT system structure and unique vital components in IoT protection ecosystems. In an IoT-based application, smart items often cannot be self-interacted with an individual or the backend program, and often need you to definitely input the qualifications required to provide access to the communication network. Fortuitously, unit authentication enabling a computer device usage of a system centered on a qualifications set pre-stored in a protected storage of the device itself, represents a possible way to resolve this predicament [3].

Together possible program, the common health-care service helps remote checking health position of people in real time. Several 6LoWPAN centered health-care systems, such as for example those in have now been planned to provide efficient, variable and reliable companies for checking and tracking people, staffs, and also bio-devices. The integration of the IP technology in low energy wireless devices can achieve end-to-end real-time communications, letting that the healthcare specialists identify the disease by the information of the people obtained from specifically remotely managed wearable devices via the Internet. Yet another probable program is to monitor the manufacture method in business, wherever varied devices, actuators and controllers are connected together to achieve inactive checking and productive control and automation. The 6LoWPAN project optimizes the traditional IP methods to enable efficient indication of IPv6 packages over the wireless networks. The mechanism includes four steps including node recognition, node authorization, certified node record propagation and knowledge filtering which derive from some current 6LoWPAN common protocols [5],[11],[12].

Target of protocols in transmission is to grant the delivery, storage and routing of information or data without requirement of implementation of different schemes in heterogeneous devices or application [21].

2. LITRATURE SURVEY

Knowledge safety is essential idea in the network as the data to be transferred must be made secure. To reach the network data safety the prevailing calculations like AES (Advance Security Standard), IDEA (International Knowledge Security Algorithm) etc. The info encryption and decryption is completed for 128 bits. To produce data better AES-192 or AES-256 portions can be used. In that sensor data can be made secure for IoT applying cryptography [1].

In Safety difficulties in the portable and IoT System pro-gram, Safety difficulties related with the IoT portable program are studied. Some safety difficulties like late recognition, hardware bug, data vulnerabilities in the computing devices even as we transfer to the regime of Web of Things. Many of them are the reincarnations of the old difficulties e.g., hardware/software validation, safety, etc. Safety conflicts like Reusability, Late Variability, Self-Securability, etc. are the portable and IoT system issues [2].

IoT is just a recent technology that enables the customers to connect everywhere, anytime, anyplace and to anyone. The various medical solutions of IoT such as for example Surrounding Assisted Residing (AAL), Web of m-health, com-munity healthcare, oblique disaster healthcare and embedded gateway configuration are surveyed. Further, the applications of IoT in detecting the glucose level, ECG tracking, blood stress tracking, wheelchair administration, and treatment administration and rehabilitation system are analyzed. The evaluation results show that the usage of IoT in the medical area increases the standard of living, user knowledge, patient outcomes and real-time illness management. The introduction of medical IoT isn’t without safety challenges. Hence, the safety threats such as for example confidentiality, authorization, privacy, accessibility get a grip on, trust, and policy enforcement are analyzed. The current presence of these threats influence the performance of IoT, thus, the cryptographic calculations like Advanced Security Standard (AES), Knowledge Security Standard (DES) and Rivest-Shamir-Adleman (RSA) are used. The investigation on these methods proves that the RSA gives better safety compared to the AES and DES algorithms [4].

Three key characteristics of IoT, such as heterogeneity, resource constraint, and dynamic environment to find out basic IoT security requirements. In addition, we analyzed overall IoT security requirements (e.g., privacy, trust, control system security) based on security issues of six key elements in IoT environment. And security requirements evaluation is performed with several researches. Most of the researches deal with only the security requirements about privacy, access control (i.e., authentication and authorization), and security threats. That is, the existing researches do not cover overall security requirement for IoT environment. The basic security requirements based on the three characteristics (i.e., heterogeneity, resource constraint, dynamic environment). Second, privacy, multicasting and bootstrapping in IoT network, availability, data protection, etc. were analyzed based on six elements (i.e., IoT network, cloud, user, attacker, service, and platform) in IoT environment [28].

A secure healthcare process on BSN architecture for IoT-oriented, where two validation techniques, planned to fulfill significant safety requirements. Even though computation price is user affordable, machine effectiveness, improvised when replaced by crypto-hash-modules substituted by the original SHA-2 techniques [2].

To increase safety performance of M2M communications in 6LoWPAN sites, EAKES6Lo technique has been provided. Hybrid cryptography has been applied to offer secure data transactions one of the 6LHs, the 6LRs, the 6LER and the distant server. The EAKES6Lo scheme is safe and can effectively reduce numerous harmful problems including replay problems, man-in-the-middle problems, impersonation problems, and Sybil problems, etc. [1].

Session key establishment with light weight public key cryptography and pairwise key during mutual authentication stage are used in SAKES to provide authentication between M2M device communications on 6LoWPAN network. DoS attacks can be avoided using this technique [17].

Light weight mutual authentication is achieved with series of messages in machines like server, node, router etc., in network with hash and XOR operation perform on parameters of communicating devices. Session key agreement, device info confidentiality and attack resistance is gain along with low computation cost, storage overhead and communication load [16].

Security strategy centered on XOR adjustment is used. Establish the shared certification method in a normal RFID program for IOT applications. Unique RFID standards imperfections and disadvantages may be increased applying the current cryptography protocol [25].

Observed as a encouraging strategy that stretches the CPSs over all actions to the professional domain. ICPSs are observed as enablers toward potential culture perspective conclusion and aim achievement [24].

Examined the seven primary attributes which are expected by multicast authentications for resource-constraint applications. Unique Nybergs rapidly one-way accumulator and build a light multicast certification mechanism [22].

An IPv6 (Internet Protocol version 6) around Low-power wireless personal area network (6LoWPAN) common has been presented, by the IETF (Internet Engineering Task Force), to be able to promote and use the progress of the IoT and M2M programs area. 6LoWPAN provides IP-based units to interconnect to the internet for M2M communication. Most importantly, possible software is always to check the production method in market [19], [20], wherever numerous detectors, actuators, and controllers are linked together to attain inactive checking and productive get a handle on and automation.

3. SYSTEM ARCHITECTURE

A. Problem Statement

In Today’s IoT time, different safety problems arises as a result of problems on the network, purposes, etc. To prevent problems the safety of the applying needs to improve. So that the information privacy can be secured from the attackers. Detectors of IoT keeps data that will influence the applying along using its user. So to avoid this situation build the machine that will reduce steadily the problems on the privacy of the information in the sensor.

In this, you can find few data safety systems like security, decryption, etc. that will improvise the privacy and safety but not at level where purposes will be strike free. Proposing the machine that will maintain the safety of the information on the network in addition to IoT application.

B. **System Overview**

The architecture shows the proposed system which consist of the human body sensor, hand-held device, server/cloud. In proposed system, the communication between the all the modules will be EAKES6Lo communication i.e. Enhance Authentication and Key Establishment Scheme for device-to-device communication in 6LoWPAN network. Data collected from the sensors will be encrypted with the encryption algorithm like RSA. The encrypted data will be then transfer over the network with the help of the tickets on the each level. EAKES6Lo communication contains two stages:

1) Pre-deployment stage,
2) Authentication and key establishment stage,

As the data passes through the network hand-held devices also provides the data security at its own phase. At the last phase the collected data can be stored on the network cloud or server and then further processing can be done.

4) Reduce the attacks on M2M device communication.
5) Improve the efficiency of communication.
6) To reduce the computational cost.

4. METHODOLOGY

A. Algorithm

1) Start
2) Do node registration.

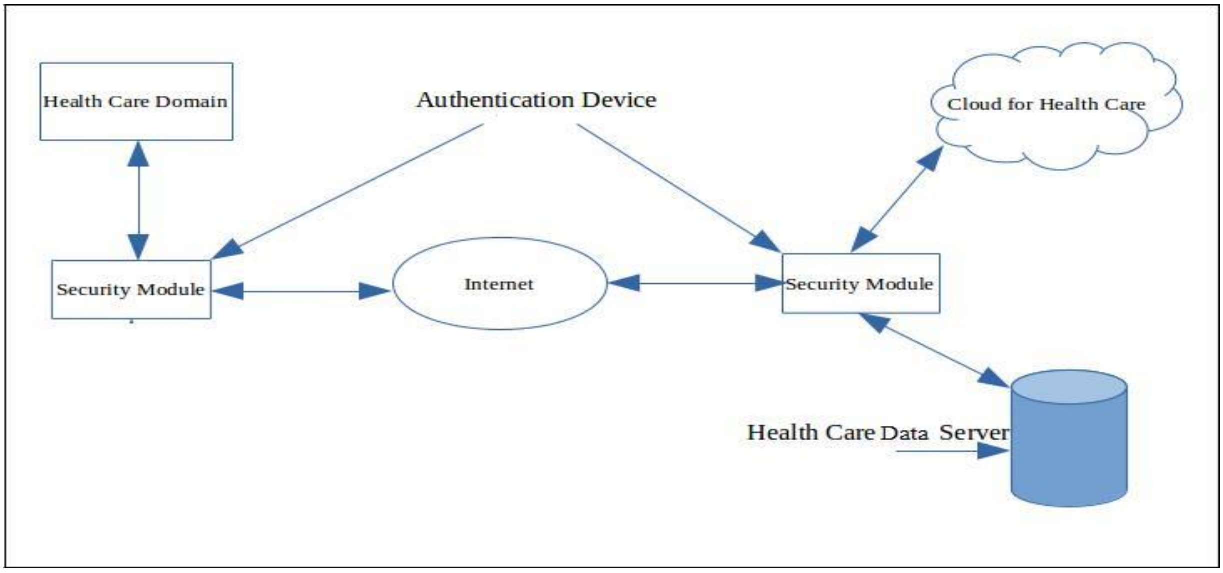


Fig. 1 Security using Proposed Scheme

In the first phase of proposed system the nodes will be registered with the server. These registered node will establish the EAKES6Lo communication between the nodes and server. In the second phase the data will be collected, encrypted and transfer over the network for the storage. At the same time server will check the node authentication and registration. If the node is new the registration will take place else the authentication validity will be checked. If the node is unauthorized the same will be notified to the authority for further process. Thus, proposed system will provide the sensor data security and privacy from the malicious attackers.

C. Objectives

1) Provide security to vital info data while giving control to authorized person.
2) Protect the authentication and access control rights for resources.
3) Improve the quality of communication.

3) Check the parameters for the message security on secure channel.
4) Do authentication on the parameter considered like session key, hash function, XOR operation.
5) If parameters in the authentication message does not match with calculated pair decline the access permission.
6) Else grant a secure communication link.
7) Generate secure communication between nodes.
8) Once communication is over dismantle the link or registration of node.
9) End

5. PROBLEM FORMULATION

A. Mathematical Model

The overall system model specific are given by mathematical model with inputs and their respective reposes to the given inputs. It also provides the several states which describe the functional modules of the problem, data flow, initial and final states of the system along with dynamic and static data required and given by the system along with user. Generalized mathematical model of the proposed system will be as:-

1) Problem Description: The System can be mathematically defined as a collection of three tuples. S can be written as:

$$S = \{I, O, A\} \quad (1)$$

Where,
I = Input (Nodes)
O = Output (Secure Communication)
A = Set of Procedures (Registration, Authentication, Key Establishment etc.)
Input X = Nodes in the network i.e.

$$X = \{x_1, x_2, \dots \dots \dots, x_n\} \quad (2)$$

Output Y = Secure Communication i.e.

$$Y = \{y_1, y_2, \dots \dots \dots, y_n\} \quad (3)$$

Set of Procedure

1) System Initialization

Input = Communication Nodes.
Output = Establishment of links.

2) Registration
Input Nr = No. of nodes.
Output Or = Node registration.

$$R = \sum_{i=0}^{n} (Nri) = \{Nr_0, Nr_1, \dots \dots \dots, Nr_n\} \quad (4)$$

Where i, n > 0

System Sr= Perform registration and establish the connection between node and server.

3) Authentication
Input Na = Check the registration.
Output Oa= Authenticate the node.

$$A = \sum_{i=0}^{n} (Nai) = \{Na_0, Na_1, \dots \dots \dots, Na_n\} \quad (5)$$

Where i, n > 0

4) Key establishment
Input Nk= Authenticate node.
Output Ok = Key establishment between node and server.

System Sk= Elliptic curve Diffie-Hellman.
p = Field that the curve is defined over.
A, B = Values that define the curve.
G = Generator point.
n = Prime order of G.
Private/public key pair.
Private: Random value d. Where $1 \leq d \leq n - 1$
Public:

$$d * G = (X_G, Y_G) \quad (6)$$

Public generator point of A and B

$$P = d * G \quad (7)$$

$$Q = e * G \quad (8)$$

Private keys of A and B

$$R = d * Q \quad (9)$$

$$R = e * P \quad (10)$$

$$R = d * e * G = (X_R, Y_R) \quad (11)$$

X and Y coordinates of point

Each procedure will be perform on the input to generate the secure communication link between the nodes in 6LoWPAN network.

6. RESULT ANALYSIS

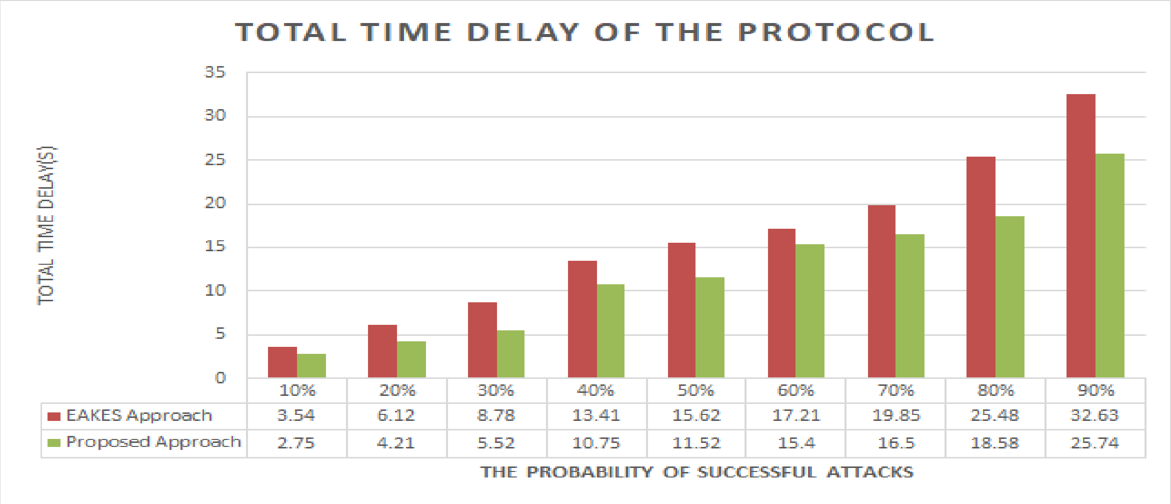
Proposed system is compared with existing system for efficiency and performance overhead. Results are depicted in terms of parameters viz. total time delay on server and protocol, probability of successful attacks and transmission data analysis on nodes. Given graphs shows performance and efficiency of proposed scheme over EAKES6Lo scheme.

Fig. 2 represents the time delay on protocol to analyze the attack on the transmission network between existing and proposed scheme. Probability of successful attack on protocol is analyzed with time delay in identification of attacks on devices.

Fig. 3 given upward shows the comparison between the EAKES6Lo scheme and proposed system at server side for efficiency of proposed scheme to identify the attacks on server area.

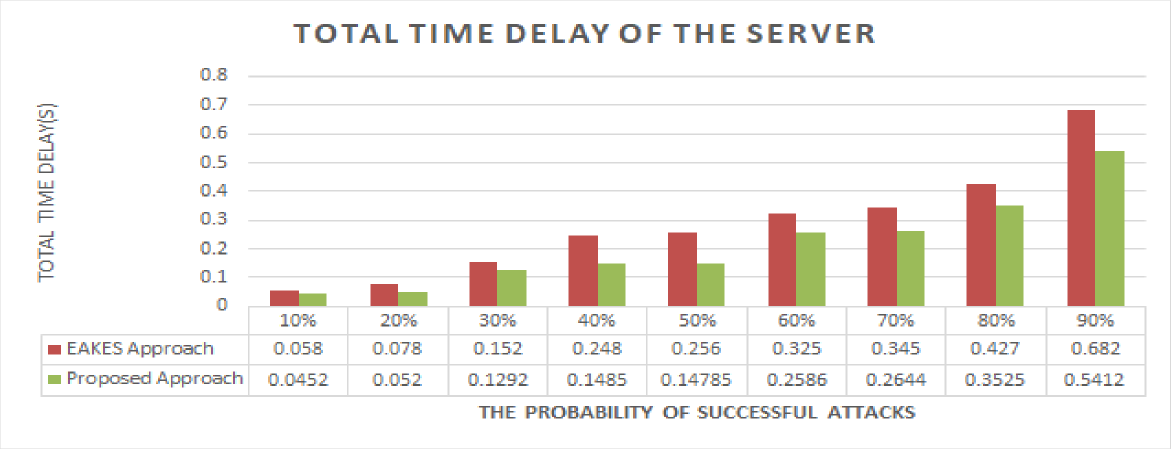
Fig. 4 presents shows the data analysis of proposed scheme when the quantity of data on network will vary the scheme is superior to EAKES6Lo scheme.

Fig. 4 Data Size Analysis



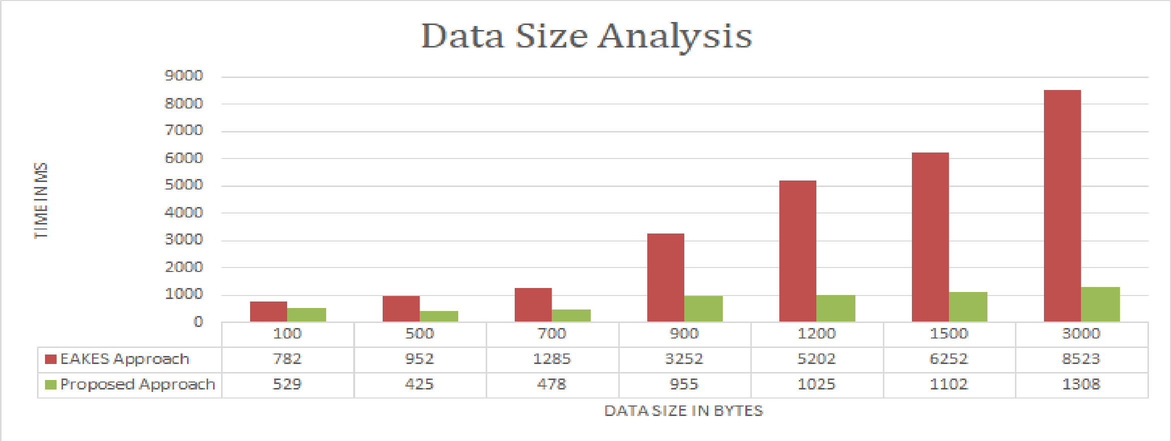
	10%	20%	30%	40%	50%	60%	70%	80%	90%
🟥 EAKES Approach	3.54	6.12	8.78	13.41	15.62	17.21	19.85	25.48	32.63
🟩 Proposed Approach	2.75	4.21	5.52	10.75	11.52	15.4	16.5	18.58	25.74

Fig. 2 Time Delay of Protocol



	10%	20%	30%	40%	50%	60%	70%	80%	90%
🟥 EAKES Approach	0.058	0.078	0.152	0.248	0.256	0.325	0.345	0.427	0.682
🟩 Proposed Approach	0.0452	0.052	0.1292	0.1485	0.14785	0.2586	0.2644	0.3525	0.5412

Fig. 3 Time Delay of Server



	100	500	700	900	1200	1500	3000
🟥 EAKES Approach	782	952	1285	3252	5202	6252	8523
🟩 Proposed Approach	529	425	478	955	1025	1102	1308

Fig. 4 Data Size Analysis

7. CONCLUTION

Network sensing devices in IoT deployment being interlink will provide new IoT application, standard deployment and development platform. Security as key characteristic for application development will lead to improvising the standard and quality of application. Security attacks on application, network, devices reduced by proposed system. Performance of devices and their application also improved. Proposed system and study of issues, protocols, techniques to overcome the attacks and ongoing research in the field is done.

Acknowledgment

I would sincerely like to thank our Professor Amit H. Palve, Department of Computer Engineering, SITRC, Nashik for his guidance, encouragement and the interest shown in project by providing valid suggestions in working field. His expert guidelines and scholarly feedback had greatly affected the effectiveness of research work.

REFERENCES

[1] Yue Qiu, Maode Ma,”A Mutual Authentication and Key Establish-ment Scheme for M2M Communication in 6LoWPAN Networks”, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, 2016, pp. 1-11.

[2] Kuo-Hui Yeh , ”A Secure IoT-based Healthcare System with Body Sensor Net-works”, IEEE Access, 2016, pp. 1-12.

[3] F. Touati, A. B. Mnaouer, O. Erdene-Ochir, W. Mehmood, A. Hassan, and B. Gaabab, ”Feasibility and Performance Evaluation of a 6LoWPAN-enabled Plat-form for Ubiquitous Healthcare Monitor-ing”, Wireless Communications and Mobile computing, vol. 16, 2016, pp.1271-1281.

[4] Oladayo Bello, Sherali Zeadally, ”Intelligent Device-to-Device Communication in the Internet of Things”, IEEE Systems Journal, Volume 10, Issue 3, September 2016, pp. 1172-1182.

[5] S. Misra, S. Goswami, C. Taneja, A. Mukherjee, and M. S. Obaidat, ”A PKI Adapted Model for Secure Information Dissemination in Industrial Control and Automation 6LoWPANs”, IEEE Access, vol. 3, 2015, pp. 875-889.

[6] Lus M.L. Oliveira, Joel J. P. C. Rodrigues, Amaro F. de Sousa, Victor M. Denisov, ”Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms”, IEEE Transactions on Industrial Informatics, 2016, pp. 1-10.

[7] Morris J. Dworkin, ”SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions”, NIST FIPS-202, dx.doi.org/10.6028/NIST.FIPS.202, Au-gust 2015.

[8] Minkeun Ha, Seong Hoon Kim, Daeyoung Kim, ”Intra-MARIO: A Fast Mo-bility Management Protocol for 6LoWPAN”, IEEE TRANSACTION ON MO-BILE COMPUTING, VOL. XX, NO. XX, 2015, pp. 1-14.

[9] S. Chen and M. Ma, ”A Dynamic-Encryption Authentication Scheme for M2M Security in Cyber-Physical Systems”, Proc. 2013 IEEE Global Communications Conf. (GLOBECOM), 2013, pp. 2897-2901.

[10] Huansheng Ning, Hong Liu, Laurence T. Yang, ”Aggregated-proof Based Hierarchical Authentication Scheme for the Internet of Things”, IEEE Transactions on Parallel and Distributed Systems, Volume 26, Issue 3, 2015, pp. 657-667.

(A.1)

[11] C. Hennebert and J. D. Santos,”Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis”, IEEE Internet of Things Journal, vol. 1, 2014, pp. 384-398.

[12] Prosanta Gope, Tzonelih Hwang,”BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network”, IEEE Sensor Journal, Volume 16, Issue 5, March 2016, pp. 1368-1376.

[13] J. Kim, J. Lee, J. Kim, and J. Yun,”M2M Service Platforms: Survey, Issues, and Enabling Technologies”, IEEE Communications Surveys & Tutorials, vol. 16, 2014, pp. 61-76.

[14] Sravani Challa, Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Alavalapati Goutham Reddy, Eun-Jun Yoon, Kee-Young Yoo, E. - J. Yoon, ”Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications”, IEEE ACCESS, 2016, pp. 1-16.

[15] Yunqiang Liu, Guanhua Zhang, Wenjie Chen, Xinming Wang, ”An Efficient Privacy Protection Solution for Smart Home Application Plat-form”, 2016 2nd IEEE International Conference on Computer and Communications, 2016, pp. 1-5.

[16] Alireza Esfahani, Georgios Mantas, Rainer Matischek, Firooz B. Saghezchi, Jonathan Rodriguez, Ani Bicaku, Silia Maksuti, Markus Tauber, Christoph Schmittner, and Joaquim Bastos, ”A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment”,IEEE,2017.

[17] H. R. Hussen, G. A. Tizazu, M. Ting, T. Lee, Y. Choi, and K.-H. Kim,” Sakes: Secure authentication and key establishment scheme for m2m communication in the ip-based wireless sensor network (6lowpan),” in Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on. IEEE, 2013, pp. 246251.

[18] J. L. Hernandez-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, ”Toward a lightweight authentication and authorization framework for smart objects,” IEEE Journal on Selected Areas in Communications, vol. 33, no. 4, April 2015, pp. 690702.

[19] L. D. Xu, W. He, and S. Li, ”Internet of things in industries: A survey,” IEEE Transactions on Industrial Informatics, vol. 10, no. 4, Nov 2014, pp. 22332243.

[20] R. Sadeghi, C.Wachsmann, and M.Waidner, ”Security and privacy challenges in industrial internet of things,” in 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), June 2015, pp. 16.

[21] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, ”Massive internet of things for industrial applications: Addressing wireless iiot connectivity challenges and ecosystem fragmentation,” IEEE Industrial Electronics Magazine, vol. 11, no. 1, March 2017, pp. 2833.

[22] X. Yao, X. Han, X. Du, and X. Zhou, ”A lightweight multicast authentication mechanism for small scale iot applications,” IEEE Sensors Journal, vol. 13, no. 10, Oct 2013, pp. 36933701.

[23] W. L. Chin, Y. H. Lin, and H. H. Chen, ”A framework of machine-to- machine authentication in smart grid: A two-layer approach,” IEEE Communications Magazine, vol. 54, no. 12, December 2016, pp. 102107.

[24] W. Colombo, S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin,”Industrial cyberphysical systems: A backbone of the fourth industrial revolution,” IEEE Industrial Electronics Magazine, vol. 11, no. 1, March 2017, pp. 616.

[25] J. Y. Lee, W. C. Lin, and Y. H. Huang, ”A lightweight authentication protocol for internet of things,” in 2014 International Symposium on Next-Generation Electronics (ISNE), May 2014, pp. 12.

[26] Shivaji Kulkarni, Shrihari Durg, Nalini Iyer, ”Internet of Things (IoT) Security,” IEEE, 2016, pp. 821-824.

[27] KrishnaKanth Gupta, Sapna Shukla,”Internet of Things: Security Challenges for Next Generation Networks,” 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016), 2016.

[28] Se-Ra Oh,”*Young-Gab Kim, Security Requirements Analysis for the IoT,” IEEE, 2017.

[29] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, Denial-of-Service Detection in 6LoWPAN based Internet of Things, Proc. 2013 IEEE 9th Int.Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 600-607, 2013.

[30] Ankush B. Pawar, Dr.Shashikant Ghumbre, A Survey On IoT Applica-tions, Security Chellenges And Counter Measures, 2016 International Conference on Computing, Analytics and Security Trends (CAST), 2016, pp. 294-299.