Volume 6, Issue 10, October 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Authentication in IoT Environment: A Survey

R. Shantha Mary Joshitta*
Research Scholar, Department of Computer Science,
St. Joseph's College (Autonomous), Tiruchirappalli,
Tamilnadu, India

L. Arockiam
Associate Professor, Department of Computer Science,
St. Joseph's College (Autonomous), Tiruchirappalli,
Tamilnadu, India

Abstract— The new paradigm Internet of Things links all objects to the Internet and allows them to sense cum communicate with themselves and the external world. This ecosystem enhances productivity, creates new business models, and generates new revenue streams. It enables an enormous exchange of data which was never available before but posts challenges in bringing users' information in a secure way. Safeguarding the connected IoT devices and networks are much crucial and very difficult because of the nature of IoT system. This paper reviews the already existing IoT authentication literatures for secure transmission of data and presents an analytical survey of the existing work. And also, the authors outline the potential issues and challenges of authentication in IoT for further research.

Keywords— Authentication; IoT Environment; Analytical Survey; Issues and challenges in IoT Authentication.

I. INTRODUCTION

In the beginning of this era, not only living being interact but also devices communicate with each other. This type of device communication is called Internet of things (IoT) and has fascinated the attention as realized as the future world. In an IoT environment, more devices are connected day-by-day. This growth brings several benefits to carry out day-to-day tasks. But, these benefits become a risk, as the hackers and cyber criminals are more and more. These tremendous security threats have drawn much attention from the researchers and academicians. Providing a right security to the Internet of Things will build confidence in the increasingly connected world. So, this research considers authentication of IoT environment as its core and works on designing a lightweight authentication mechanism for IoT devices and users.

II. AUTHENTICATION OF IOT DATA

Authentication is the process of recognizing users and devices in a network and limiting admittance to authorized persons and non-manipulated devices. This process actually relies on username and password and do not work with unattended devices. Authentication can be of one-way authentication and mutual authentication. In an IoT environment, the object authenticates the server and vice-versa. Here, the server is managing security certificates provided by the IoT devices. So, only legitimate users and servers can participate in the information transfer. Figure 1 depicts the communication scenario of IoT environment.

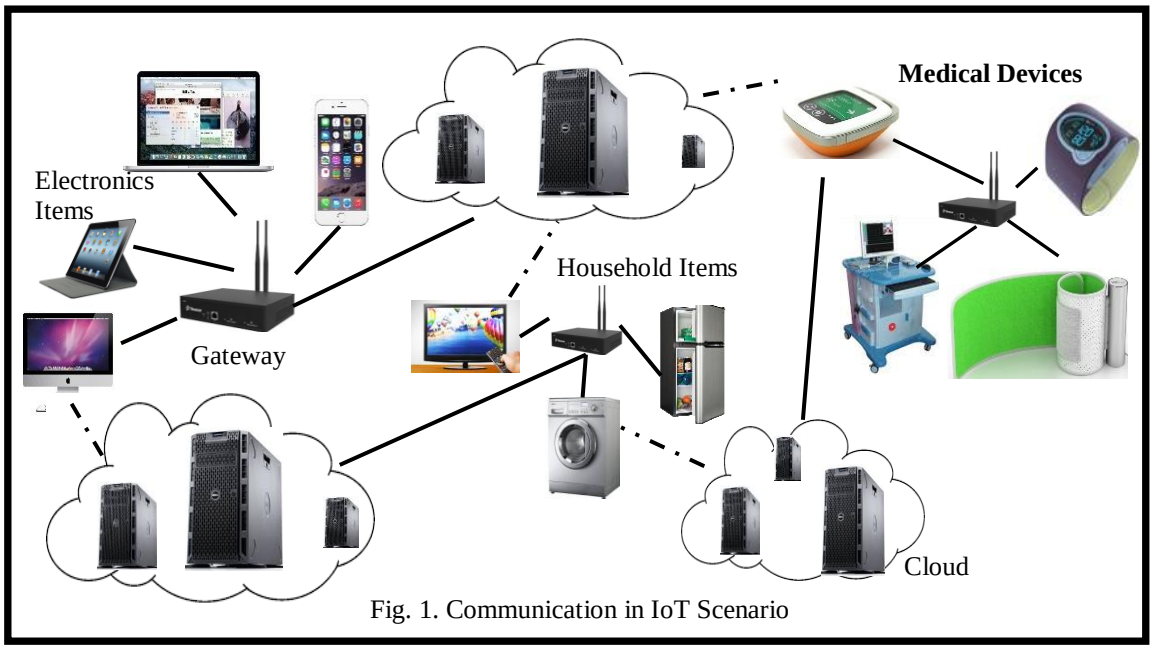

Fig. 1. Communication in IoT Scenario

III. RELATED WORKS

Anjali Yeole et al. offered a two way authentication scheme along with dynamic variable cipher security certificate [1]. They used hash algorithm to provide an asymmetric two-way authentication scheme between the platform and terminal. They combined one time one cipher method in communication process. They compared the performance of the present and the proposed security protocols. In the proposed scheme, the terminals were authenticated themselves based on secure hash function to ensure their identity and simulated in Contiki OS using COOJA simulator. The proposed scheme was well suited for authenticating short range technologies.

Ajit A. Chavan et al. used combination of CoAP and DTLS compacted by 6LoWPAN standards for confidential communication within constrained devices [2]. These compressed DTLS diminished packet size and evaded fragmentation. And also they used raw public key to authenticate the multi-vendor constrained devices. Results showed that CoAPs with raw public key provided communication security and authentication portability in multi-vendor environment at negligible energy usage. The proposed scheme improved the interoperability as well as lifetime of network.

Byung Mun Lee proposed an authorization protocol in a NFC P2P mode [3]. The author connected a mobile device with the public health device using NFC P2P facility and used intelligent service algorithm. The proposed protocol had an authorization facility to govern the sharing of devices with the public. Debiao He et al. deliberated the security necessities of RFID authentication mechanisms [4]. They presented a review of these authentication schemes based on performance and security. They pointed out that many authentication schemes could not satisfy all security requirements, but had satisfactory performance. They suggested three ECC-based authentication schemes for the healthcare environment.

C. Gehrmann et al. presented SMACK, a security service based on short Message Authentication Codes (MACs) [5]. This code detected the invalid messages while receiving and reduced the impact of Denial of Sleep attacks. They suggested a tunable and adaptive reaction mechanism to detect invalid messages. It specifically addressed Denial of Sleep attacks and forestalling battery exhaustion. They experimentally evaluated SMACK performance through proposed prototype implementation for the resource constrained CC2538 platform. It was efficient in terms of memory requirements, energy consumption and computing time. Also, the proposed approach detected invalid messages while displaying a smaller computing overhead, and required no additional communication with the constrained device.

Hamza Khemissa et al. proposed a new lightweight authentication scheme for an e-health application [6]. The proposed scheme allowed sensors and the Base Station (BS) to authenticate the secure collection of health-data. It used nonces and Keyed-Hash message authentication to check the integrity of authentication exchanges. It provided authentication with less energy consumption, and it terminated with a session key agreement between sensor and the Base Station. The proposed scheme was assessed by a performance and security analysis. The test results showed that it saved energy and was resistant against different types of attacks.

Hamza et al. designed a new lightweight authentication scheme for resource constrained environment [7]. It allowed both the sensor and the remote user to authenticate each other for secure communication. It used nonces, exclusive-or operations and Keyed-Hash message authentication to check the integrity of the different exchanges. It provided authentication with less energy consumption. Jia-Li Hou et al. suggested a sensor based communication architecture for IoT healthcare systems [8]. A secure single sign-on authentication scheme and a robust co-existence proof protocol were explained. The proposed method used SSO technique along with one-way hash function and random nonce to provide security and efficiency.

Jose L. Hern´andez-Ramos et al. proposed few lightweight authentication and authorization schemes for smart objects [9]. These mechanisms were framed within a proposed security framework, the Architectural Reference Model (ARM). The resulting architecture provided a holistic security approach in the design of lightweight security protocols for IoT environments. S. Kalra et al. proposed a mutual authentication protocol for communication of embedded devices and cloud servers [10]. It achieved mutual authentication and provided essential security requirements. It was proved against multiple security attacks. Verification of the proposed protocol was performed using AVISPA tool, which confirmed its security in the presence of a possible intruder.

Luciano Barreto et al. presented an architectural model and use cases based on the Identity Provider / Service Provider (IdP/SP) model [11]. The authors discussed the IoT Cloud security and presented a generic authentication system blueprint for IoT Clouds. They described several authentication use cases for IoT Cloud and the resulting protocol was formalized by means of different sequence diagrams. Manoj Kumar classified the ECC-based RFID authentication schemes based on its types such as heavyweight, middleweight, and lightweight schemes [12]. Performance and security of these schemes were evaluated based on communication cost and storage requirements. The author expressed his concern over the malicious attacks on ECC-based RFID schemes which provided better security.

Mian et al. proposed a lightweight mutual authentication scheme to validate the identities of the devices for the resource observation [13]. The presented scheme incurred less connection overhead and provided a robust defense solution to fight various types of attacks. The authors had chosen CoAP as the underlying application layer protocol for enabling communication among various physical objects. Oladayo Bello et al. presented the achievement of intelligent D2D communication in IoT ecosystem [14]. They focused on implementation of routing algorithms to achieve intelligent D2D communication in IoT. They presented various types of communications such as D2D, device to human and vice versa, and device to distributed storage. The IoT device operations on constrained and unconstrained networks and usage scenarios of D2D communications were also elaborated. The authors classified routing algorithms and protocols for intelligent D2D communication in IoT. They outlined the future challenges based on communication resource optimization, optimized route discovery and management, cooperation between devices and security.

Pablo Punal Pereira et al. presented a CoAP-based scheme for service-level access control on power limited devices [15]. They provided a holistic framework for secure SOA-based low power networks using resource limited devices. Using this, a device could allow read / write access to its service to one group of users and the other group members could read its content only. Users without the right credentials were not even allowed to discover available services. The authors presented several implementations along with test results. Pádraig Flood et al. presented a new protocol to combine zero-knowledge proofs [16]. They also offered key exchange mechanisms to authenticate communication in machine-to-machine (M2M) networks. It addressed all the issues with limited computational resources and could be deployed in wireless sensor networks. The authors proposed another method for peer-to peer authentication. In the proposed method, encryption was based on the GMW graph isomorphism zero knowledge protocol and the DH key exchange. The new method lacked the flexibility of a public key cryptosystem, but avoided the complexity of a public-key.

Pawani Porambage et al. projected an implied certificate-based authentication scheme for Wireless Sensor Networks in distributed IoT use cases [17]. They had developed two-phase authentication protocol for sensor nodes and the end-users to authenticate and start secure communications. The proposed protocol strengthened the resource constrained sensor nodes, heterogeneity and scalability of the network. The performance and security analysis was justified to deploy WSNs. K. A. Rafidha Rehiman et al. introduced a zero knowledge protocol with accumulated hashing function [18]. It provided a secure authentication to sensor enabled mobile devices in IoT and allowed a communication party to prove his known secret without revealing the secret. The verifier only knew the integrity of the information. To ensure confidentiality in communication, the authors proposed key exchange in current time. The proposed method fulfilled the need of resource constrained mobile devices.

Rene Hummen et al. identified resource requirements for the DTLS handshake for peer authentication and key agreement purposes [19]. They proposed a delegation architecture to offload the expensive DTLS connection to a delegation server. The proposed delegation architecture reduced the resource needs of DTLS-protected communication for controlled devices. It provided authorization functionality in the connection establishment. They presented a comprehensive result for authentication, authorization, and protected data communication in the IP-based IoT. The evaluation results showed that the proposed architecture reduced the memory overhead by 64 %, computations by 97 % and network transmissions by 68 % compared to a public-key-based DTLS handshake.

S R Moosavi et al. developed an authentication and authorization architecture for IoT-based healthcare [20]. The resource constraint medical sensors had drawbacks to utilize conventional cryptography. The authors presented an architecture for authentication and authorization of a remote end-user. The proposed architecture was more secure than a centralized delegation-based architecture. It used a secure key management scheme between sensor nodes and the smart gateway. The impact of DoS attacks was also reduced. Sanaz Rahimi Moosavi et al. designed an authentication scheme for RFID implantation system [21]. They used elliptic curve cryptography and the D-Quark lightweight hash design in their proposed scheme. The small key sizes and the efficiency of the elliptic curve-based cryptosystems made them select ECC algorithm for their computations. The projected authentication scheme was secure against the pertinent threat models and offered a higher security level. The proposed system gave 48 % less communication overhead and 24 % less memory need than the previous systems.

Shantha Mary Joshitta et al. presented an overview of security issues in IoT environment [22]. They presented the existing research work in IoT security and outlined the research issues in confidentiality, integrity, authentication, authorization, availability and privacy. Shivraj V L et al. reviewed an authentication scheme based on One Time Password (OTP) for IoT and proposed a scalable OTP scheme [23]. The authors evaluated the performance of the scheme and observed that the proposed scheme with a smaller key size and lesser infrastructure performed on par with the existing OTP schemes without compromising the security level. It could be implemented in real-time IoT networks and good for two-factor authentication among devices, applications and their communications.

Usha devi et al. proposed two different approaches in authentication scheme [24]. If an IoT device tried to connect to the network of the same area, the basic information of the device was collected, stored in a database and updated frequently. This existing user was authenticated by login id and hashing password or with the MAC passwords. It had resistance against node compromise, computation and communication overheads, message entropy and robustness to packet loss. It was used to authenticate the end user and the sensor network data in a smart house application. Vitaly Petrov et al. described a user authentication paradigm called as “wireless key” [25]. Using this, a many-to-many authentication scheme with passive NFC tags was proposed. The authors suggested to use a passive NFC tag to minimize the key size and reduce the cost. The security of data on the tag was guaranteed by a specific data encryption scheme developed on the top of strong cryptographic primitives. It presented a user-friendly, cost-efficient and secure solution which could be applied to Bluetooth Low Energy and Wireless USB.

Yuichi K et al. focused on data collection for location-based authentication system [26]. The authors proposed a data collection method considering the requirements from the authentication system. The proposed work was considered as a significant contribution to the future industrial IoT society. In addition, they demonstrated the method for optimizing the operation of the proposal by using mathematical analysis. Moreover, the efficiency of the proposed method was validated through numerical results.

IV. ANALYTICAL SURVEY ON EXISTING WORKS

An analytical survey of the existing literatures studied and presented in Table 1. The (□) – mark refers that the specified attribute was enhanced in the specified research work whereas (□) denotes that there was a considerable degradation in that attribute. (-) indicates that, that particular attribute was not discussed in that literature.

Table. 1. Analytical Survey of Existing Literatures

S.No.	Reference No.	Authentication	Authorization	Security	Performance	Computation Cost	Communication Cost	Scalability	Routing	Energy Efficiency	Memory Overhead
1.	[04]	□	-	□	□	□	□	-	-	-	-
2.	[18]	□	-	-	□	□	□	-	-	□	□
3.	[14]	□	-	□	□	-	-	-	□	-	-
4.	[09]	□	□	□	-	-	-	-	-	-	-
5.	[17]	□	-	□	□	□	-	□	-	□	-
6.	[03]	-	□	-	-	□	-	-	-	□	-
7.	[21]	□	-	□	□	□	□	-	□	-	-
8.	[19]	□	□	□	-	□	-	-	-	-	□
9.	[01]	□	-	□	-	-	□	-	-	-	-
10.	[07]	□	-	□	□	-	□	-	-	□	-
11.	[06]	□	-	□	□	-	□	-	-	□	-
12.	[25]	□	-	□	-	□	-	□	-	□	-
13.	[26]	□	-	□	□	-	-	-	-	-	-
14.	[20]	□	-	□	□	-	□	□	-	□	-
15.	[08]	□	-	□	□	-	-	-	-	-	-
16.	[21]	□	□	□	□	-	□	-	-	-	□
17.	[12]	□	-	□	□	-	-	-	-	-	-

V. OPEN ISSUES AND CHALLENGES

From the comprehensive literature review of existing mechanisms, it is evident that there are some major issues and challenges in Authentication in IoT environment. These issues and challenges are highlighted and categorized based on the architectural layers.

5.1. Issues in Data Acquisition Layer:

- Mutual authentication
- Integrity
- Confidentiality
- Anonymity
- Availability
- Forward security

5.2. Issues in Data Transmission Layer:

- Node compromise
- Communication overhead
- Robustness to packet loss
- Message entropy

5.3. Issues in Application Layer:

- Computation overhead
- Data Storage and Retrieval
- Device identification
- Data extraction

After reviewing the aforementioned literatures, the motivational points for this paper are listed below.

- ✓ Ensuring security is extremely challenging because of the characteristics of IoT [29].
- ✓ It will take more than 10 years for IoT concept to reach the Plateau of Productivity because of its security challenges, data and wireless standards and privacy policies [27]
- ✓ Communication of collected information has to ensure the integrity and confidentiality [29].
- ✓ A secure communication channel should be implemented and a light weight authentication should be provided for IoT [24]
- ✓ IoT is extremely vulnerable to different attacks due to its wireless communications [7]
- ✓ Data access should be guaranteed only to authorized people [29]

- ✓ Encryption algorithms need to be less energy consuming but more efficient, and efficient key distribution schemes need to be well-defined [30]
- ✓ Most security schemes for IoT devices use public key cryptography. If the key is hacked then the security of the entire system will be affected [1].
- ✓ Secure and trustworthy connection of resource constrained devices are difficult, because of the heterogeneity in IoT networks [2].
- ✓ Authentication is very important in the context of IoT. But the authentication scheme must respond to the characteristics of the Internet of Things [6].
- ✓ Major requirements of IoT is the security improvements and privacy [18].
- ✓ The limitation of network resources made difficult to collect data from numerous IoT devices in real time. Thus, it is essential to control the data collection in order to improve the performance of the authentication system. [26]
- ✓ The existing communications in IoT has limited inbuilt single-factor authentication security mechanism which is not sufficient to mitigate the threats and requires augmented authentication scheme. Hence, IoT architecture needs to envisage a two-factor authentication scheme to meet basic security requirements such as confidentiality, integrity and availability of the devices and their communications to envisage smart applications [23]
- ✓ Security and privacy are major areas of concern in IoT-based healthcare applications as most devices and their communications are wireless in nature. Providing robust and secure data communication among healthcare sensors, actuators, patients, and caregivers are crucial [20]
- ✓ IoT devices are constrained in terms of battery life, processing power, and memory and operate in a wireless environment. It creates a number of networking challenges [14]
- ✓ Because of the resource constrained environment, classic security mechanisms cannot be applied on IoT devices because, they consume more energy [28]
- ✓ Security is one of the major issues that hinder the adoption of IoT Cloud providers and making of IoT devices trusted with the Cloud system is a big concern. [11]

VI. CONCLUSIONS

This paper presents the overview of authentication in IoT environment and its research challenges. A wide variety of literatures were presented. Each study was reviewed to understand the problems and issues in the security of IoT environments. According to the above presented literature study, it is identified that security in IoT is a major issue when it becomes a reality. So, IoT security system must be designed for enhancing the authentication and authorization to deliver better security service. If the authentication mechanism is stronger and well established, then it will prevent many security threats like eavesdropping, impersonation and replay attack, etc. Moreover, the authentication mechanisms should be fast and light weighted without compromising security.

REFERENCES

[1] Anjali Yeole, Sadaf Ahmedi, KirtiMadhwani, SnehaSahijwani, Pooja Talreja, “A Robust Scheme for Secure Communication in Internet of Things”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 11, November 2015, pp. 10401 – 10406

[2] Ajit A. Chavan and Mininath K. Nighot, “Secure and Cost-effective Application Layer Protocol with Authentication Interoperability for IOT”, Science Direct, Elsevier, Procedia Computer Science, Vol, 78, 2016, pp. 646 – 651.

[3] ByungMun Lee, “Authorization Protocol using a NFC P2P mode between IoT device and Mobile phone”, Advanced Science and Technology Letters, Vol.94, 2015, pp.85-88, http://dx.doi.org/ 10.14257/astl. 15.94.18

[4] Debiao He and SheraliZeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography”, IEEE Internet of Things Journal, Vol. 2, No. 1, February 2015, pp. 72 -83.

[5] C Gehrmann, Marco Tiloca, and RikardHoglund, “SMACK: Short Message Authentication ChecK Against Battery Exhaustion in the Internet of Things”, 12th International Conference on Sensing, Communication, and Networking (SECON), IEEE, 2015, pp. 274 – 282.

[6] Hamza Khemissa and DjamelTandjaoui, “A Lightweight Authentication Scheme for E-health applications in the context of Internet of Things”, IEEE Digital Library, 2015, pp. 90 -95, DOI: 10.1109/NGMAST.2015.31

[7] Hamza Khemissa, DjamelTandjaoui, “A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things”, Wireless Telecommunications Symposium (WTS), IEEE, 2016, DOI: 978-1-5090-0314-3, pp. 1-6.

[8] Jia-Li Houand Kuo-Hui Yeh, “Novel Authentication Schemes for IoT Based Healthcare Systems”, International Journal of Distributed Sensor Networks, Volume 2015, 2015, pp. 1-9.

[9] Jose L. Hern´andez-Ramos, Marcin P. Pawlowskix, Antonio J. Jara, Antonio F. Skarmeta and Latif Ladid, “Towards a Lightweight Authentication and Authorization Framework for Smart Objects”, IEEE Journal on Selected Areas in Communications, Vol. 33, Issue. 4, 2015, DOI: 10.1109/JSAC. 15.2393436, pp. 690 – 702

[10] Kalra S and S. Sood, “Secure authentication scheme for IoT and Cloud Servers”, Pervasive and Mobile Computing, Vol. 24, Issue C, 2015, pp. 210-223.

[11] Luciano Barreto, Antonio Celesti, Massimo Villari, Maria Fazio and Antonio Puliafito, “An Authentication Model for IoT Clouds”, IEEE / ACM International Conference on Advances in Social Networks Analysis and Mining, 2015, pp. 1032 – 1035.

[12] Manoj Kumar S, "An Analysis of Authentication Schemes for Internet of Things", International Journal of Engineering Sciences & Research Technology, Vol. 4, Issue 6, 2015, pp. 978 – 984.

[13] Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Zhiyuan Tan and Ren Ping Liu, "A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment", IEEE Computer Society, pp. 205 – 211

[14] Oladayo Bello and SheraliZeadally, "Intelligent Device-to-Device Communication in the Internet of Things", IEEE Systems Journal, 2014, pp.1-11

[15] Pablo Punal Pereira, Jens Eliasson, Jerker Delsing, "An Authentication and Access Control Framework for CoAP-based Internet of Things", Proc. of the 40th Annual Conference of the IEEE Industrial Electronics Society, 2014, pp. 5293 – 5299.

[16] Pádraig Flood and Michael Schukat, "Peer to Peer Authentication for Small Embedded Systems - A zero-knowledge-based approach to security for the Internet of Things", Proc. of the 10th IEEE International Conference on Digital Technologies (DT), 2014, DOI: 978-1-4799-3303-7, pp. 68 – 72

[17] PawaniPorambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov and Mika Ylianttila,"Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications", Proc. of the IEEE Wireless Communications and Networking Conference (WCNC), 2014, ISSN : 1525-3511, pp.2728 – 2733.

[18] K. A. RafidhaRehiman and S. Veni, "A Secure Authentication Infrastructure for IoT Enabled Smart Mobile Devices – An Initial Prototype", Indian Journal of Science and Technology, Vol 9. No. 9, March 2016, DOI: 10.17485/ijst/ 16/v9i9/86791, pp. 1-6.

[19] Rene Hummen, Hossein Shafagh, Shahid Raza, Thiemo Voigtz, Klaus Wehrle, "Delegation-based Authentication and Authorization for the IP-based Internet of Things", Proc. of the Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), 2014, ISSN : 2155-5486, pp. 284 – 292.

[20] SanazRahimiMoosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, JouniIsoaho, HannuTenhunen, "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways", Science Direct, Elsevier, Vol. 52, 2015, pp. 452 – 459.

[21] SanazRahimiMoosavi, Ethiopia Nigussie, Seppo Virtanen, JouniIsoaho, "An Elliptic Curve-based Mutual Authentication Scheme for RFID Implant Systems", Procedia Computer Science (Elsevier), Vol. 32, 2014, pp. 198 – 206.

[22] Shantha Mary Joshitta R, L. Aroickiam, "Security in IoT Environment: A Survey", International Journal of Information Technology and Mechanical Engineering (IJITME), ISSN: 2349-2865, Volume: 2, Issue: 7, July 2016, pp. 1-8

[23] Shivraj V L, Rajan M A, Meena Singh, Balamuralidhar P, "One Time Password Authentication Scheme based on Elliptic Curves for Internet of Things (IoT)", IEEE, 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), 2015, pp. 1-6

[24] G. Usha Devi, E. Vishnu Balan, M. K. Priyan and C. Gokulnath, "Mutual Authentication Scheme for IoT Application", Indian Journal of Science and Technology, Vol 8. No. 26, 2015, pp. 2-5.

[25] VitalyPetrov, SviatoslavEdelev, Maria Komar, YevgeniKoucheryavy, "Towards the Era of Wireless Keys:How the IoT Can Change Authentication Paradigm", 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 51-56.

[26] Yuichi Kawamoto, Hiroki Nishiyama, NeiKato, Yoshitaka Shimizu, Atsushi Takahara, and Tingting Jiang, "Effectively Collecting Data for the Location-Based Authentication in Internet of Things", IEEE Systems Journal, Vol. PP , No. 99, 2015, pp.1 -9.

[27] C. Schmitt, B. Stiller and M. Noack, "Two-way Authentication for IoT", IETF, Ser., ACE Working Group, June 2015, pp. 1-19.

[28] Mohammad SabzinejadFarash, MuhamedTurkanović, SaruKumari and Marko Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment", Ad Hoc Networks, 2015, doi: http://dx.doi.org/ 10.1016/j.adhoc. 15.05.014, pp. 1 - 40.

[29] Eleonora Borgia, "The Internet of Things vision: Key features, applications and open issues", Computer Communications Vol. 54, 2014, pp.1-31.

[30] Andrew Whitmore, Anurag Agarwal, and Li Da Xu. "The Internet of Things-A survey of topics and trends." Information Systems Frontiers Vol. 17, Issue. 2, 2015, pp. 261-274.

