iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

Securing Constrained IOTs Data

Sonali S. Dambaye[1], Vaishali L. Kolhe[2]
[1,2]*Dept.of Computer Engineering, D. Y. Patil College of Engineering, Akurdi, Savitribai Phule Pune University*

Abstract: ***Internet of Things is the integration of physical world with virtual world of internet, comprising of number of smart devices that are interconnected and are able to communicate with each other with the help of an IoT protocol. However, managing large number of devices securely in IoT is an emerging challenge, specially the sensor devices. In future IoT, the integration of WSN with computer network is obvious, which necessitate the solution to the secure management of those sensor devices. Most important is the security of sensor data, which the sensor devices transfer to the requested client via server. To tackle the data security issue of such IoT applications, the token generation process can be used in combination with the lightweight cryptographic techniques. This provides limited access to the client to obtain a resource with the permission of a resource owner. By using token generation process the proposed system works more efficiently considering data security features.***

Keywords: ***IoT, CoAP, RESTful, UDP, Constrained devices***

I. INTRODUCTION

The term “IoT” is recently become popular [1] and is well known as a new communication media. The concept of IoT [1] varies from application to applications. In general IoT consists of the uniquely identifiable physical devices, which are connected via internet. The devices in IoT can either communicate with each other or can send data to the remote server [2] for further processing. A traditional WSN is a wireless sensor network of the sensor devices that can collect sensor data from the environment and send it to the base station for further processing over the data.

WSN is now seen as a key component of the IoT environment yielding a distributed network of intelligent sensor devices. Recent WSN application include sensor nodes deployed in environments near to humans and focused on facilitating applications such as building automation, industrial automation etc. These sensor devices are resource limited in many aspects such as with limited storage and processing capabilities, limited energy in the form of battery which is energy prone, and are connected through low power lossy links, vulnerable radio conditions, no direct human interaction [3] etc.

Interconnecting these sensor devices with low-cost wireless communication technologies, a new ecosystem with a large number of smart applications has been formed. With the technological development in IoT, number of standardization working group, such as IP smart object alliance (IPSO) [8] and Internet Engineering Task Force (IETF) [7], are formed based on the selection of technology and commercial markets. The IoT applications can be one of two types: non-Internet protocols (IP)-based and IP-based solutions [5] [7]. IPSO actively promotes IPv6-embedded devices for machine-to-machine (M2M) applications. Whereas IETF focuses on standardizing the communication protocols for resource constrained devices [7][8][9]. The future IoT applications could be IP-based. However, those applications will necessitate the deployment of large number of sensing devices which may arise many problems due to the complex nature of the system [7]. To manage such a large scale sensor networks require the standard IoT resource management solution.

II. BACK GROUND

Recently there is an increase use of wireless sensor devices in IoT applications, e.g. environmental monitoring, home automation etc. however the sensor devices are limited in resources and configuring and deploying them manually is not a good idea. Managing those sensor devices is a challenging issue of IoT. To address this issue many research work has been done. The solutions are basically based on the type of web service used. The web services (WS) technologies can be classified into Big WS and RESTful WS [13]. Both the architectural design styles are similar in principal level but they are differing in technological level. The Big-WS architectural design style has different web service technology stack, that include technologies such as SOAP, WSDL, WS-Addressing, WS-Reliable Messaging, WS Security [11] etc. Big WS, or WS-*, provides interoperability features for both the Remote Procedure Call (RPC) and messaging integration styles. Whereas Representational State Transfer (REST) architectural design style is used to build the large-scale hypermedia applications. This RESTful WS approach supports a simple and flexible communication stack on top of some features to deploy on the constrained devices. Using RESTful approach on devices could not require any special application programming interface providing easy data access of the wireless sensor devices from the server. It

provides the special feature of abstracting all devices as the resources thus allows accessing those resources over the Internet with the help of some standard protocol.

However, the literatures [11] [12] used the WS-* architectural design style, bring extensive overheads for resource constrained devices. And the solutions involving RESTful approach [14] [15] [16] need to use multi-protocol gateway, but translation of protocol includes converting the routing logics of particular protocol and their mechanisms which may in-turn increase the overhead on the constrained devices. The solution [17] also uses RESTful web service architectural design style with lightweight protocol, but it does not require the protocol translations and it thus reduces the overhead on resource constrained devices. The device management functions mapped with the CoAP methods are used to remotely manage the sensor devices. All such functions can share common resources on the same sensor device. In [17] made use of GET, PUT, POST and DELETE methods [10] of the CoAP protocol, thus making this solution a simple, efficient and promising one to drive the IoT development. Many other literatures have focused on introducing the new technology or protocol over the CoAP protocol so that it could provide a multi-protocol gateway that in-turn provides the common interface for all technologies. Various such integration oriented approach found in [18] [19]. Such approaches either tried to build management functionalities on top of CoAP or require supporting multiple protocols simultaneously. Building management functionalities as well as developing facility to support multiple protocols at a time in turn may bring extra complexity to the solution. Though the existing lightweight RESTful approach is simple to implement, it lack in other features such as it does not provide the security and privacy features, the solution cannot be used in the situation where the sensor devices need to manage at real time and where the sensor devices need to monitor dynamically. The different cryptographic techniques to assure security in IoT are discussed in [18] [19] and the detail of token generation process is found in [20]. In the proposed system AES and SHA3 cryptographic techniques are used in incorporation with the token generation process.

III.SYSTEM ARCHITECTURE

The system architecture of the proposed system is as shown in Fig. 1. In general the system consists of the set up of three laptops. Out of which one laptop generate the sensor data randomly and send that data to the IoT remote server, database in the encrypted form.

The sensor data is taken from the sensor devices deployed on one computer system, the sensor data travel to the IoT remote server and MySQL database at which data is stored in encrypted form using AES and then client application is used to access that data. The admin accept the registration request from user and send specific user ID and password to the user. IoT server receives request and generate the public and private keys and send encrypted data to the user.

User application is used to register to IoT server using login credentials provided by the admin; user can send request to access the sensor data to the server.

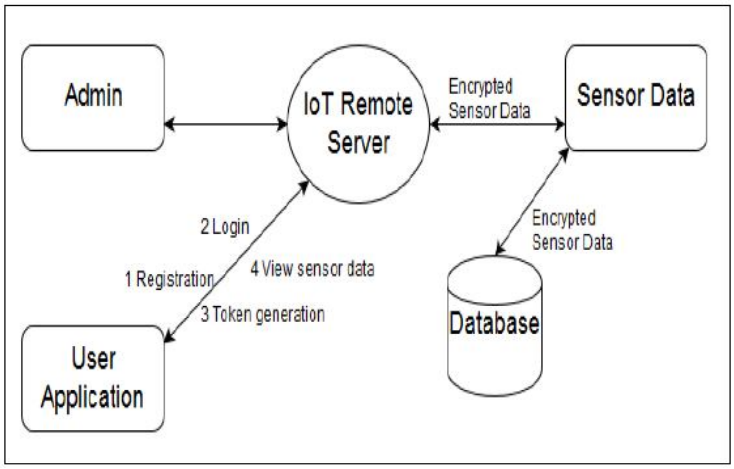


Fig. 1 System Architecture

A. *Algorithms*

Algorithm: Advanced Encryption Standard (AES)

1) *Input:* in[4 * Nb], word w[Nb * (Nr+1)])
2) *Output:* out[4 * Nb]

begin

```
byte state[4,Nb]
state = in
AddRoundKey(state, w[0, Nb-1])
for round = 1 step 1 to Nr1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state, w[round * Nb, (round+1) * Nb-1])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr * Nb, (Nr+1) * Nb-1])
out = state
end
```

IV. SYSTEM ANALYSIS

System will be analyzed for IoT attack. As the sensor nodes are wireless connected with each other via the router, while transmitting sensor data from the sensor node to client a third party attack may happened to steal or alter the data. To prevent this attack the token generation process is used which will allow only the authorized client to access and analyzed the data. After first registration of the client the analysis task will be done at client application on behalf of the client, such as checking the data integrity and the time consumption in invoking the original data.

A. Results

In the proposed system the AES algorithm is used for encryption decryption purpose that can send the message securely in the network. For avoiding and reducing the IoT attack a token generation process of the authorization framework is used.
For that SHA3 algorithm is used which generate the tokens and the tokens are sending to the client via email.
The system is evaluated for the data security by considering the data integrity factor as shown in following graph. The Fig. 3 shows that the data sent by the client is reached 100 percent safe to the client while considering no IoT attacks.

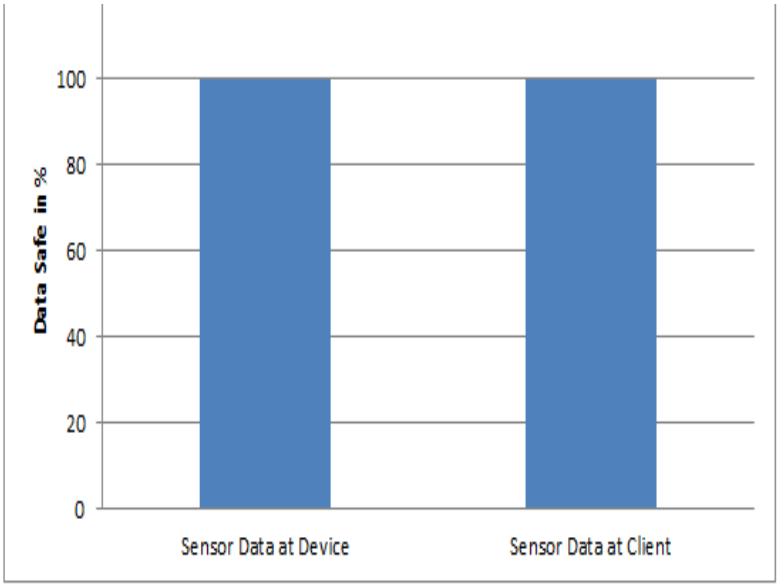


Fig. 3 Data Integrity

The system is also evaluated for the time overhead for running the particular tasks, it is found that the time taken to send the data from sensor device to the client via the intermediate trusted server is not exceed more than 6s as shown in following graph.

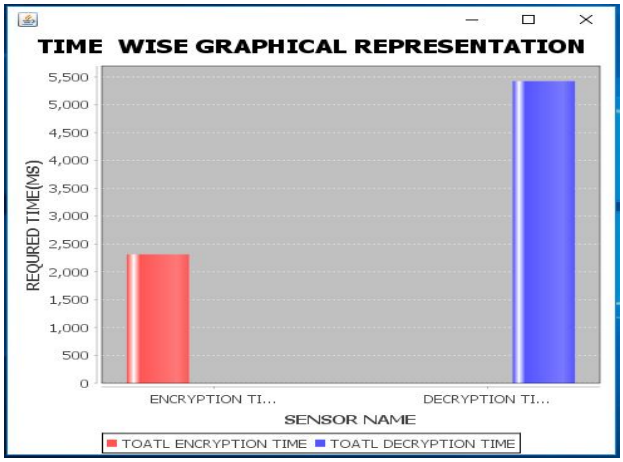


Fig. 4 Time Overhead

From the above results, the proposed approach can be applicable one in IoT scenario considering the use of sensor devices.

V. CONCLUSIONS

In the IoT scenario choosing the best authentication and authorization technique to be implemented in constrained network is challenging. The existing device management system could not provide the security features to ensure the safety of data. Data security for IoT sensor applications is proposed. This paper presents the use of token generation process to securely access the resources of IoTs. The main objective is to provide the data integrity and to ensure that only authorized user have access to data sent by the sensor devices. The experimental evaluation shows that the sensor data reached the destination client safely. It is also found that the time required decrypting that data at client side does not exceed 2 seconds.

VI. FUTURE WORK

The proposed approach can be improved for managing the devices' resources dynamically at real time with the help of growing IoT protocols, and further the approach can made more lightweight using other lightweight cryptographic techniques by avoiding the attacks.

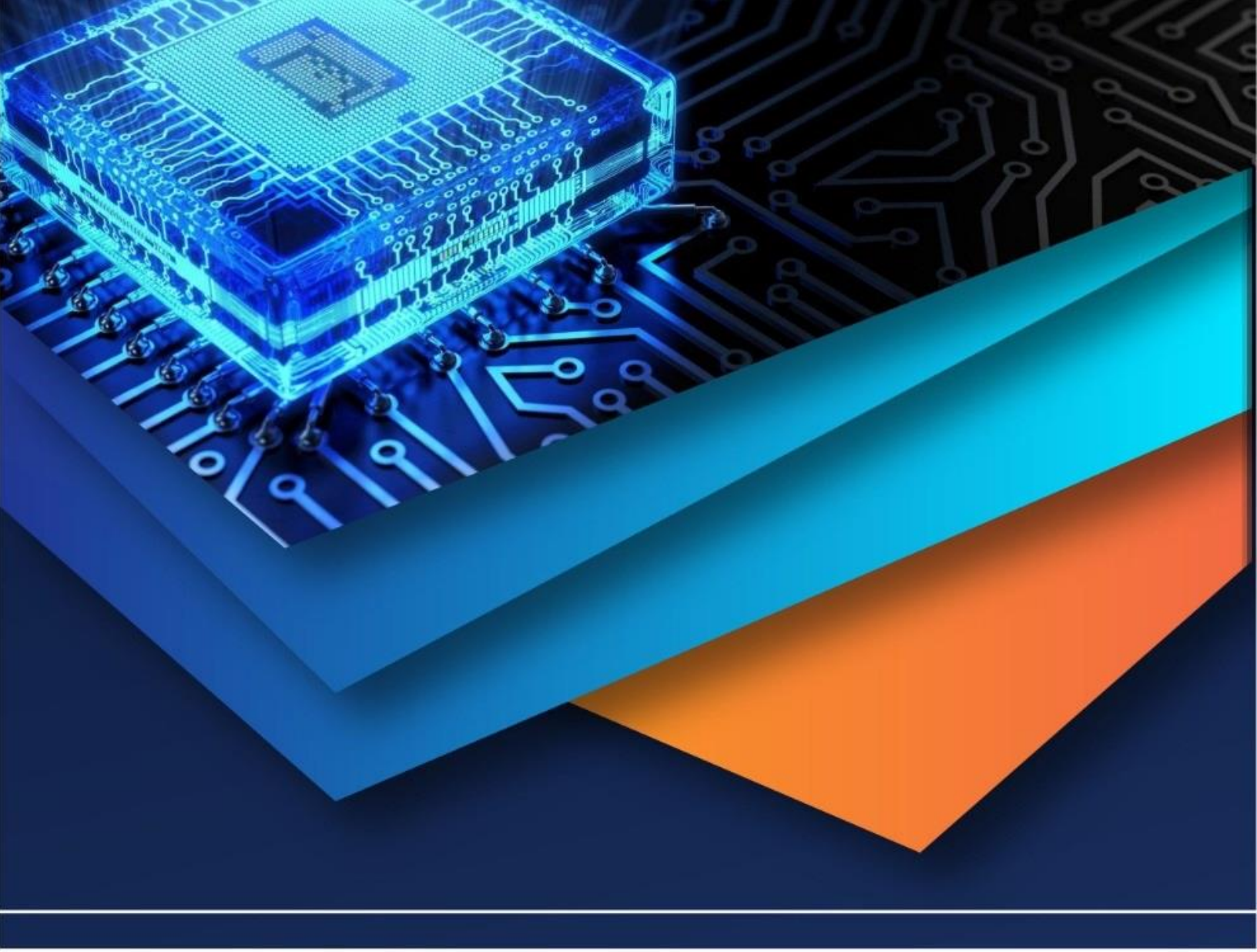
VII. ACKNOWLEDGMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. Authors are thankful to the authorities of Savitribai Phule University of Pune for their constant guidelines and support. Authors also thank the college authorities for providing the required infrastructure and support. Finally, authors would like to extend a gratitude to friends and family members.

REFERENCES

[1] Da Xu, L., He, W. and Li, S., "Internet of things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233-2243, 2014.
[2] Gungor, V.C. and Hancke, G.P., "Industrial wireless sensor networks: Challenges, design principles, and technical approaches." IEEE Transactions on Industrial Electronics, vol 56, no. 10, pp. 4258-4265, 2009.
[3] Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S. and Wehrle, K., "Security challenges in the IP-based Internet of Things," Wireless Personal Communications, vol. 61, no. 3, pp. 527-542, 2011.
[4] Hennebert, C. and Dos Santos, J., "Security protocols and privacy issues into 6LoWPAN stack: a synthesis," IEEE Internet of Things Journal, vol. 1, no. 5, pp. 384-398, 2014.
[5] Mulligan, G., "The 6LoWPAN architecture." Proceedings of the 4th workshop on Embedded networked sensors. ACM, pp. 78-82, 2007.
[6] Rachidi, H. and Karmouch, A., "A framework for self-configuring devices using TR-069," in Proc. Int. Conf. Multimedia Comput. Syst. (ICMCS), pp. 1–6, Apr. 2011.
[7] Shelby, Z., Hartke, K. and Bormann, C., "The constrained application protocol (CoAP)," Tech. Rep., No. RFC 7252. 2014.M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.
[8] T. Cucinotta, A. Mancina, G. F. Anastasi, G. Lipari, L. Mangeruca, R. Checcozzo, and F. Rusina, "A realtime service-oriented architecture for industrial automation," IEEE Transactions on Industrial Informatics, vol. 5, no. 3, pp. 267-277, 2009.
[9] R. Kyusakov, J. Eliasson, J. Delsing, J. van Deventer, and J. Gustafsson, "Integration of wireless sensor and actuator nodes with it infrastructure using service-oriented architecture," IEEE Transactions on industrial informatics, vol. 9, no. 1, pp. 43-51, 2013.
[10] C. Pautasso, O. Zimmermann. and F. Leymann, "Restful web services vs. big'web services: making the right architectural decision." Proceedings of the 17th international conference on World Wide Web. ACM, pp. 805-814, 2008.

[11] Z. Sheng, C. Zhu, and V. Leung, "Surfing the Internet-of-Things: lightweight access and control of wireless sensor networks using industrial low power protocols," EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, vol. 14, no. 1, p. e2, 2014.
[12] Guinard, D. and Trifa, V., "Towards the Web of Things: Web mashups for embedded devices," in Proc. Int. World Wide Web Conf. (WWW), p. 15, Apr. 2009.
[13] Guinard, D., Trifa, V. and Wilde, E.,"A resource oriented architecture for the Web of Things," in Proc. Internet of Things (IoT), pp. 18, IEEE, Dec. 2010.
[14] Z. Sheng, H. Wang, C. Yin, X. Hu, S. Yang, and V. C. Leung, "Lightweight management of resource constrained sensor devices in Internet of Things," IEEE Internet of Things journal, vol. 2, no. 5, pp. 402-411, 2015.
[15] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of resource constrained devices in the Internet of things." IEEE Communications Magazine, vol. 50, no. 12, pp. 144-149, 2012.
[16] M. Jung, J.Weidinger,W. Kastner, and A. Olivieri, "Building automation and smart cities: An integration approach based on a serviceoriented architecture," Advanced Information Networking and Applications Workshops (WAINA), pp. 1361-1367, IEEE, 2013.
[17] N. Gligoric, S. Krco, D. Drajic, S. Jokic, and B. Jakovljevic, "M2M device management in LTE networks," in Telecommunications Forum (TELFOR), 2011 19th, pp. 414-417, IEEE, 2011.
[18] I. Luhach and A. Kr. Luhach, "Analysis of Lightweight Cryptographic Solutions for Internet of Things." Indian Journal of Science and Technology, vol. 9, no. 28, 2016.
[19] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power IoT devices." In Advances in Computing, Communications and Informatics (ICACCI), pp. 1725- 1729. IEEE, 2016.
[20] E. Y. Chen, P. Yutong, S. Chen, Y. Tian, R. Kotcher and P. Tague. "Oauth demystified for mobile application developers." In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 892-903. ACM, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY