Research Journal of Engineering Technology and Medical Sciences (ISSN: 2582-6212), Volume 05, Issue 03, September-2022
Available at www.rjetm.in/

Access and Authentication Frameworks for IoT Networks

Dewesh Tiwari, Ajit Kumar Tiwari
Department of Computer Science and Engineering, RKDF University, Bhopal, India

* Corresponding Author: Dewesh Tiwari

Abstract

The phrase "Internet of Things" (IOT), which was coined by Kevin Ashton [1], portrays a future world in which both living and non-living physical elements would be connected to the internet and be able to communicate with one another and with web service applications. In the web, the hosts are represented by the entities that are attached to the sensors and microcontrollers. enable real-world residents to become top-tier Internet citizens by allowing them to grow out of their limitations.A framework is developed by the Internet of Things that encourages acknowledging future developments and visions. As an illustration, think of "smart urban areas," which take into account a more effective management of the city, such as management of road lights, element illumination taking into account current movement stream, identifying and obsessing. (ii) Smart homes, in which most features, including heating and cooling, doors, windows, stairways, and equipment, may be operated remotely.Implanted frameworks that are constrained in terms of power, compute, and memory are frequently physical things that are coupled to restricted devices. These devices that are required to be used by law are online and utilize the unstable services of the Internet. Some types of security features are required because of this. The most modern security alternatives, such TLS [3] and IPsec [4], are IP-based, but because communication costs are so high and expensive handshaking procedures are necessary, they are not designed for restricted devices. As a result, it is impossible to directly and successfully apply current IP-based security standards.Implanted frameworks that are constrained in terms of power, compute, and memory are frequently physical things that are coupled to restricted devices. These devices that are required to be used by law are online and utilize the unstable services of the Internet. Some types of security features are required because of this. The most modern security alternatives, such TLS [3] and IPsec [4], are IP-based, but because communication costs are so high and expensive handshaking procedures are necessary, they are not designed for restricted devices. As a result, it is impossible to directly and successfully apply current IP-based security standards. In this paper we present a delegation-based framework to enable security services for IOT Networks.

Keywords: -Authentication, IOT Networks, Handshaking,Cryptography

I.INTRODUCTION

The internet of things, or IoT, is a network of interconnected computers, mechanical and digital equipment, objects, animals, or people who may exchange data across a network without needing to interact with other people or computers. Things include people with implanted heart monitors, farm animals with biochip transponders, cars with built-in type pressure monitors, and other examples. The term "thing" refers to any natural or artificial object that can be given an

Internet Protocol (IP) address and has the ability to transfer data over a network. IoT is being used by businesses across a variety of industries to improve operations, better understand their customers to deliver better customer service, speed up decision-making, and increase the value of the firm.The need for IOT is growing daily as a result of the widespread usage of the internet and automated devices. Although other sensor technologies, wireless technologies, and QR codes may also be used, RFID was once believed to be the only means of communication. Today's IP-based protocols and technologies incorporate IPV6's advantages. In addition to being viewed by the owner, the service-providing business is now linked to adjacent websites and databases. In order to provide ambient intelligence, many factors interact.

Therefore, in an IOT network, data security is of primary concern, necessitating adequate authentication and access control, which is the major goal of this paper. The rest of the paper is organized as follows. Section II presents Literature Review about the topic. Section III tells us about problem formulation. Section IV gives us simulation resultsand finally Section V gives concluding remarks which are then followed by the bibliography.

II. LITERATURE REVIEW

- The Datagram Transport Layer Security (DTLS) protocol is discussed in this document's version 1.2 by authors**N. Modadugu and R. Rescorla.** The DTLS protocol provides communication privacy for datagram communications. The protocol allows client/server applications to communicate in a method that aims to avoid message forging, eavesdropping, and tampering. The DTLS protocol, which is based on the Transport Layer Security (TLS) protocol, provides similar security guarantees. The datagram semantics of the underlying transport are preserved by the DTLS protocol. DTLS 1.0 is made TLS 1.2 compatible by this document.
- IPv6 over Low-Power Wireless Personal Area Networks, by **N. Kushalnagar, G. Montenegro, and C. Schumacher**, discusses This study examines prospective use cases and application scenarios for low-power wireless personal area networks (LoWPANs). For LoWPAN applications, this paper specifies design space dimensions. With the features of each dimension, a list of use cases and market sectors is presented that may benefit and inspire the work currently being done in the 6LoWPAN Working Group. This article does not aim to provide a comprehensive list of real-world application scenarios. This document is not a standard for the Internet Standards Track;It is distributed for educational purposes.In the first section, we go over the characteristics of the restricted devices and the network in which they function. The relevant cryptography requirements are then briefly summarised. The Datagram Transport Layer Security (DTLS) protocol is the topic of our final discussion.
- Cross-level sensor network modelling using cooja is covered by **F. Osterlind, A. Dunkels, J. riksson, N. Finne, and T. Voigt** in Local Simulators for Wireless Sensor Networks. Current simulators, however, can only model one level of a system at a time. Since developers cannot utilise the same simulator for both high-level algorithm development and low-level development, such as device-driver implementations, this makes system development and evolution challenging.We suggest cross-level simulation, a brand-new kind of wireless sensor network simulation that permits comprehensive concurrent simulation at several levels. We offer COOJA, a simulator for the Contiki sensor node operating system, as an implementation of such a simulator. Simultaneous simulation at the network, operating system, and machine code instruction set levels is possible using COOJA. We demonstrate the viability of the cross-level simulation approach with COOJA.

III. PROBLEM FORMULATION

The DTLS handshaking protocol is generally used to establish authentication. In the event that mutual certificate sharing is used for authentication, DTLS activates and overrides memory portion and communication. The extensive handshaking messages advance the conversation. These large messages must be processed, and sufficient buffers are needed. Once more, more effort is put into verifying and approving the authenticity of the certificates. The previously stated proposals require a thorough examination of the overheads, which is something we deal with in our work. This enables us to be able to come up with solutions to lessen these overheads.

In order to provide secure M2M communication between enterprises and the internet, secure IoT must achieve the security goals of confidentiality, integrity, and authenticity. Current methodologies use pre-shared keys on both ends and certificate-based schemes that are impossible for entities with limited resources. We contend that PKI that is integrated with IP-based authentication can be used.In this case, we rely on DTLS as a method to achieve secure communication. We need to implement a secure IoT network in order to measure resource requirements and overflow. This should be as lightweight as is reasonable given the circumstances in order to fit the available resources of constrained entities. While developing such an execution, overheads that already exist can be recognized and solutions for lessening them can be created. The expensive PKC operations are carried out using a delegation method. This would allow for the use of PKC advantages, such as key agreement without prior learning, with a wide range of devices.

The server can be authenticated more seriously using a certificate, as is typically done for web services. In any case, the overwhelming PKC operations might be appointed to a more extensive off-road device that meets the required level of confidence.

At the same time, we implemented a capability-based security strategy [24] to manage access management in the Internet of Things. An access token used for authentication and access management is called a capability. It refers to a value that specifically identifies a subject with the collection of access privileges granted to that subject. Certain advantages of capability-based permission include its assistance with delegation, support for granularity in access control, and assistance with revoking authorization. This method is crucial for a fine-grain based access control environment because of these advantages.

3.1 PROPOSED FRAMEWORK

As seen in Figure 3.1, the DTLS handshaking is delegated to the powerful server known as the Authentication, Authorization and Key Distribution Server (AAKDS).The model consists of 4 events: Entity Registration, Remote server Registration,Authentication of entities,communication.

3.1.1 Registration of Entities

A predefined key and predefined protocol suit are provided with an entity. Prior to the actual communication taking place, the entity must be registered in the home network. The steps taken for registration are depicted in Figure 3.3.

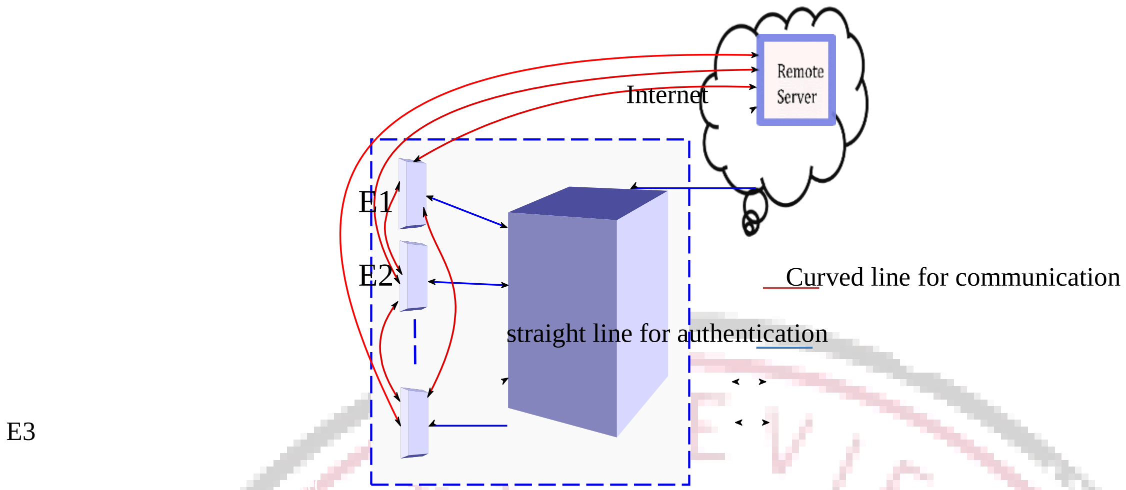


Figure 3.1: Proposed Framework.

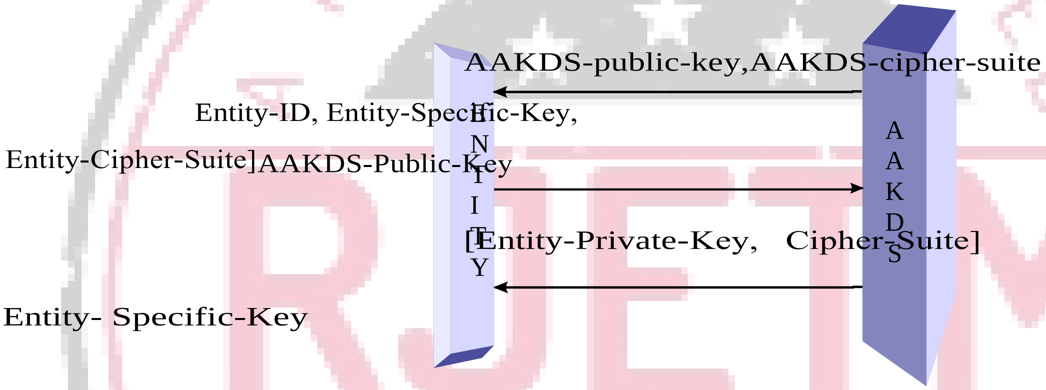


Figure3.2:EntityRegistrationProcess

Procedure 1: ENTITY

---

1. The AAKDS publishes its public key.
2. TheEntitysendsitscredentials(Entity-specific-keyanditsEntity-specific-ID)andits cipher suit to AAKDS, encrypted with the AAKDS-public-key.
3. AAKDS stores the credentials of the Entity in an encrypted form and sends aPrivate-key to the entity encrypted with the Entity-specific-key.

3.1.2 Registration of RemoteServer

TheRemoteServerisregisteredusingtheDTLShandshakingasshowninFigure3.3

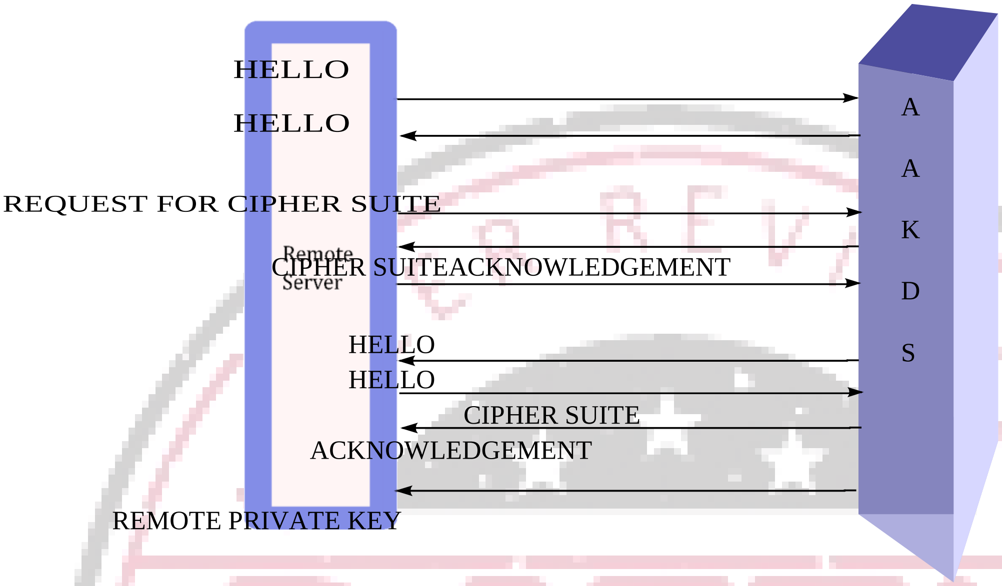
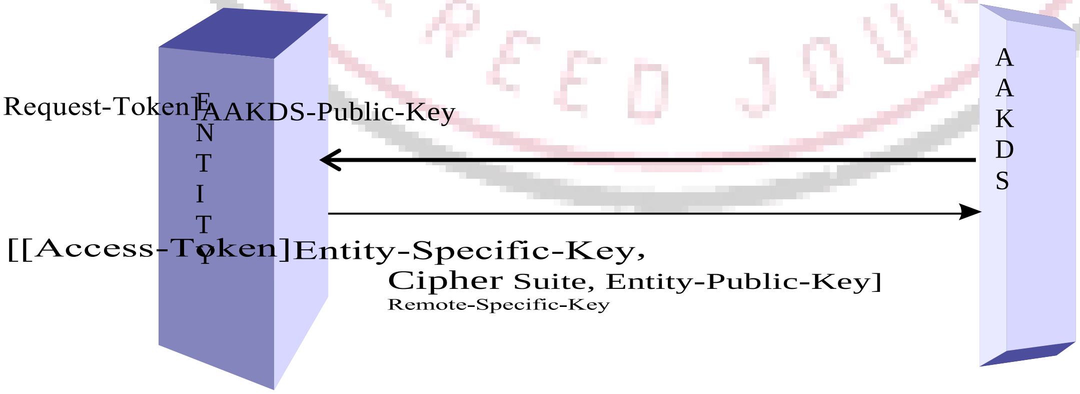


Figure3.3 :Remote ServerRegistrationProcess

Procedure 2 :- REMOTE SERVER

1. The Remote Server sends a HELLO message to theAAKDS
2. The AAKDS sends HELLO VERIFIED message
3. TheRemoteServerrequestsforthecipher-suiteandkeyoftheAAKDS.
4. AAKDSsend’s it’scipher-suiteandkeyandwaitsfortheacknowledgment.
5. AAKDSrequeststheRemoteServerforit’scipher-suiteandkeys.
6. The Remote Server send’s it’s cipher-suite and key and waits for acknowledgment

3.1.3 Authentication and Authorization of Entities



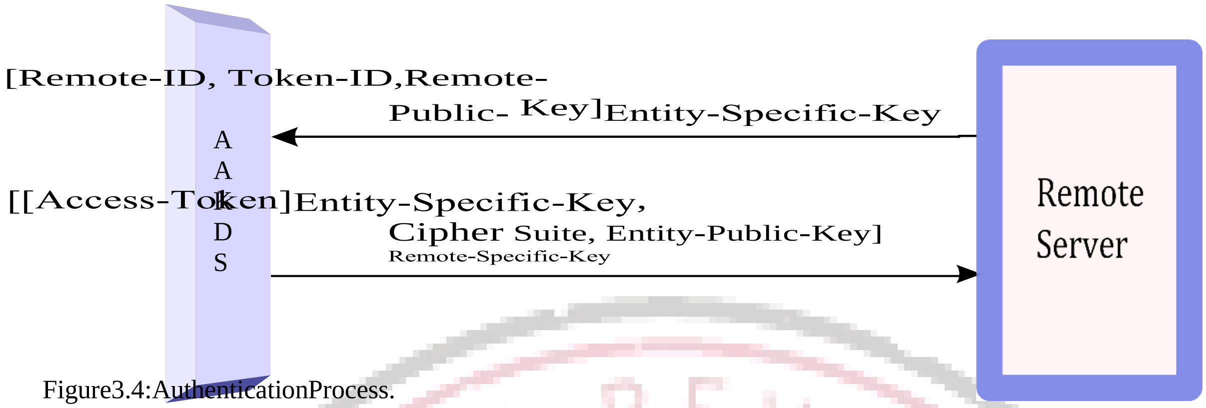
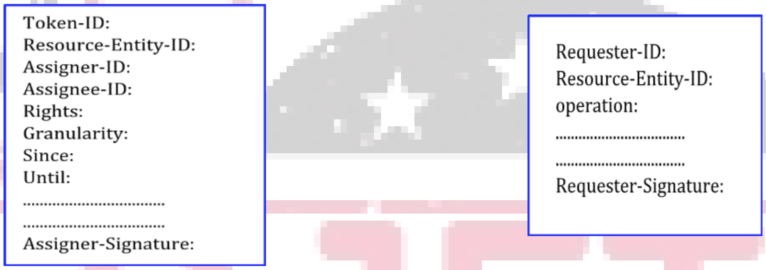


Figure3.4:AuthenticationProcess.

Theauthenticationandauthorizationofentitiesusethefollowingstepsshownin Figure 3.4



(a) Action Token (b) Request Token

Figure3.5:Tokens usedforAuthentication

Procedure 3: Authentication and Authorization

---

1. TheRemoteServersendsarequesttoken,asshowninFigure3.5,totheAAKDSto access an entity.
2. AAKDScheckstheauthenticityoftheRemoteServerandfinalizeitsAuthorization
3. AAKDSthenissuesanaccesstoken,asshowninFigure3.5,totheRemoteServerencryptedwiththeEntity-specific-key.Theaccesstokenrepresentsthecapability token.ItalsosendstheEntity-public-key.
4. The Remote-ID and the Token-ID is sent to the entity encrypted withEntity-specific-key.
5. TheEntitystorestheRemote-IDandtheToken-IDforfutureverification.

3.1.4 Communication

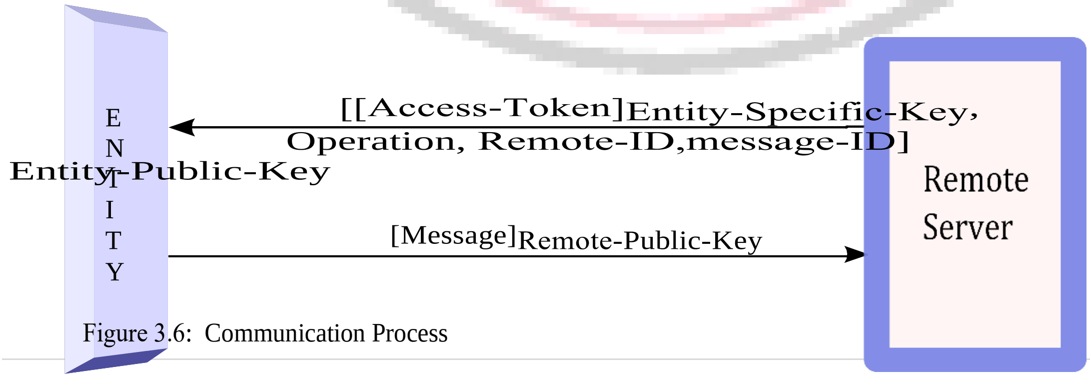


Figure 3.6: Communication Process

ThecommunicationprocessisshowninFigure3.6.

Procedure 4: Communication

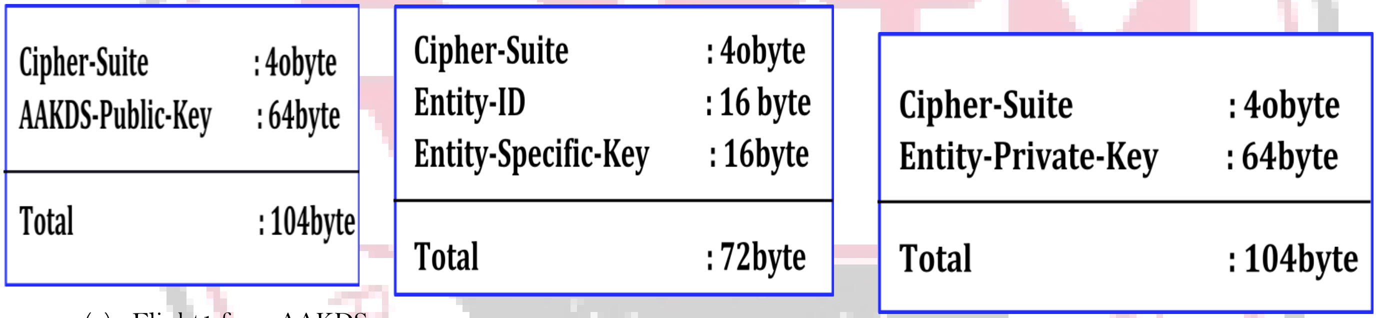
---

[1] The Remote Server sends a message containing access token, Remote-ID,operationto perform, and a message-ID encrypted with the Entity-public-key.
[2] Theentitydecryptsitandverifiestheaccesstoken.
[3] Theentitysendstherequiredresponseafterverifyingtheauthorization.
[4] IftheRemoteServerisnotauthenticated,thenthe operationrequestisrejected.
Twoentitiesalsocommunicateusingthesameprocedure.

IV. RESULTS OBTAINED

4.1 ENTITY REGISTRATION EVENT

Following Results are obtained. Thespecificationsused for entity registration in our test bed are shown in Figure 4.1.



Cipher-Suite	: 4obyte
AAKDS-Public-Key	: 64byte
Total	: 104byte

Cipher-Suite	: 4obyte
Entity-ID	: 16 byte
Entity-Specific-Key	: 16byte
Total	: 72byte

Cipher-Suite	: 4obyte
Entity-Private-Key	: 64byte
Total	: 104byte

(a) Flight1 from AAKDS
to Entity (b) Flight2 from Entity(c) Flight3 from AAKDS to Entity
to AAKDS

Figure4.1:FlightsusedforEntityRegistrationEvent.

The comparison of time unit taken for entity registration using different Cryptographic algorithm sets are shown in the Table 4.1

Table4.1:ComparisonofdifferentalgorithmsetsforEntityRegistration

ALGORITHM/TIME	**TIME-UNIT TAKEN FOR CONNECTION**	**TIME UNIT TAKEN FOR ROUND ABOUT TRANSMISSION**	**TOTAL TIME UNIT TAKEN**
RSA & AES	00:02.488	12:48.220	12:50.708
RSA & PRESENT	00:02.488	12:10.977	12:13.465
ECC & AES	00:02.488	10:43.285	10:45.773
ECC & PRESENT	00:02.488	10:15.472	10:17.960

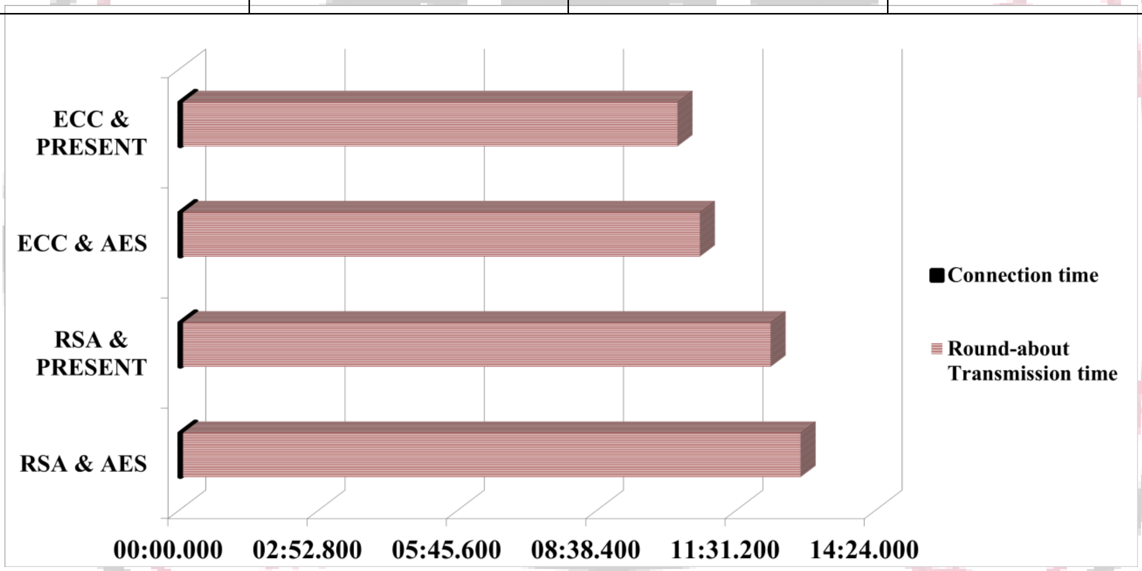
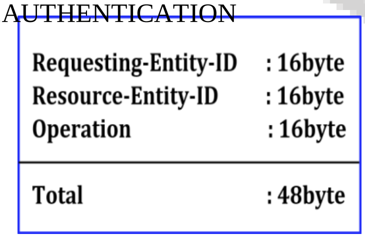
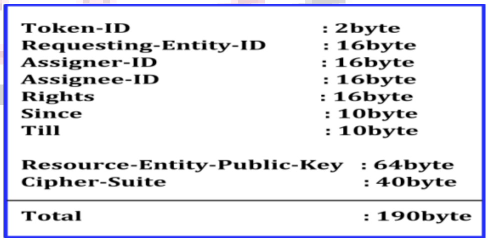


Figure 4.2: EntityRegistration Plot

4.2AUTHENTICATION



Requesting-Entity-ID	: 16byte
Resource-Entity-ID	: 16byte
Operation	: 16byte
Total	: 48byte



Token-ID	: 2byte
Requesting-Entity-ID	: 16byte
Assigner-ID	: 16byte
Assignee-ID	: 16byte
Rights	: 16byte
Since	: 10byte
Till	: 10byte
Resource-Entity-Public-Key	: 64byte
Cipher-Suite	: 40byte
Total	: 190byte

(a) Flight1: request from Entity toAAKDS
(b) Flight2: Respond from AAKDS to Entity

Token-ID	**: 2 byte**
Requesting-Entity-ID	**: 16byte**
Requester-Entity-Public-Key	**: 64byte**
Cipher-Suite	**: 40byte**
Total	**: 122byte**

(c) Flight3 from AAKDS to resourceEntity

Figure4.3:FlightsusedforAuthenticationEvent.

Table4.2:ComparisonofdifferentalgorithmsetsforAuthenticationProcess

ALGORITHM/TIME	**TIME-UNIT TAKEN FOR CONNECTION**	**TIME UNIT TAKEN FOR ROUND ABOUT TRANSMISSION**	**TOTAL TIME UNIT TAKEN**
RSA & AES	00:02.488	11:10.376	11:12.864
RSA & PRESENT	00:02.488	10:34.048	10:36.536
ECC & AES	00:02.488	09:28.316	09:30.804
ECC & PRESENT	00:02.488	09:09.962	09:12.450

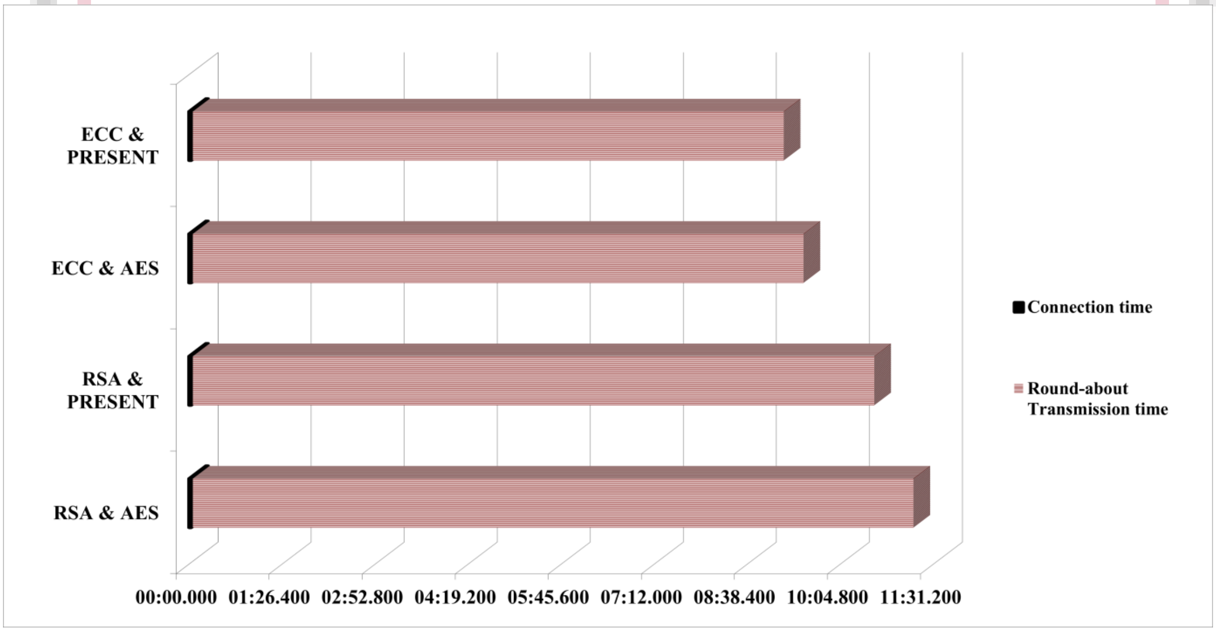


Figure 4.4: Entity Authentication Plot.

4.3 COMMUNICATION

Communication results between the entities event is discussed below

Access-Token	**: 86byte**
Requesting-Entity-ID	**: 16byte**
Operation	**: 16byte**
Nonce	**: 2byte**
Total	**: 120byte**

Requesting-Entity-ID	**: 16byte**
Resource-Entity-ID	**: 16byte**
message	**: 16byte**
Total	**: 48byte**

(a) Flight1: Request from Entity to AAKDS (b) Flight2: Respond from AAKDS to Entity

Figure4.5:Flightssenttoaccessaservice.

Table 4.3 Comparison of different algorithm-sets for Communication Event.

ALGORITHM/TIME	TIME-UNIT TAKEN FOR CONNECTION	TIME UNIT TAKEN FOR ROUND ABOUT TRANSMISSION	TOTAL TIME UNIT TAKEN
RSA & AES	00:02.488	11:48.583	11:51.071
RSA & PRESENT	00:02.488	11:16.604	11:19.092
ECC & AES	00:02.488	09:58.294	10:00.782
ECC & PRESENT	00:02.488	09:34.296	09:36.784

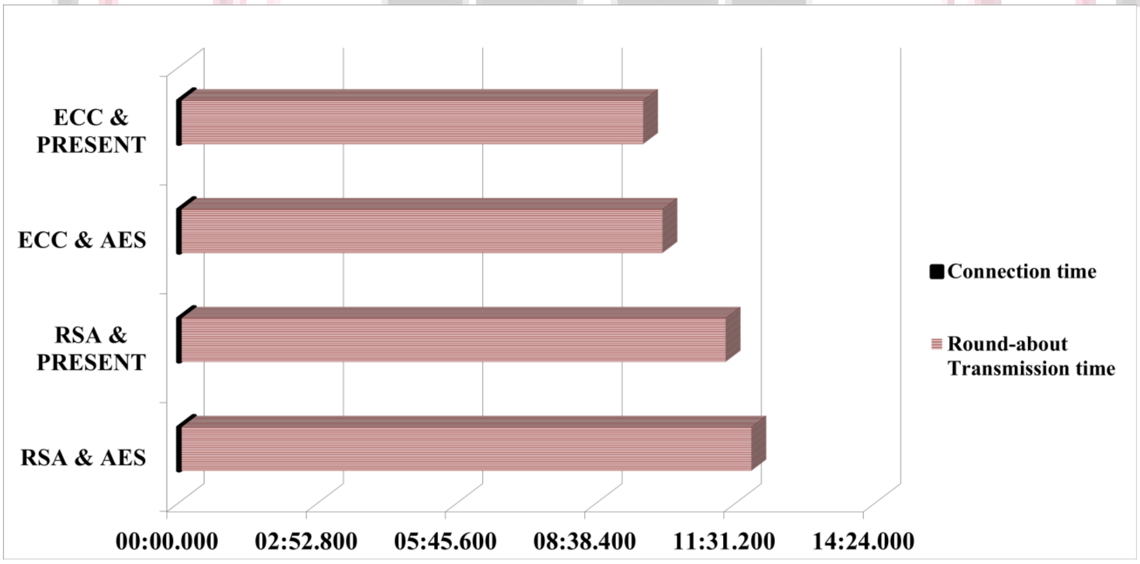


Figure 4.6 Communication Plot.

V. CONCLUSIONS

In conclusion, the work provides a framework and a proposed model that may be used to protect and manage the data in the IOT Network. Here we have presented an authentication and access network which secures IOT network and gives an authentication process to follow so that we can get a secure and efficient network.

REFERENCES

[1] K. Ashton, “That internet of things thing,” *RFiD Journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] Friedman Mattern. Hundert Jahre Zukunft,Visionen zum, Available: http://link.springer.com/Chapter/10.1007%2F978-3-540-71455-2 18.

[3] T. Dierks, E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246, IETF,” August 2008, Available: http://tools.ietf.org/html/rfc5246

[4] S. Frankel, S. Krishnan, “IP Security (IPsec) and Internet Key Exchange

[5] (IKE) Document Roadmap. RFC 6071, IETF,” February 2011, Available: http://tools.ietf.org/html/rfc6071.

[6] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, “Cross-level sensor network simulation with cooja,” in *Local Computer Networks, Proceedings2006 31st IEEEConferenceon*. IEEE, 2006, pp.641–648.

[7] Z. Shelby,et al., “Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks(6LoWPANs). RFC 6775, IETF,”November 2012, Available: http://tools.ietf.org/html/rfc6775

[8] E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl, “Home networking with ieee 802. 15. 4: a developing standard for low-rate wireless personal area networks,” *IEEE Communications magazine*, vol. 40, no. 8, pp. 70–77, 2002.

[9] N. Venkatesh, “Ultra-low power 802.11 n Wi-Fi–wireless connectivity for the internet of things.,” *Low-Power Wireless as White Paper, Last visited on*, vol. 16, p. 2013, 2010.

[10] S. Bluetooth, “The Bluetooth core specification, v4. 0,” *Bluetooth SIG: San Jose, CA, USA*, 2010.

[11] N. Kushalnagar, G. Montenegro, C . Schumacher, “ IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919, IETF,” August 2007, Available:http://tools.ietf.org/html/rfc4919.

[12] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, IETF,” September 2007, Available: http://tools.ietf.org/html/rfc4944.

[13] D. Cooper, S . Santesson, S .Farrell, S. Boyne, R . Housley, W. Polk, Available: Certificate Available“InternetX.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.RFC 5280, IETF ,” May2008,http://tools.ietf.org/html/rfc5280.

[14] T. M. Heer, *Direct end-to-middle authentication in* cooperative*networks*. Universitätsbibliothek,2011

[15] M. Champagne, D.Stebila, “ECMQV ECQV Cipher Suites for Transport Layer Security (TLS). draft-campagna-tls-ecmqv-ecqv-01, IETF,” January 2010, Available: http://tools.ietf.org/html/draft-campagna-tls-ecmqv-ecqv-01.

[16] A. Dunkels, B. Gronvall, and T. Voigt, “Contiki-a light weight andflexible operating system for tiny networked sensors,” in *Local Computer Networks, 2004. 29th Annual IEEE InternationalConferenceon* IEEE, 2004, pp.455–462.

[17] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler, “Spins: Security protocols for sensor networks,” *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.

[18] O. G. Morchon and H. Baldus, “Efficient distributed security for wireless medical sensor networks,” in *Intelligent Sensors, Sensor Networks and InformationProcessing, 2008. ISSNIP 2008.International Conference on*. IEEE, 2008, pp. 249–254.

[19] T. Freeman, A. Malpani, D. Cooper, and R. Housley, “Server-based certificate validation protocol (scvp),” 2007.

[20] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, “Secure communication for smart iot objects: Protocol stacks, use cases and practical examples,” in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*. IEEE, 2012, pp. 1–7.

[21] M.Ceriotti,M.Corrà,L.D’Orazio,R.Doriguzzi,D.Facchin,S.Guna,G.P.Jesi, R. Lo Cigno, L. Mottola, A. L. Murphy *et al.*, “Is there light at the ends of the tunnel? wireless sensor networks for adaptive lighting in road tunnels,” in *Information Processing in Sensor Networks (IPSN), 2011 10th International Conferenceon*. IEEE, 2011, pp. 187–198.

[22] J. Beutel, S. Gruber, A. Hasler, R. Lim, A. Meier, C. Plessl, I. Talzi, L. Thiele, C. Tschudin, M. Woehrle*et al.*, “Permadaq: A scientific instrument for precision sensing and data recovery in environmentalextremes,” in *Proceedingsof the 2009 International Conferenceon Information Processing in Sensor Networks*.IEEE Computer Society, 2009, pp. 265–276.

[23] T. Heer, O. Garcia-Morchon, R.Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, “Security challenges in the ip-based internet of things,” *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[24] S. Gusmeroli, S. Piccione, and D. Rotondi, “A capability-based security approach to manage access control in theinternet of things,” *Mathematical and Computer Modeling*, vol. 58, no. 5, pp. 1189–1205, 2013.

[25] DOtte, “Avr–crypto–lib.–2009,” *Online: http://www.das–labor.org/wiki/AVR–Crypto–Lib/en*, 2009.

[26] R. L. Rivest,A. Shamir,and L. Adleman,“A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126,1978.

[27] P. Chown, “Advanced encryption standard ciphersuites for transport layer security (tls),” 2002.