iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4777

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 6 Issue IV, April 2018- Available at www.ijraset.com

Design and Development of Security Mechanism for IoT Devices

Priya[1], Subhangi Bhadouria[2], Vidya Rajole[3], Pratibha Babar[4]
[1, 2, 3, 4]*Information Technology Department Bharati Vidyapeeth's College of Engineering for Women*

Abstract: ***The growing number of applications based on Internet of Things (IOT) technologies is pushing towards standardized protocol stacks for machine-to-machine (M2M) communication and the adoption of standard-based security solutions, such as the Datagram Transport Layer Security (DTLS). Despite the huge diffusion of DTLS, there is a lack of optimized implementations tailored to resource constrained devices. High energy consumption and long delays of current implementation slim it their effective usage in real-life deployments. (CoAP) .The proposed system aims at the implementation of security for authentication and communication of the constrained as well as non-constrained devices in a network. The communication between the devices is established through a mobile application. Depending on various factors like mac address, Bot ID, SSID etc. the developed application using hybernet framework detects and blocks the access to the attacker.***
Keywords: IOT, CoAP , DTLS

I. INTRODUCTION

The IoT is a technological revolution that expands the already common concepts of 'anytime' and 'anyplace' to the connectivity for "anything". It is the network of physical objects that contain embedded technology to communicate with the external environment. It encompasses hardware (the 'things'), embedded software, connectivity services, and information services associated with the things. It includes low power, low memory footprints (RAM/ROM), low processing power devices. They should have provision of IPv6 with 6LoWPAN Adaptation Layer. The transition from a closed network to the public Internet is growing rapidly and the raising alarms about security. As we are getting dependent on the independent, interconnected and smart devices day by day, how do we protect potentially a huge number of them from attacks, intrusions and interference that could compromise the personal privacy or may threaten the public safety? A large number of security issues with the IoT devices are present till date like Ubiquitous data collection, potential for unexpected uses of consumer data, increased automation and digitization that can pose safety risks, potential of privacy breaches, large amount of data will be generated, both for big data and personal data. WAN links are optimized for human interface applications; IoT is expected to automatically transmit the data. The proliferation of the IoT offers opportunities, but may also bear risks. A neglected aspect of the IoT is the possible increase in power consumption. IoT devices are usually expected to be reachable by other devices at all times. It means the devices consume electrical energy even when the device is not in use for its primary function. Our proposed system has a network of a certain number of nodes (IoT devices) communicating with each other within the same network. The client requests the server and gets serviced if it is genuine. The attacker node tries to get through the network by matching various IoT parameters with the genuine nodes. The proposed system is designed in such a way that if any unauthorized user with one or more unmatched parameter tries to login , an alert will be generated and that particular MAC address will be blocked. Once the user is blocked it cannot get access or unblocked.

II. BACKGROUND

A. HTTP(Hyper Text Transfer Protocol)

It is defined as the rules governing the conversation between a Web client and a Web server. It is an Application Layer protocol. It is a request/response protocol that operates by exchanging messages across a reliable TCP/IP connection. It makes use of the Uniform Resource Identifier (URI) to identify a given resource and to establish a connection. The http request method indicates the method to be performed on the resource identified by the given Request-URI. The GET method is used to retrieve information from the given server which is using a given URI A POST in return request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.

B. CoAP(Constrained Application Layer Protocol)

CoAP is an application layer protocol that runs over the unreliable UDP protocol and is designed primarily for the IoT .CoAP provides a REST(GET,PUT,POST,DELETE request) interface similar to HTTP, it focuses on being more lightweight and cost-

effective than its variant for today's Internet. CoAP architecture is divided into two layers: The lower message layer and the upper request/response layer. Lower layer-provides reliability and sequencing. RR layer-manages the mapping between request and response. The message layer provides reliability and sequencing by the means of a stop and wait protocol using the following types of messages: confirmable messages which requires an acknowledgement message as a response, non-confirmable which does not require a response, and reset which is used in case a confirmable message cannot be processed. The request/response layer manages the mapping between requests, responses and their semantics.

C. DTLS(Datagram Transport Layer Security)

Transport Layer Security (TLS) protocol runs over a connection-oriented and reliable channel, typically TCP, to secure network traffic. Due to its lossy nature, it becomes difficult to maintain a continuous connection in 6LoWPAN. Hence an adaptation of TLS for datagram transport (UDP) called DTLS protocol is used. To secure the CoAP communication over the network, DTLS becomes a mandatory security solution- Secure CoAP (CoAPs). DTLS consists of two layers: lower and upper. The lower layer contains the record protocol. It provides connection security, that is connection is private and reliable. It also encapsulates various higher layer protocols. The upper layer contains one of the three protocols: Handshake, Alert and ChangeCipherSpec. The Handshake protocol negotiates and authenticates a session using cryptographic cipher suites, security keys and the application can send secure messages.

III. LITERATURE SURVEY

Shahid Raza et. al [3] provide specification and implementation of IPsec (Internet Protocol security) for 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks). The 6LoWPAN standard's LOWPAN_NHC encoding for the next header compression is proposed for IPsec AH (Authentication Header) header as LOWPAN_NHC_AH Encoding and IPsec ESP (Encapsulating Security Payload) header as LOWPAN_NHC_ESP Encoding. The paper these for the Contiki operating system. SHA 1(Secure Hash Algorithm 1) and AES (Advanced Encryption Standard) implementations are used. Using IPsec, true end-to-end security is implemented between a sensor device and the Internet hosts. Header compression ensures large IPv6 and Transport Layer headers are reduced. Jitendra Singh et. al [4] proposes a technique to remove the problem of cold cache pollution in LRU (Least Recently Used) cache replacement technique. When an object is first accessed, it is placed at a distance D from the bottom of stack. The value of D is taken as half the number of the total objects, i.e. the middle of the stack. If accessed again, it is placed at mid of distance D and the top of the stack. If accessed again, its placed at mid of previous position and the top of the stack. The process continues until object is at top of stack. An object that is not accessed frequently thus takes less time to drop from the cache. The proposed algorithm does not require previous knowledge about workloads, is easier to implement than other advanced algorithms and handles all types of data types. Angelo Capossele et. al [5] explains the integrations of DTLS inside CoAP minimizing memory occupancy. IoT technology, WSN interacts and exchange info outside own network providing an open and standardized solution for IPv6 through 6LoWPAN. TLS protocol provides flexibility to IoT system due to its capability to support negotiation of cryptographic key and symmetric cipher. Security services are flexibly negotiated due to DTLS using cryptography mechanism. ECC based operations speeds up computations of DTLS. Security Associations are created exploiting block wire transfer and message reordering by CoAP to minimize communication overhead and ROM consumption. Chad Brubaker et. al [6] designed, implemented and evaluated the logic for testing of certificate validation in SSL/TLS implementation. This paper focuses on server authentication for protection against man-in-the-middle attack. The testing carried out uncovered many flaws in SSL/TLS libraries. The differential testing implemented describes the vulnerabilities in how the SSL/TLS implementations report error. This testing carried out on 8,127,600 frankencerts uncovered 208 discrepancies. Server authentication guarantees against man-in-themiddle attacks.

Stephen Hallar [7] discusses various things and concepts that collectively describe IoT. The paper discusses about device's identification and resolution. It explains that any object with its attributes describing its state, useful from the user's perspective can be termed as "Entity of Interest". Resolution and discovery, the two approaches to find the information about an entity are described in detail here. The distinction between entities and the devices has been described.

Karthikeyan Bhargavan et. al [8] have implemented, tested and cryptographically verified a reference implementation of TLS1.2. The code is written in F# and specified in F7. This paper provides security by using authenticated stream encryption for record protocol and using key establishment for handshake. This can be verified using f& typechecker. The verified reference implementation of TLS in the paper is interoperable with mainstream web browsers and servers. The theorems implemented in the paper ensure end-to-end security.

Nadhem J. AlFardan et. al [9] present the plaintext recovery attacks against TLS and DTLS based on the timing analysis. They have performed experimental results to show the feasibility of the attacks for OpenSSL implementation. Countermeasures like add random time delays and use authenticated encryption for these attacks are provided. TLS requires a multi-session attack hence this limits the practicability of attacks but can be improved using standard techniques.

Mikael Asplund [10] aims to identify the security requirements in various sectors like health management, energy, etc. The issue of resource efficiency for security building blocks is studied in detail. Various Intrusion detection systems like Snort in various processors like Raspberry are studied. Interview based results are presented asking the various actors of the society their perceptions and attitude regarding the IoT. Risk assessment results are also provided along with the infrastructure dependency.

Jana Krimmling et. al [11] present a framework to evaluate lightweight intrusion detection techniques for CoAP applications. The framework combines an OMNeT++ simulation with C/C++ application code to evaluate intrusion detection techniques for a smart public transport application. Evaluations indicate that a hybrid IDS approach is favorable. As a result, they give a hardware testbed and a simulation setup implementing the smart transport scenario. While the testbed provides general functional validation of the application, protocols and IDSs also are applied in the simulation to analyze the quality of different IDS approaches.

IV. PROPOSED SYSTEM

Figure shows the proposed system architecture for end-to-end secure communication between the IoT devices. The system architecture aims to provide security at the application layer to all the devices connected in the same network. The setup consists of server , client IoT devices and attacker. The client requests service from the server. For accessing the service, the client uses the MAC address. The server authenticates the client when the client requests for service. A database is maintained by the server for the information of each client requesting for service along with the information on status of its denial or acceptance of the service .Android app sends request for bot connection to server .Server has its static ip address, acknowledgement is sent from server to android app for bot connection.

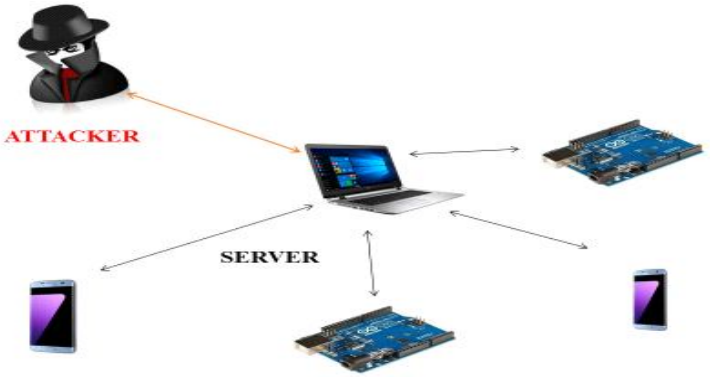


Fig 1. Client IOT devices

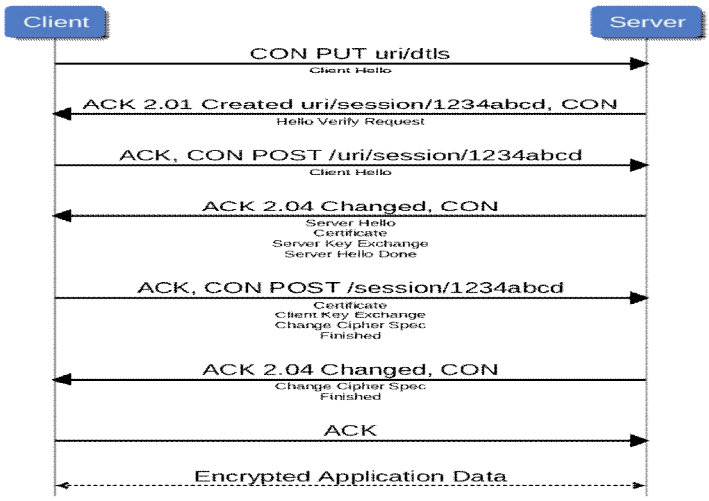


Fig 2: Handshaking Diagram

V. FUTURE SCOPE

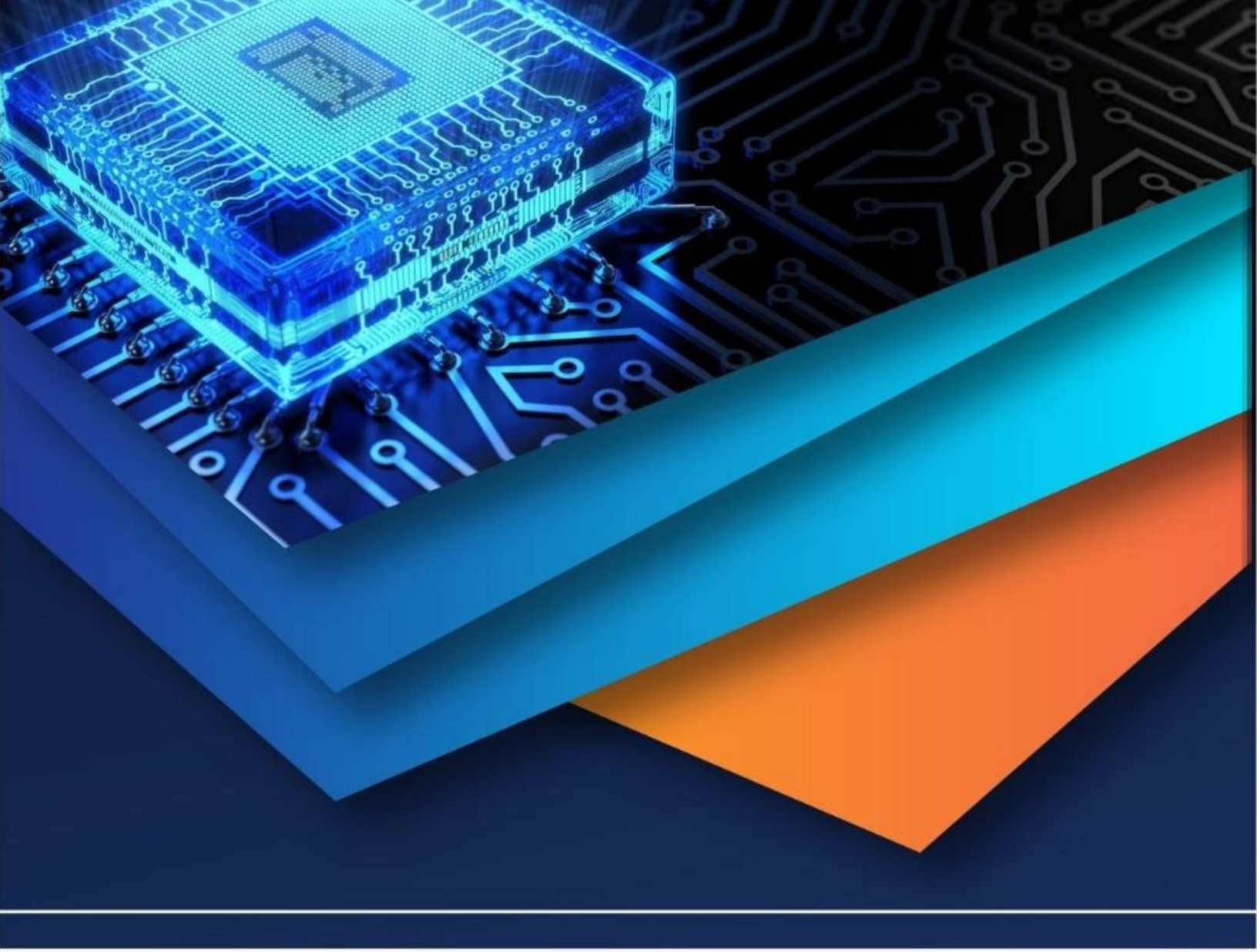
The proposed system can be implemented in a larger network area with a large number of IOT devices connected and also non-constrained devices. It can be deployed in automated system like SCADA (Supervisory Control and Data Acquisition). It can be used in big organizations where access to sensitive data outside the organization should not be encouraged.

VI. CONCLUSION

Thus, a secure communication between constrained as well as normal devices is made possible. Full implementation of CoAP and DTLS to provide security over computer network is performed. Handshake is guaranteed to communicate between the devices. Attack detection and blocking of it from accessing the Network is also provided.

REFERENCES

[1] Ajit A. Chavan, Mininath K. Nighot; "Secure and Cost-effective Application Layer Protocol with Authentication Interoperability for IoT"; International Conference on Information Security &amp, Privacy (ICISP2015); 11-12 December 2015, Nagpur, India.
[2] Zach Shelby "6LoWPAN: The Wireless Embedded Internet" Sensinode, Finland
[3] Shahid Raza, Simon Duquennoy, Tony Chung†, Dogan Yazar Thiemo Voigt and Utz Roedig; "Securing Communication in 6LoWPAN with Compressed IPsec"; Lancaster University School of Computing and Communications, Lancaster, UK; 2011 IEEE
[4] Jitendra Singh Kushwah, Jitendra Kumar Gupta, Brijesh Patel; "Modified Lru Algorithm to Implement Proxy Server with Caching Policies"; International Journal of Computer Trends and Technology- volume2 Issue1- 2011
[5] Angelo Capossele, Valerio Cervo, Gianluca De Cicco and Chiara Petrioli; "Security As A Coap Resource: An Optimized DTLS Implementation For The IoT"; IEEE Xplore; 2015/June/12
[6] Chad Brubaker, Suman Jana, Baishakhi Ray, Sarfraz Khurshid,Vitaly Shmatikov; "Using Frankencerts for Automated Adversarial Testing of Certificate Validation In Ssl/Tls Implementations"; 2013 IEEE Symposium on Security and Privacy.
[7] Sephan Haller; "The Things in the Internet of Things"; Internet of Things Conference 2010, Tokyo, Japan.
[8] Karthikeyan Bhargavan, C´edric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub; "Implementing TLS with Verified Cryptographic Security"; 2013 IEEE Symposium on Security and Privacy.
[9] Nadhem J. AlFardan and Kenneth G. Paterson; "Lucky Thirteen: Breakin The Tls and Dtls Record Protocols"; 2013 IEEE Symposium on Security and Privacy.
[10] Mikael Asplund, Simin Nadjm-Tehrani;"Attitudes and Perceptions of IoT Security in Critical Societal Services"; IEEE Access; May 23, 2016
[11] S. Vanjale, P.B. Mane, S. Thite Elimination of Rogue access point in Wireless Network", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-201
[12] S. Vanjale, S. Thite, "A novel approach for fake access point detection and prevention in wireless network", International Journal of Computer Science Engineering and information,Technology Research (IJCSEITR), Vol 4, Issue 1, Feb 2014, 35-42



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY