ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# DESIGN AND DEVELOPMENT OF SECURITY FRAMEWORK BY USING APPLICATION LAYER PROTOCOL

**Asawari Waikul, Snehal Belgaonkar, Karishma Tyagi, Prerna Sharan**
Department of Information Technology, BVCOEW, Pune, India
**G. V. Ramana Rao**
Central Water and Power Research Station, Pune, India
**DOI**: 10.5281/zenodo.557204

## ABSTRACT
Internet of Things (IoT), a revolution in the ordinary life of people, transforming the global IT landscape, the development strategy of different types of businesses in various sectors and much more. Due to the various flaws like limited energy, low processing power, lossy wireless links, constrained storage of the IoT devices; it's the need of the hour that security should be the trivial enabler of IoT. Till date, no silver bullet exists that can effectively implement security in IoT on devices. The closed source security solutions do not help to inculcate security in IoT so that they can communicate securely.
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 proxy server. Depending on various factors like timestamp, the developed application using .net framework detects and blocks the access to the attacker.

**KEYWORDS**: IoT, Proxy Server, SQL Injection

## 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 proxy server and gets serviced if it is genuine. The attacker node tries to extract the password from the database using various patterns of the password. The proposed system is designed in such a way that if any user tries to login within a specified time limit incorrectly, an alarm will be generated and that particular IP address will be blocked. Also there are cases when the genuine user cannot get access to the services due to technical faults and they also gets blocked. So, the Administrator also

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

has the rights to unblock the IP address as and when required. SQL Injection attacks are addressed and corresponding attacker is banned from the network.

## RELATED WORK

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. Th 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-the-middle 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

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

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.

## BACKGROUND

### HTTP: Hypertext 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 using a given URI
A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.

### OPEN SSL

It is defined as a software library for applications to secure communications over computer networks. It is an open source implementation of the SSL and TLS protocols.
SSL, Secure Sockets Layer, a standard behind secure communication on the Internet, integrating data cryptography into the protocol. It encrypts and decrypts the data. It makes the use of certificates and cryptographic algorithms.

### PROXY SERVER

Proxy server is a computer that sits between a client computer and the Internet, and provide indirect network services to a client. It is a computer that sits between a client computer and the Internet, and provide indirect network services to a client. A client computer is connected to the proxy server, which acknowledges client requests by providing the requested resource/data from either a specified server or the local cache memory. Client requests include files or any other resources available on various servers.


### SQL INJECTION

SQL injection is the placement of malicious code in SQL statements, via web page input. Some web developers use a "blacklist" of words or characters to search for in SQL input, to prevent SQL injection attacks. In order to run malicious SQL queries against a database server, an attacker must first find an input within the web application that is included inside of an SQL query. In order for an SQL Injection attack to take place, the vulnerable website needs to directly include user input within an SQL statement. An attacker can then insert a payload that will be included as part of the SQL query and run against the database server.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

## DTLS

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.

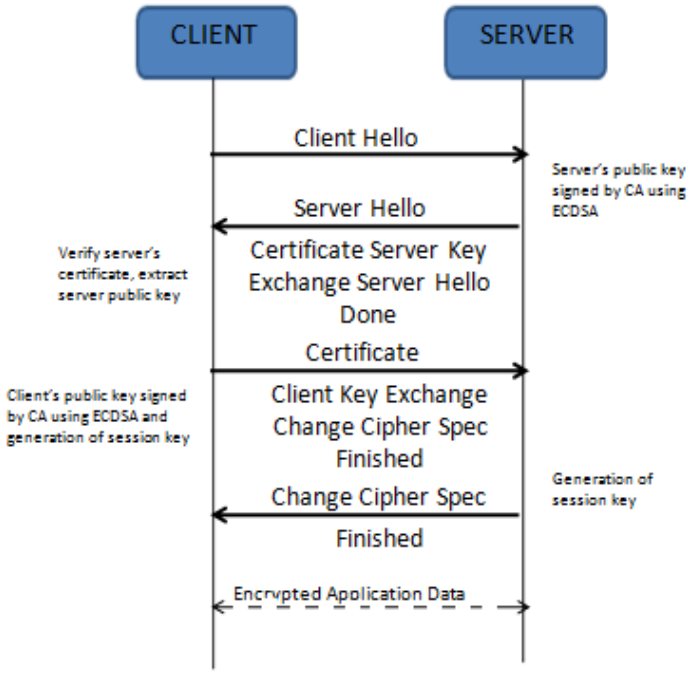


**Figure 5: DTLS Handshake**

Handshake protocol, as shown in figure 5, is implemented in between the client and the server. First client sends a Hello message. This is followed by server sending a Hello message along with the server's public key. The server generates a session key and exchanges it with the client. The session key is used to identify an active session state. Then the application data is communicated between the two in encrypted form.

The Alert protocol conveys warning or fatal messages and a description of the alert. The ChangeCipherSpec message notifies that subsequent messages will be encrypted by the newly negotiated CipherSpec and keys.

## PROPOSED SYSTEM

Figure 6 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 a proxy server and client IoT devices.

The client requests service from the proxy server. For accessing the service, the client uses the username and password. The proxy server authenticates the client when the client requests for service. A database is maintained by the proxy server for the information of each client requesting for service along with the information on status of its denial or acceptance of the service.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

By using the URL to access the proxy server (which opens a port to accept the client request and its IP address) and logging in using username and password, the client devices can access the services of the proxy server, if they are authorized. If unauthorized, the access id denied.
If an attacker tries to access the resources of the proxy server by performing SQL injection attack, the login attempt fails. If such a situation repeats itself five times in 5 milliseconds then an alert message with an alarm ringing on the proxy server alerts the proxy server admin of an attack by an attacker. Then the proxy server takes the necessary precaution by blocking the attacker's IP address.

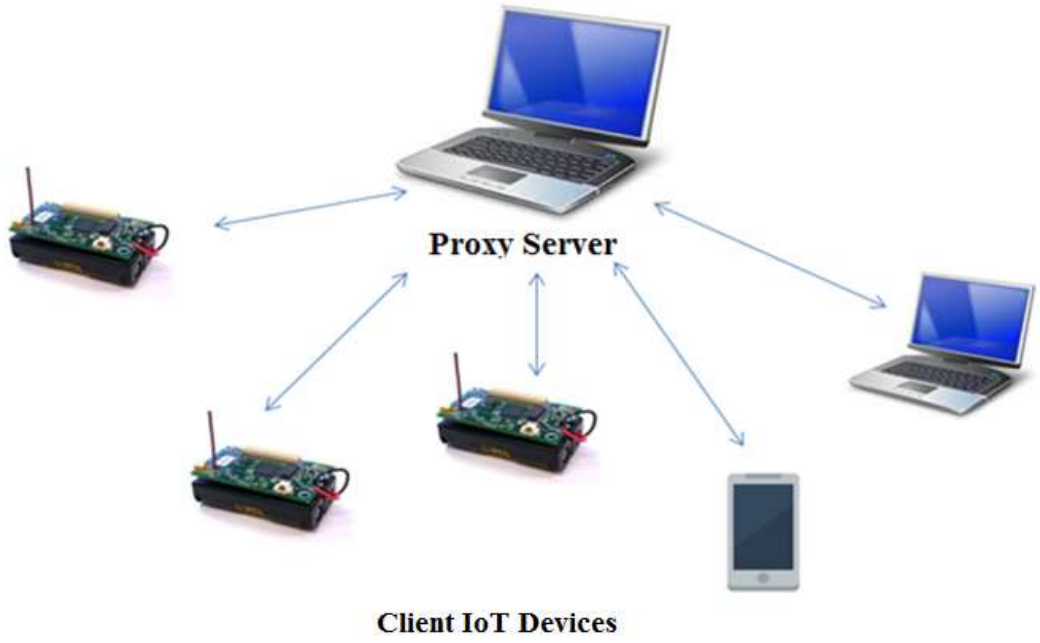


**Figure 6: System Architecture**

The proxy server maintains a record of the blocked IP addresses. The blocked IP addresses are listed by the proxy server and admin can unblock them.

## RESULTS AND DISCUSSION

### 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 organisations where access to sensitive data outside the organization should not be encouraged.

## CONCLUSION

Thus, a secure communication between constrained as well as normal devices is made possible. Full implementation of TLS and SSL 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.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

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. Stephan 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. Jana Krimmling and Steffen Peter; "Integration and Evaluation of Intrusion Detection for CoAP in Smart City Applications"; M2MSec- Workshop on Security and Privacy in Machine-to-Machine Communications, in conjunction with IEEE Conference on Communications and Network Security(CNS), San Francisco, CA, USA; October 29-31, 2014.