Comparision of Application Layer Protocol For IoT Via Experimentation

Kuntal V. Bhangale
Department of Computer Science and engineering
SSBT's College of engineering and technology ,
Kaviyatri Bahinabai Chaudhari N.M.U, Jalgaon ,[M.S], India
Email: Kbhangale25@gmail.com

Nilima P. Patil
Department of Computer Science and engineering
SSBT's College of engineering and technology,
Kaviyatri Bahinabai Chaudhari N.M.U, Jalgaon ,[M.S], India
Email: ramtekenilima25@gmail.com

Abstract— **Internet of Thing is an open network of intelligent objects to share information about devices. The IoT architecture consist of sensor node use for collection of data, gateway use for aggregation of data, Cloud is use for collects the data. IoT communication consist of protocols which are resource optimized such as Constrained Application Layer protocol(CoAP), Message Queue Telemetry Transport(MQTT), Representational State Transfer(REST). Application layer protocols vary in the performance with varying payload and network bandwidth. Hence there is need for transmission of payload to the cloud in optimized and secured way. Here, in IoT the possibility to explored HTTP2 protocol which is not much popular amongst the IoT Developer. Security is also the major aspect in IoT as the data is sent to cloud, it is more prone to man-in-the middle attacks. Hence in this paper, proposing a solution which support multiple protocols to collect the data from IoT devices and transfer it fast and securely to the cloud. It is possible via header translation for inter-protocol transfer. This approach also takes care of the man-in-the middle attack as data is sent via SSL(Secured Socket Layer) to the cloud. In the approach the data is collected from various sources supporting multiple protocols and is sent to the cloud using only REST protocol encapsulated in SSL. During the proposed system it is found that the data is sent to the cloud via single secured protocol, significantly improves the transmission time as header translation and encapsulation is done locally in IoT domain before sending to the cloud. The evaluation result shows improved transmission time and no possibility of man-in-the middle attack as SSL certificates are used.**

Keywords—**Internet of Thing, Secure Socket Layer, Application Layer Protocols, Round Trip Time, MQTT, CoAP, HTTP2, REST**

I.INTRODUCTION

It has been more than fifteen years since the term Internet of Things was introduced to the public. But still no common IoT architecture has not been clearly defined and no common agreement to defining protocol and standards for all IoT modules. IoT is the internetworking of smart device, things and embedded with electronics and software to provide network connectivity which enable objects to collect and exchange data. The application running on IoT is responsible for M2M(Machine2Machine) communication between devices. IoT application uses application layer protocols are MQTT, CoAP, REST, AMQP, XXMPP, HTTP2 for transferring request/ response between devices. Developers are using currently available technologies to build the IoT applications and working on adapting protocols suitable for IoT devices in order to optimize communication. Protocols vary in the performance as the payload size changes. Their is need for developing system that transmit payload efficiently and securely.

IoT developers community is continuously working on improving the communication in IoT system to transmit the data from IoT devices to the cloud. In proposed system provide the various protocols to be used in the IoT as well as the newly invented advance protocols such as HTTP2. The proposed system will give flexibility to the IoT developers to select any protocol in IoT for developing IoT system application. These will reduce the overhead of multiple configurations for multiple protocols in IoT and transfer the data securely to the cloud via single protocol. Also with the approach one of the common security attacks such as man-in-the middle attack is avoided.

The paper is organize as follows : Section II described the Related Work of application layer protocol. Section III described the Methodology. Section IV described the Result and Discussion, while Section V Conclusion and Future work of the paper.

II. RELATED WORK

The structure of literature survey is shown in Figure 1. Communication plays important role in transmission between client and server.

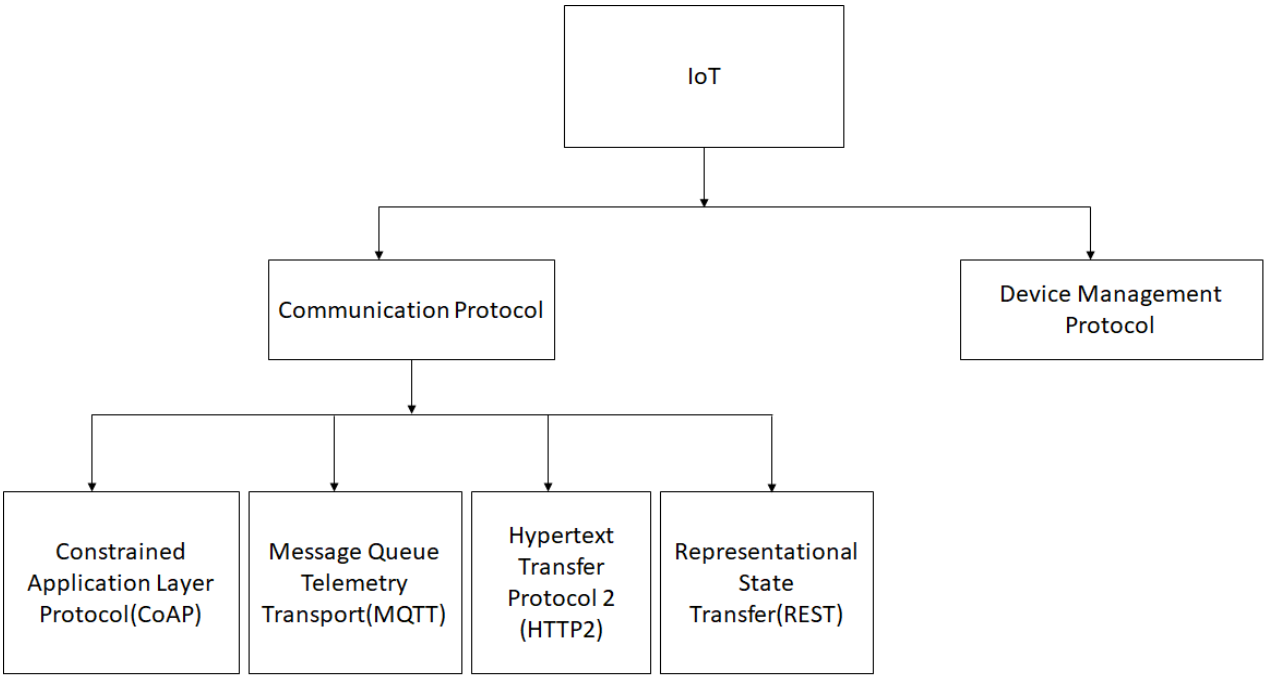

Figure 1: Structure of Literature survey

Dinesh Thangavel et al., in [1], proposed the performance measurement of MQTT and CoAP through Middleware. CoAP and MQTT implemented on common middleware that provides common programming interface. Message Queue Telemetry Transport, Constrained Application Protocol are use to handle requirement of wireless sensor network environment. Experimental result shows that performance of protocols are dependent on network conditions. MQTT protocol performance is high for higher message size and low for lower message size. CoAP protocol generates less traffic for lower packet. The protocol performance depend on difference in the network performance that can improve the help middleware.

Upendra et al., in [2], proposed application layer protocols for IoT. The main objective is to analyzed the performance of CoAP, MQTT, REST protocols in IoT environment. Raspberry pie is use for gateway device which collects data from various sensors nodes and send to cloud through network. Chosen protocols can reduce network traffic, improve reliability. Experimental result indicate performance is measure in term of bandwidth consumed and time taken by protocol. 4G and broadband connection is use for performance measurement of protocol. The bandwidth consumption remains same with change in network but time required changes as network varies. Results show that CoAP is best performer for small payloads and bad performer for bigger payloads. MQTT protocol performance is longer as payload size increases.

Stefan et al., in [3], The system compare the performance of three application layer protocols that are CoAP, MQTT, Websocket. Three protocols implemented in low cost, low complexity hardware platform, suitable for IoT applications. Performance parameters are average round trip time, efficiency, overhead. IEEE 802.11 is use as air interface between IoT devices and access point and connected to the final server. Two different network setting is considered: first is local area network(LAN) configuration, where AP and server in same LAN, second is remote server. Results shows that COAP achieves the highest protocol efficiency and lower RTT than websocket. MQTT protocol performance depend on quality of service.

Tarek, in [4], proposed Effective and Extensive Virtual Private Network. A virtual private network allows provisioning of private network services for an organization over public network. Virtual Private Network transform the characteristics of publically which may be non secure network of private secure network through using encrypted tunnels. The work is standardies in Effective Extensive VPN and it transmits small data size through network in a reasonable time without affecting the security level. Effective Extensive virtual private network is more effective where it takes small data transmission time with achieving high level security and also it is not effective for any specific environment.

Amankatiyar et al., in [5], proposed Research on Tunneling Techniques in Virtual Private Networks. Virtual private networks is established for information exchange between client and server. Various protocols are present for tunneling such as GRE, L2TP, IPSec and IP. Tunneling is encapsulation technique in in which protocol X in encapsulate into Protocol Y. Protocol X is travel through public network. Generic Routing Encapsulation protocol is general encapsulation protocol which aiming scheme

IPX encapsulated in IP and X.25 encapsulate in IP. The L2TP is encapsulation scheme which encapsulated IP within UDP within L2TP within protocol X. IPSec encapsulation scheme which encapsulate IP within AH or ESP.

Priyanka and Yoohwan Kim, in [6], proposed Implementation and Comparison of M2M Protocols for Internet of Things. The system is to analyze the efficiency and applicability of different M2M protocols for IoT communication. Protocols are evaluated on raspberry-pi and sensors. The major protocols that for for IoT are MQTT and CoAP are light weight in terms of operation and data transfer IoT. In the experiment contain one publisher, server and broker. MQTT and CoAP achieved 100% data transfer even if packer loss is implicitly induced. As packet loss is less then CoAP handles less amount of data as compared to MQTT. Finally results shows the performance of protocols are depends on network condition. Efficiency of protocol change according to data overhead, middleware and gateway

III.METHODOLOGY

In proposed solution, Application Layer protocols are use in the systems are MQTT, CoAP, HTTP2 and REST. Header translation is done on protocols such as CoAP, MQTT, HTTP2. In header translation original protocols header are converted into REST protocol header. REST protocol performance is very efficient for any payload between client and server so CoAP, MQTT, HTTP2 protocols performance are improved after the translation. After the header translation REST protocol are encapsulated in internet secure connection protocol(ISC). After that encapsulatated REST protocol are transfer through secure communication between client and server. Secure communication between client and server is done through SSL tunneling. In SSL tunneling first step is to carry out authorization between client and server after that header and data transfer through client and server. Header and data is decapsulated then reach to the REST server which is present on cloud.

Architecture

Proposed solution consist of the 3 parts. First, client running on the different protocols such as CoAP, MQTT, and HTTP2. Second, CoAP, MQTT, HTTP2 protocol header is translated into REST protocol header format then encapsulate in the SSL protocol. Third, the SSL socket server which is running on cloud and stores the data on cloud storage. In the proposed system the client running on various protocols generates the source of data that is these clients are assumed to be industry standard applications which collects the data via various sensor nodes. In proposed system the various payloads are generated from stub and is used by these client viz. CoAP client, MQTT client and HTTP2 client. The Transmission of the data from IoT premises to the Cloud takes place via single application running on REST encapsulated in custom SSL socket layer protocol. Proposed system architecture is shown in Figure 2.

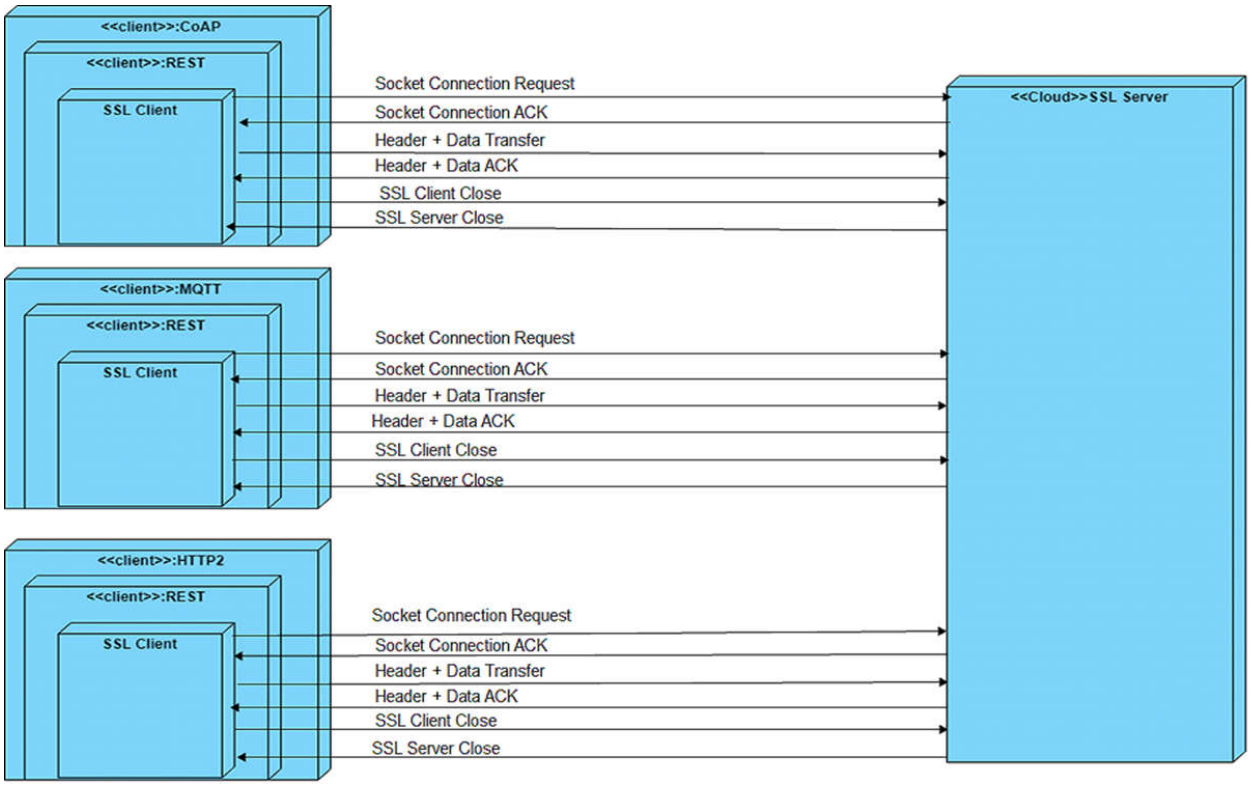

Figure 2 : Structure of Proposed system

Secure connection through tunneling given in Algorithm 1. The propose algorithm is provide secure connection between client and server. Secure connection is established then header and payload is transfer between client and server

Algorithm 1: Secure connection through Tunneling

Require: S_{Client} *is secure socket SSL client.* S_{Server} *is secure socket SSL server*

1: *Initialize* S_{Server} *with certificate file*
2: *Initialize* S_{Client} *with certificate file*
3: Perform below steps
4: if $Error_{(Flag)} == 1$ then
5: *close connection*
6: end if
7: $S_{Client} \rightarrow$ *Socket connection request to* S_{Server}
8: S_{Client}*receiveSocket connection ack* $\leftarrow S_{Server}$
9: *Header and data send* $\rightarrow S_{Server}$
10: *Response receive Header and data* $\leftarrow S_{Client}$
11: *ConnectionClose* $S_{Client} \rightarrow S_{server}$
12: $S_{Client} \leftarrow$ *ConnectionClose* S_{Server}

Header Translation given in Algorithm 2. Header translation algorithm improved overall transmission time of payload between IoT device and cloud. These is achieve by converting header translation of CoAP, MQTT, HTTP2 protocol header is translated into REST header.

Algorithm 2: Header Translation

Require: C is Set of CoAP protocol header, M is set of MQTT protocol header, R is set of REST protocol header, H is et of HTTP2 header, S is set of secure Socket connection Protocol header.

Start (S) on cloud and initialize secure certificate
Initialize (I) on client
Perform step below at client
$REQ \leftarrow Request\ of\ client\ protocol$
if $Header_{(REQ)} = Header_{(C)}$ **then**
  $H_{(REST)} \leftarrow convert\ CoAP \rightarrow REST$
  $D_{(REST)} \leftarrow Add\ payload\ to\ REST$
end if
if $Header_{(REQ)} = Header_{(M)}$ **then**
  $H_{(REST)} \leftarrow convert\ MQTT \rightarrow REST$
  $D_{(REST)} \leftarrow Add\ payload\ to\ REST$
end if
if $Header_{(REQ)} = Header_{(H)}$ **then**
  $H_{(REST)} \leftarrow convert\ HTTP2 \rightarrow REST$
  $D_{(REST)} \leftarrow Add\ payload\ to\ REST$
end if
$Send\ data\ using\ SSL\ (H_{(REST)}, D_{(REST)})$
$RES \leftarrow Response\ receive\ from\ SSL$
$H_{(REST)} \leftarrow Response\ Header_{(RES)}$
$D_{(REST)} \leftarrow Response\ Data_{(RES)}$
if $Header_{(C)} \leftarrow Header_{(REST)}$ **then**
  $H_{(CoAP)} \leftarrow convert\ REST \rightarrow CoAP$
  $D_{(CoAP)} \leftarrow Add\ payload\ to\ CoAP$
end if
if $Header_{(M)} \leftarrow Header_{(REST)}$ **then**
  $H_{(MQTT)} \leftarrow convert\ REST \rightarrow MQTT$
  $D_{(MQTT)} \leftarrow Add\ payload\ to\ MQTT$
end if
if $Header_{(H)} \leftarrow Header_{(REST)}$ **then**
  $H_{(HTTP2)} \leftarrow convert\ REST \rightarrow HTTP2$
  $D_{(HTTP2)} \leftarrow Add\ payload\ to\ HTTP2$
end if

IV. RESULT AND DISCUSSION

The performance of proposed system against the existing system is measured in Round Trip Time. Round Trip Time is measure in milliseconds Different protocols have different latency in communication. The total round time is calculated based on the below formula.

$$t\_round = t\_up + t\_down$$

Where, t _round : Total Round Trip time to payload to cloud
t _up : Total time to upload the given payload to cloud
t _down : Total time to download the given payload from cloud

Experimental result consist of the round trip time of protocols such as CoAP, MQTT, HTTP2 of various payload sizes with respect to proposed system as well as existing system. The effectiveness of proposed system is carried out by involvement of proposed protocol is proved better by carrying out the experiment.

Table 1 shows Round Trip time of proposed approach and existing approach for payload 100Bytes. The graph shows in Figure 3 is plotted by consider the Round Trip time. Round trip time is calculation of both upload time and download time.

Table 1: Round Trip Time for Payload 100Bytes

Protocols	CoAP	MQTT	HTTP2
Proposed Approach	650	951	489
Existing Approach	1056	1455	851

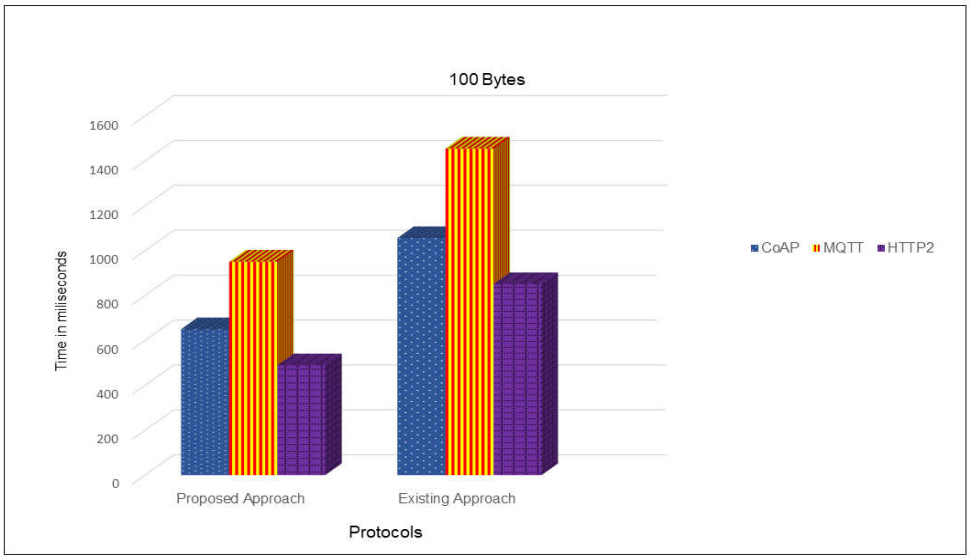

Figure 3 : Round Trip time for payload 100Bytes

Table 2 shows Round Trip time of proposed approach and existing approach for payload 1KBytes. The graph shows in Figure 4 is plotted by consider the Round Trip time. Round trip time is calculation of both upload time and download time.

Table 2 Round Trip Time for 1KBytes

Protocols	CoAP	MQTT	HTTP2
Proposed Approach	786	850	756
Existing Approach	950	1114	1150

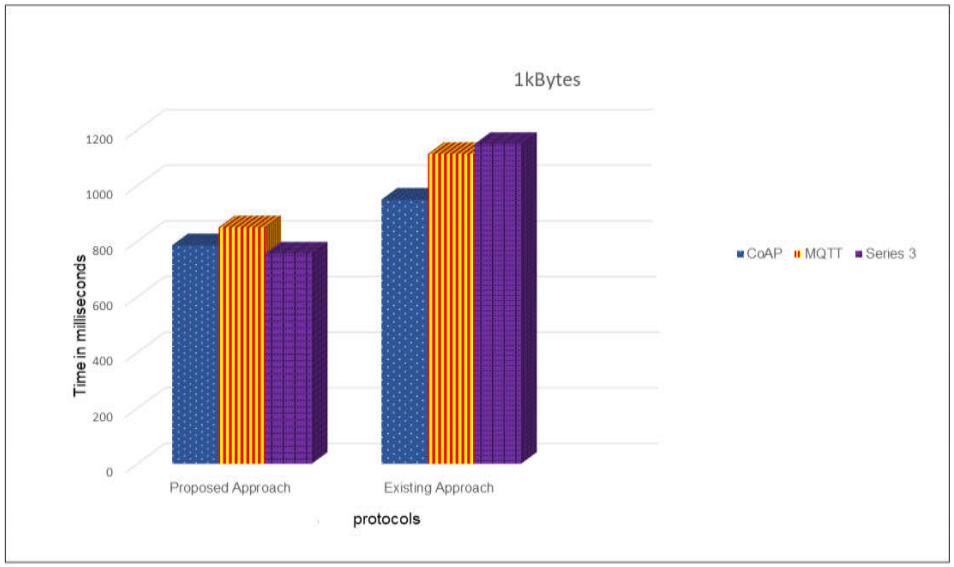

Figure 4 : Round Trip time for payload 1KBytes

Table 3 shows Round Trip time of proposed approach and existing approach for payload 10KBytes. The graph shows in Figure 5 is plotted by consider the Round Trip time. Round trip time is calculation of both upload time and download time.

Table 3 : Round TripTime for 10KBytes

Protocols	CoAP	MQTT	HTTP2
Proposed Approach	1050	1650	1258
Existing Approach	1526	1899	1711

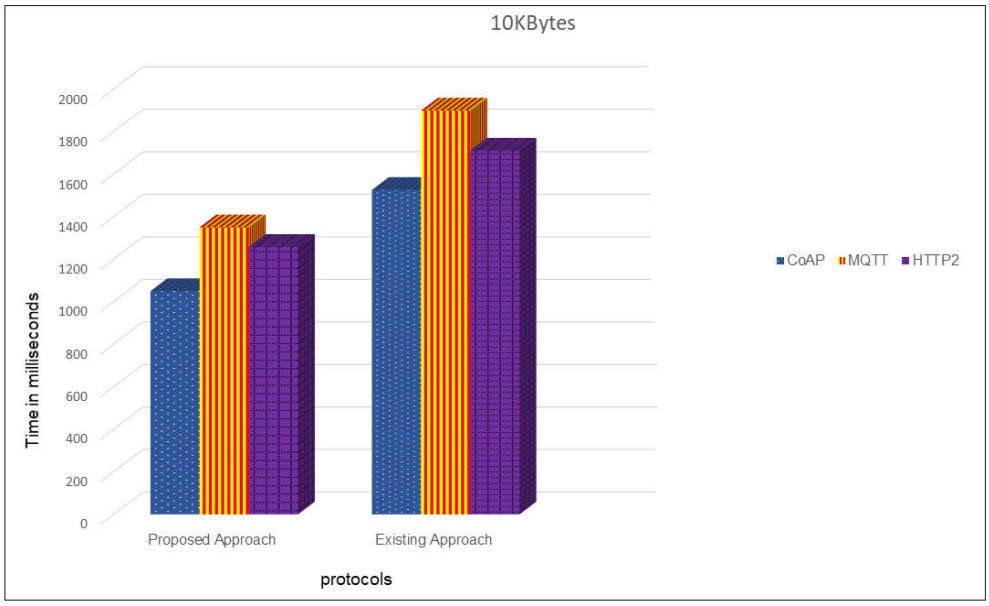

Figure 5: Round Trip time for payload 10KBytes

Table 4 shows Round Trip time of proposed approach and existing approach for payload 100KBytes. The graph shows in Figure 6 is plotted by consider the Round Trip time. Round trip time is calculation of both upload time and download time.

Table 4 : Round Trip Time for 100KBytes

Protocols	CoAP	MQTT	HTTP2
Proposed Approach	1036	1211	1413
Existing Approach	16521	17250	7699

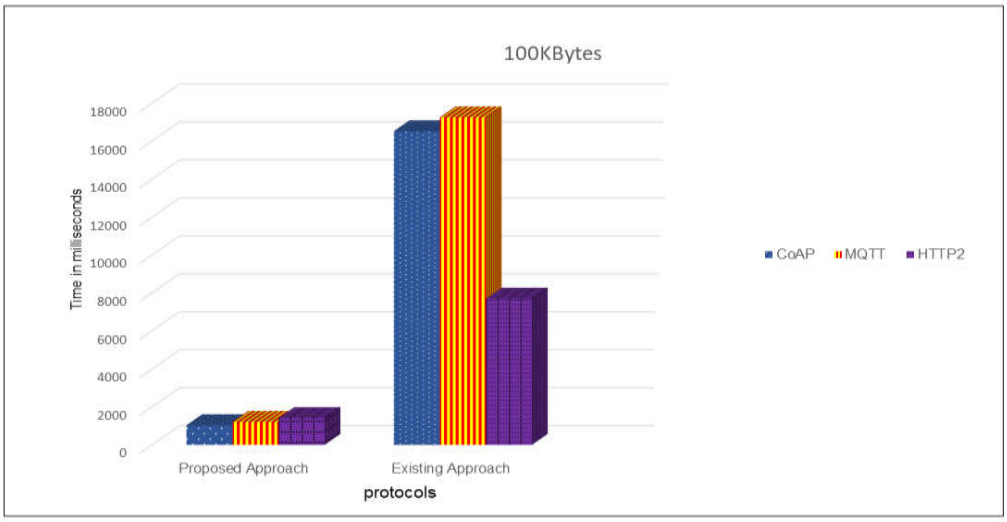

Figure 6 : Round Trip time for payload 100KBytes

Table 5 shows Round Trip time of proposed approach and existing approach for payload 1MBytes. The graph shows in Figure 7 is plotted by consider the Round Trip time. Round trip time is calculation of both upload time and download time.

Table 5 : Round Trip Time for 1MBytes

Protocols	CoAP	MQTT	HTTP2
Proposed Approach	1653	1960	1885
Existing Approach	16285	18960	9275

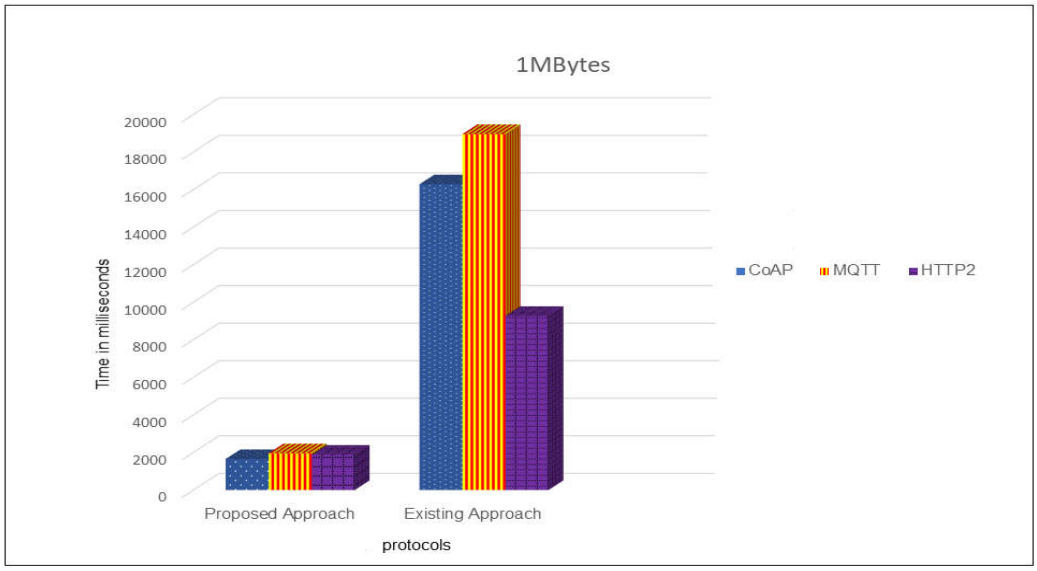

Figure 7 : Round Trip time for payload 1MBytes

The implementation result of the proposed system seems to have reduced the transmission time for higher payload as well. From the past analysis in IoT domain it has been observed that CoAP protocol performance is efficient for smaller payload, as payload size increases performance of CoAP decreases. MQTT protocol performance is worst for both smaller and larger payload. Hence, proposed approach the data is transmitted to the cloud via REST encapsulated in SSL. The transmission time seems to have increased here, because the header translation and encapsulation is done locally in IoT domain and then the data is transferred to the cloud. For safe and secure communication between client to remote server can be possible through SSL

tunneling. In SSL tunneling encapsulating REST protocol packet into SSL protocol which prone network attack between client and server. Hence, secure communication between client and server is achieved. Single secure server present on cloud which reduces multiple server overhead on cloud. These reduces effort reduces effort required for developers to develop different server on cloud depending on client configuration. Therefore the result of experiment shows improvement of transmission time and security of the system.

V.CONCLUSION AND FUTURE WORK

In IoT (Internet of Things) domain the protocols use for communication are called as M2M protocols (Machine To Machine Protocol). The protocols are majorly CoAP, MQTT and REST. The protocols are responsible for communication between machines i.e. sensor nodes in IOT and the Cloud storage. The sensor data is aggregated on IoT gateway and then transmitted to the cloud. It is observed that the protocols varies in terms of time consumption for different set of payloads. Also the security is the major aspect for IOT domain communication and it affects the performance of the protocol. There are newer advance protocols available in Web domain for communication but its use is still very less popular amongst IOT developers. In the proposed system is a secure for IoT which can communicate with different types of clients supporting COAP, MQTT and HTTP2 protocols converted into REST protocol. Proposed system is design for analysis of the performance of the existing protocols and advance protocols in terms of turn round time. The proposed system is flexible enough to communicate with different type of clients to gather the data and transmitting it to the cloud via secured communication running on SSL(TLS). The system help the IoT developers to securely transmit the data to the cloud even through data generated by variety of clients like CoAP, MQTT, HTTP2. The system will beneficial for the industries where different protocols are use instead of single protocol to transmit the different types of payload and different size of payloads to the cloud. The experimental result of the system shows the performance of the system is efficient and secure and take less amount of time than existing system. Future work will be aimed at implementing the protocols in the actual industry wide lab environment and compare the protocol performance. The system can also be extended to send data using other protocols(other than SSL) to cloud on the go (runtime) based on payload and bandwidth if required.

REFERENCES

[1] Dinesh Thangavel, Xiaoping Ma, Alvin Valera ,Colin Keng Yan Tan, “Performance Evaluation of MQTT and CoAP via a Common Middleware”, IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp.1-6, april 2014.

[2] Upendra Tandale, Dr. Bashirahamad Momin, Deva P. Seetharam, “An Empirical Study of Application Layer Protocols for IoT”, IEEE International Conference on Energy, Communication, Data Analytics and Soft Computing(ICECDS), pp.2447-2451, 2017.

[3] Stefan Mijovic, Erion Shehu, Chiara Buratti, “Comparing Application Layer Protocols for the Internet of Things via Experimentation”, IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), pp.1-5, 2016.

[4] Tarek S.Sobh, “Effective and Extensive Virtual Private Network”, Scientic Research Journal of Information Security, Volume 2, Number 1, pp.39-49, January 2011.

[5] Amankatiyar, AnupamVishwarkarma, Aditya soni, Hemantjain, Jayesh Surana, “Research on Tunneling Techniques in Virtual Private Networks”, International Journal of Engineering Development and Research(IJEDR), Volume 5, Issue 2, pp.2321-9939, 2017.

[6] Priyanka Thota, Yoohwan Kim, “Implementation and Comparison of M2M Protocols for Internet of Things”, IEEE 4th Intl Conf on Applied Computing and Information Technology/3rd Intl Conf on Computational Science/Intelligence and Applied Informatics /1st Intl Conf on Big Data, Cloud Computing, Data Science and Engineering(ACITCSIBCD), pp.43-48, 2016.

[7] Hedi I, Speh I, Sarabok A, “IoT Network Protocols Comparison for the Purpose of IoT Constrained Networks”, IEEE Fourty International Convention on Information and Communication Technology, Electronics and Microelectronics(MIPRO), pp.501-505 May 2017.

[8] Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez Gallego, Jesus Alonso Zarate, “A Survey on Application Layer Protocols for the Internet of Things”, Transaction on IoT and Cloud Computing, Volume 1, No 1, pp.11-17, march 2015.

[9] Vasil Sarafov, “Comparison of IoT Data Protocol Overhead”, Network Architectures and Services, Website: https://www.net.in.tum.de, accessed on 23 March 2018

[10] Kushal Reshamdalal, Bobby Singh Rathore, “A Comprehensive Study of Application Layer Protocols (ALP) for IoT Application”, International Journal of Innovations and Advancement in Computer Science, Volume 6, pp.2347-8616, October 2017

[11] Markel Iglesias Urkia, Adrian Orive, Aitor Urbieta, “Analysis of CoAP Implementations for Industrial Internet of Things: A Survey”, The 8th International Conference on Ambient Systems, Networks and Technologies, pp.1877-0509, 2017

[12]Anusha.M, Suresh Babu.E, Sai Mahesh Reddy.L, Vamsi Krishna.A, Bhagyasree.B, “Performance Analysis of protocols of Internet of things: A Qualitative Review”, International Journal of Pure and Applied Mathematics, Volume 115, Number 6, pp.37-47, 2017