iAAP: INTERDEPENDENCY ATTRIBUTE AUTHENTICATION PROTOCOL FOR IoMT SYSTEMS SECURITY ENHANCEMENT AND ANALYSIS

Sindhuja R[1], Arvind S. Kapse[2*]

[1,2]Information Science and Engineering, New Horizon College of Engineering, Bengaluru,Visvesvaraya Technological University, Belagavi-590018

Emails: sindhu.muthu@gmail.com[1], dr.arvindsk@newhorizonindia.edu[2]*

ABSTRACT

Internet has changed and evolved since its origin and in recent time the communication channel for the internet has developed a flexible system design to accommodate newer devices and customized services. Internet of Medical Things (IoMT) is one such blooming service for larger data processing and customization. In this paper, we propose a novel interdependency attribute protocol for authentication and enhancing security aspects of IoMT communication. The protocol is developed on remote monitoring and Message Queuing Telemetric Transport (MQTT) protocol foundation values to secure data transmission and communication via active public domain internet and cloud storage. The approach is developed on machine learning models for attribute customization and classification. The model has been validated with AWS open pipeline cloud platforms for IoMT devices customization. The IoMT device cloud server evaluation and authentication via interdependency attribute protocol has outperformed the existing security models and analysis with Machine learning tools.

Keywords: IoMT; Interdependency security; MQTT; data security analysis; Cloud server analysis.

1.0 INTRODUCTION

The Internet of Things (IoT) represents a transformative technological paradigm that has revolutionized human interaction with the surrounding environment. Fundamentally, IoT constitutes an expansive network of interconnected devices and objects, encompassing a diverse spectrum of entities, including everyday commodities like household appliances and wearable devices, as well as industrial apparatus and urban infrastructure. These intelligent devices are endowed with sensors, software, and network connectivity, enabling them to capture, exchange, and real-time data analysis. This data serves as a catalyst for bolstering decision-making processes, automating operations, and optimizing efficiency across a multitude of sectors, spanning from healthcare and agriculture to transportation and smart urban ecosystems. IoT's salient capability resides in its capacity to seamlessly bridge the chasm between the physical and digital realms, thereby engendering a milieu ripe with innovation and transformative potential for our modus vivendi, professional endeavors, and environmental interactions. The devices connected via IoT are operating in a generic mode or under a Standard Operational Protocol (SOP), thus making way to have a dedicated channel stream for medical devices.

IoT-enabled medical devices communicate data to servers and data analyzers to facilitate visualization and decision-making processes. However, this continuous data transmission poses security challenges, as these devices often operate within a standard operational framework. To address these issues, there is a need to regard IoT medical devices as a distinct spectrum with well-defined and customized protocols for their operations, thus giving rise to the concept of the Internet of Medical Things (IoMT). The Internet of Medical Things (IoMT) represents a burgeoning and revolutionary technological framework that has wrought profound changes within the healthcare and medical services domain. IoMT is founded upon the intricate interlinking of a diverse spectrum of medical apparatus, sensors, and equipment, all meticulously crafted to execute the collection, transmission, and real-time analysis of health-centric data. This intricate network encompasses a wide-ranging assortment of devices, spanning from unobtrusive wearable health monitoring gadgets to sophisticated, data-intensive smart medical instruments, in addition to the very bedrock of healthcare infrastructure, encompassing hospital equipment, and far-reaching remote patient monitoring systems.

The IoMT ecosystem thrives on devices fortified with sophisticated sensor arrays, robust software architectures, and stringent security and communication protocols. These elements collectively empower IoMT devices to undertake the ceaseless surveillance of vital signs, the intricacies of chronic ailments, and an array of other pertinent health parameters. This treasure trove of real-time health data, derived from the network of IoMT

devices, becomes an invaluable resource that catalyzes substantial improvements in clinical decision-making processes. Furthermore, it serves to fine-tune patient care regimens, bolster treatment outcomes, and streamline the often-complex operational facets of healthcare services. The transformative potential of IoMT is manifest in its seamless integration of cutting-edge technology into the healthcare ecosystem. This synergy engenders an environment ripe for innovation and enhanced efficiency. Ultimately, IoMT's overarching goal is to uplift patient well-being by delivering superior medical services that are underpinned by data-driven insights and technological advancement, thus steering the future of healthcare towards a more connected and responsive paradigm.

In this research, we have proposed a novel and effective solution for securing authentication of IoMT devices under third party channels and servers. The demand of driving a dedicated protocol for IoMT is seen a massive rise in recent times, whereas the efforts to attempt the authentication solution is based on the influence of data and the data format, in this research we have considered the attributes as main theme for security enhancement. This improves the context of security by selecting random and customizable attributes for authentication. The proposed protocol shall server as a stepping stone to upcoming research in IoMT stream. The main contribution is to define the Interdependency Attribute Authentication (IAA) protocol on open public domain of servers for IoMT data streaming. The manuscript is organized under the standard format with introduction to the domain and theme setting in first section, followed by a brief summary of literature and critical reviews in section 2.0 with a proposed methodology and architecture in section 3.0. The problem statement is discussed in section 4.0, with supporting materials and methods in section 5.0. The manuscript is concluded by results and discussion in section 6.0 followed by conclusion in section 7.0.

2.0 LITERATURE REVIEWS

The Internet of Things (IoT) was primary defined to connect, control and coordinate devices across servers connected with a centralized unit of computation or storage. On this theme, researchers, scientist and industries have proposed and reported various enhancement and standards for IoT [1] [2] [3]. With the advancement of devices connectivity and the scope of data management, the Internet of Medical Things (IoMT) is proposed [4], the standards, operations and challenges are discussed. The authors of [5] have discussed on human centric perspectives for enhancing IoMT. The major research challenge in IoMT scope is the aspect of security. The survey [6] discussed on communication challenges and protocols used to manage and upgrade the IoT to IoMT. The survey spots on various attacks and threads related to IoMT communication in a given open environment and the characteristics for decision making. IoMT-SAF [7] is proposes an enhanced version on security by preserving the privacy of the patients. Under this study, a Security Assessment Framework (SAF) is developed to assure and extract the IoMT features. The process of feature engineering and attribute mining of IoMT data plays a vital role for larger computations with interdependency mapping. The feature extraction via augmented intelligence (AuI) is proposed by [8] with a defined resource recommendation framework for Telemedicine data generated on IoT devices in a smart cities environment.

Typically, the framework of smart health infrastructure is enhanced and represented with a modified format by [9] under a blockchain based operation of edge-IoT connectivity feature. These frameworks are governed and mapped under a single operation framework i.e. centralized server. The challenge in maintaining centralized command center is to restrict the security firewalls as multiple servers and devices are communicating in a given instance of time. The process is further complicated with heavy algorithms computing on server for decision making. The risk assessment and challenges are vital [10] and thus the study [10] [11] is subjected to discuss the potential representation of attacks and IoMT architecture standards and approaches for heterogeneous IoMT devices communication. The analysis is further brief with a requirement of dedicated protocol for operations and thus many studies [12] [13] [14] discusses on protocols and associated standards of IoMT operations. [14] The malware based analysis and customization of protocol is demonstrated under Denial of Service (DoS) attack. In this section, we have assured the critical surveys and reviews are discussed and represented from multiple prospective of research challenge. [15] The observation drawn in this survey is to understand the requirement of security protocol for upgrading the IoMT services under network layer.

3.0 METHODOLOGY

The proposed Interdependency Attribute Authentication (IAA) protocol is based on the objective to enhance the security prospective of IoMT devices operating in public domain. The proposed IAA protocol architecture is represented in Fig. 1. In the initial phase of IAA, the IoMT devices are customized into clusters (C1, C2, C3 ….) such that, the location and Internet Protocol (IP) of the devices are mapped to an individual clusters. The clusters

are connected to inference computation layer at the network layer of IoMT devices. The GSM/Connectivity unit (4G/5G/WiFi) are operated under the HTTP/RTSP operating standards. The communication protocols undertake the channel operations via third party service providers as per the regular operating standards such that, the existing infrastructure is adapting the changing frame-priorities. The remote monitoring unit or authentication unit on the server side (termed as listing pod) captures the data stream and process using MQTT protocol. The MQTT acts as an interfacing layer and accumulator for IoMT device request. The attributes from IoMT device request is processed and validated in customized protocol layer, i.e. Interdependency Attribute Authentication (IAA) protocol layer. The IAA protocol fetches the data stream from the database and synchronizes the network servers with updated configuration request. The detailed representation and flow of IAA is discussed in section 5.0, with a summarized representation of problem statement and research motivation requirement in section 4.0.

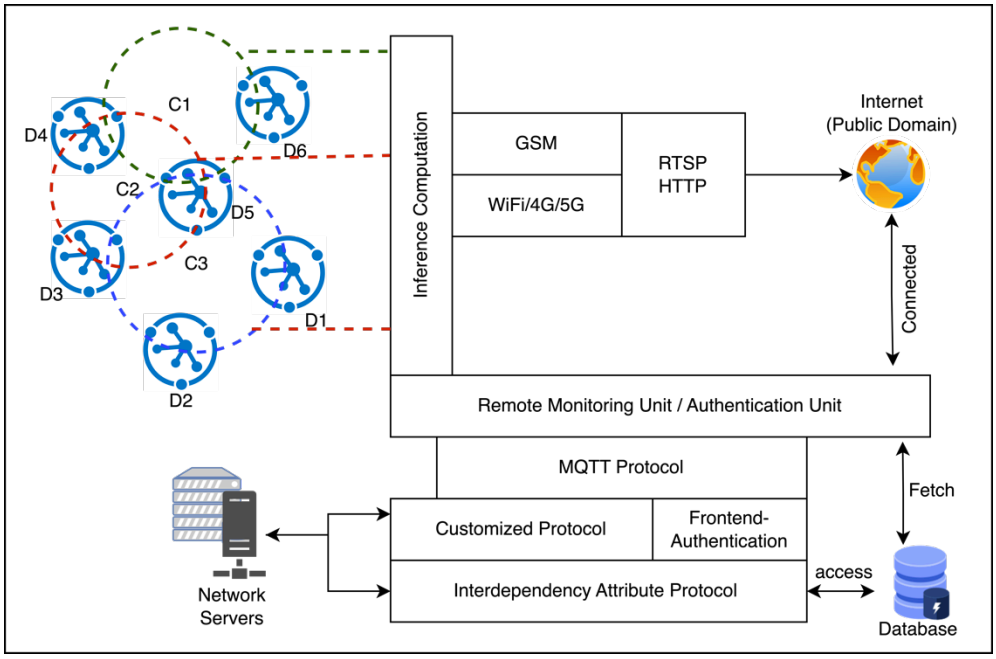

Fig. 1: Proposed Interdependency Attribute Authentication (IAA) protocol for IoMT authentication and security analysis

4.0 PROBLEM STATEMENT

In IoMT, the data connectivity and security is a major concern of operation. Since the data communicated via these IoT devices is medical data and hence classified as sensitive data format in the communication channel. Typically, under the normal operation standards, this is communicated via regular third party channels and optimized under normalizing standards. The major channel in the operation is controlled and coordinated by third party service providers and thus reflecting the data security aspects. The data under this channel is responsible for end to end communication whereas reflective indexing in open network causes breaching of third party data security. Consider the data (D) communicated via IoMT devices s (I_T) uch that $(\forall D \Rightarrow \sum I_T)$ at a given time (t) interval. Typically, if (D) is communicated via third party channel (O) as shown in Eq. 1 to cause security breaching.

$$D = \int_0^n \frac{\delta(D)}{\delta t} \oplus \left(\sum I_T\right) \xrightarrow{O} D^{|}(s) \tag{1}$$

Where, $D^{|}(s)$ is receives data at the receiver (R). Typically, the data transferred via open third party channel (O) is associated with security compromises (s). In this research article, the objective is to secure the data before the receiver stores the data. This proposed protocol is based on the incoming data attributes such as

request_ID, data-type, data-size, source, origin and hopping route to destination and much more via third party channels$^{(O)}$.

5.0 METHOD AND MATERIALS

The data transferred from the IoMT devices are fetched at the inference computing layer via device driven communication devices such as (4G/5G or WiFi) as per communication protocol. The communication is established via Real-Time Streaming Protocol (RTSP) and Hyper Text Transfer Protocol (HTTP) to connect the servers with the data streaming from IoMT devices via Internet. The proposed framework has chooses RTSP or HTTPs only for the device to internet communication as it provides reliable solution for end-user packet management. Further the system via internet (Public domain) is connected to the remote monitoring unit or authentication blocks before hitting request for communication at the server-end. Typically, the connectivity is resultant of information authentication and request validation. In general, the authentication is integrated with the communication channel for ease in connectivity and operations.

The authentication layer is supported by Message Queuing Telemetry Transport (MQTT) protocol for data transfer via publisher-subscriber model. The role of MQTT protocol is to retain the messages quality preserved from requesting IoMT devices. Further expanded and evaluated for customized protocol supported with proposed "Interdependency Attribute Authentication Protocol (IAAP). These protocols are detailed in upcoming sections. The IAP is coordinated with server storage systems or databases and network server's infrastructure for operations.

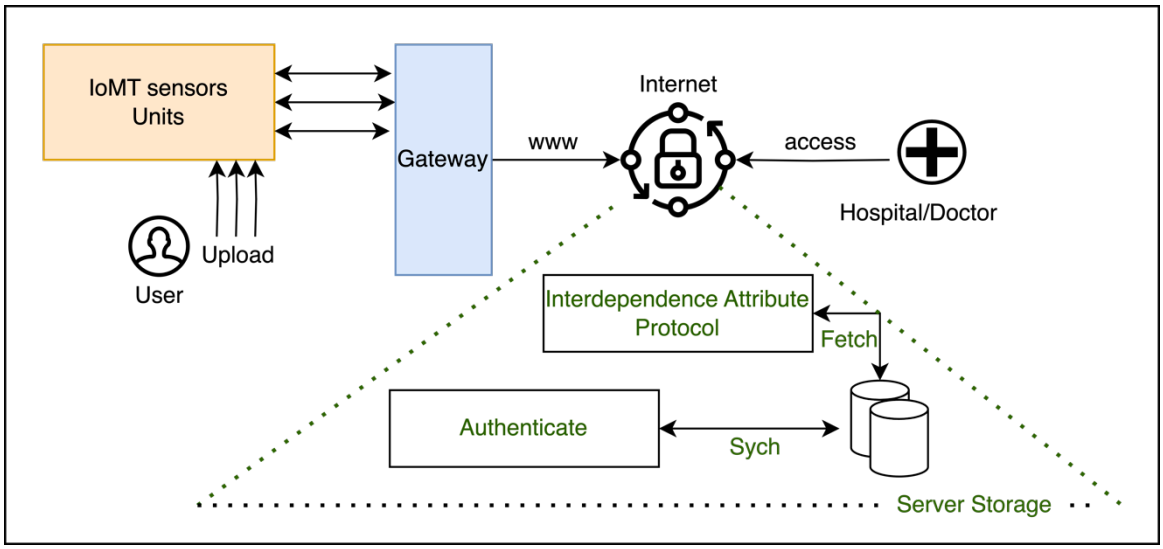

Fig. 2: Architectural representation on proposed IAA protocol communication stack via IoMT channel

In general, the defined IAP is dependent on generic information transfer and hoping/spoofing attacker's identification with the MQTT protocol for transmitting request. The detailed architecture is represented in Fig. 2 for authentication and data accessing scenario, where a medical expert (doctor) accesses the information via defined AAPI approach in public domain (Internet) to MQTT protocol. Thus the proposed request is validated via proposed IAP for authentication and access permission management. The outcome of this protocol is to shift the regular validating process of IoMT devices from device-end to server-end via IAP and machine learning models.

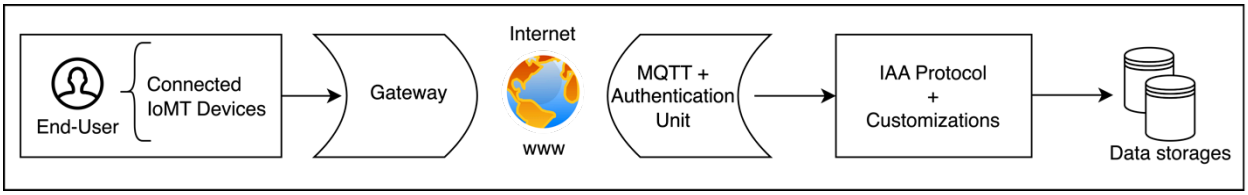

Fig. 3: Control flow diagram of user-data upload to server via IAA + Customization protocol

5.1 IoMT: Request generator and data uploading unit

Consider the scenario of data uploading into servers (public domain) via IoMT devices, the IoMT devices are $\left(I_T\right)$ and summarizes as $\left(\sum I_T\right)$ for computational requirements. The end-users $\left(U_i\right)$ at a given time (t) accesses the data stream from $\left(I_T\right)$ for transmission/storage, then the input requirement of each server data is driven via gateway (third party services) providers. Typically the connection can be defined as shown in Eq. 2.

$$\left(Conn\right)_t = \int_0^{\infty}\left(\sum\left(I_T\right)\oplus O_T\right)\times\partial t \tag{2}$$

Where, $\left(O_T\right)$ is the third party service provider carrying the input signals from IoMT devices via $\left(O_T\right)$ channel. The orientation further aligns with authentication and block value attribute extraction from incoming request via front-end authentication system as shown in Eq. 3.

$$\left(Conn\right)_t = Authn\left\{\frac{\phi\left(\sum I_T\right)}{\Delta \mathrm{T}}\oplus\left(O_T\right)_{Channel}\right\} \tag{3}$$

$$\therefore\left(Conn\right)_t = Authn\left\{\frac{\phi\left(\sum I_T\right)\oplus\left(O_T\right)_{Channel}}{\Delta \mathrm{T}}\right\}\times\partial t \tag{4}$$

Thus according to Eq. 4, the propagating channels request $\left(O_T\right)_{Channel}$ is aligned and coordinated with $\left(\sum I_T\right)$ devices in operation requirements. Typically, this includes a series of authentication pinging from one IoMT device to another such that, $\forall\left(I_{T1}\oplus I_{T2}\oplus I_{T3}\oplus....\right)\Rightarrow\sum I_T$ at a given interval of time (t), such that if $\left(I_{T1}\exists I_{T2}\Rightarrow\sum\left(O_T\right)_{Channel}\right)$ and $\left(I_{Ti}\neq null\right)$ then the computational value of IoMT devices is associated as shown in Eq. 5.

$$\therefore\left(Conn\right)_t = \forall\left[\left(\frac{\left\{I_{Ti}\oplus I_{Tj}\right\}\oplus\left(O_T\right)_{Channel}}{\delta t}\right)\times\lim_{n\to\infty}\left(\left(O_T\right)_{Channel}\neq 0\right)\right]_{(i,j)}^{n} \tag{5}$$

$$\therefore\left(Conn\right)_t = \lim_{n\to\infty}\left(\prod_{i}^{n}\prod_{j=i+1}^{n+1}\left\{\frac{\delta\left(I_{Ti}\oplus I_{Tj}\right)}{\delta t}\right\}\oplus\left\{\sum_{k}^{n}\left(O_T\right)_{Channel}\right\}\right) \tag{6}$$

$$\therefore\left(Conn\right)_t = \lim_{n\to\infty}\left(\prod_{i,j}^{n+1}\left\{\frac{\delta\left(\sum_{k}\left(I_T\right)_{k(i,j)}\right)}{\delta t}\right\}\oplus\left\{\sum_{k}^{n}\left(O_T\right)_{Channel}\right\}\right) \tag{7}$$

Thus, the operational values of each device and its incoming connection are validated via third party channel $\left(O_T\right)_{Channel}$ service providers with correlation to IoMT $\left(I_T\right)_{k(i,j)}$ devices associated in the transmission. This implementation scenario is validated with dual authentication approach and customization. According to Eq. 6 and Eq. 7, the customization of devices under $\left(O_T\right)_{Channel}$ is flexible compared to the time (t) of service request. Thus the authentication of connection of devices $\left(I_k\right)$ under $\left[Authn\left(I_k\right)\right]$ is shown in Eq. 8.

$$Authn\left(I_k\right) = \Delta T\oplus\delta\left(Conn\right)_t\Big]_0^n \tag{8}$$

The authentication provides by individual connection is associated with incoming request format of multi-operational devices $\left(I_k\right)$ connected to the gateway and requesting servers at a given point of time. Typically, from the proposed system, the orientation of connection from user via IoMT devices authentication is explained in this proposed section.

5.2 IoMT Customization of protocol and authentication routing

On receiving the authentication acknowledgement as defined by Eq. 8, the process of customization protocol id initiated to assure the supporting operations of data access and transmission. The transmission stream is evaluated and operated as the functional entity of routing secure transmission, for instance when $(Conn)_t$ is established, the secure authentication as per Eq. 8 generate an authentication request for processing the access of data/storage server. The process of routing (R) is defined in Eq. 9

$$R = (\Delta T)_{Conn(t)} \oplus \left\{ \lim_{n\to\infty} \left(\frac{R_t (Conn)_t \to \arg\min(R_t)}{\Delta T} \right) \right\} \tag{9}$$

Where, (R) is the routing protocol of $(Conn)_t$ at a defined outreach with routing recommendations (R_t) is defined, such that $\forall (R_t) \Rightarrow \Delta \mathrm{T}$ (i.e.) $(\Delta \mathrm{T})$ is the minimal time of operation and sustainability of regular routing and information customization. Generally, the value of routing is defined with minimal time required for revoking and validating the user needs. The time to reach the accessing server is bound with operational round-trip-time (RTT) and with Time to Live (TTL) for termination of $(Conn)_t$ at time beyond secure channel.
In general the operations manager (default user) attains the customization of information with RTT and TTL associated to $(Conn)_t$ at given time interval. The manager also tracks and validates the out coming request queries on data accessing and customization for resultant analysis in validating the type of data processed, computed and accessed in the given $(Conn)_t$ connection window. The ratio of security assurance is dependent on $(\Delta \mathrm{T})$, the minimum operation time associated with connection window $(Conn)_t$ in Eq. 10.

$$(Conn)_{Window} \Rightarrow \left\{ \int_0^n \sum_{i=1}^{n} \left(\frac{\delta \left[(Conn)_t \right]}{\delta t} \right) \cong \left(\frac{\Delta RTT \oplus \Delta TTL}{\Delta \mathrm{T}} \right) \right\} \tag{10}$$

$$\therefore (Conn)_{Window} \Rightarrow \left\{ \left(\frac{\delta \left[\sum (Conn)_t \right]}{\delta t} \right) \bigcap \left(\frac{\Delta RTT \oplus \Delta TTL}{\Delta \mathrm{T}} \right) \right\} \tag{11}$$

Thus, the simplified representation of Eq. 11 is subjected to the availability of (ΔRTT) and (ΔTTL) in the process of deciding connection window's activation time, as if the window is open under the secure mode of operations and customization. Thus from the proposed experimental setup, the customization protocol is developed to retain valuable information secure by analyzing the time to evaluate.

5.3 Experimental setup and Implemntation

The proposed interdependency attributes authentication (IAA) protocol is developed with an objective to build a reliable solution for IoMT data optimization and formulation of security gateway in accessing sensitive medical information/data processed in IoMT devices and streamlined in cloud servers. The experimentation setup at IoMT devices includes a pulse monitoring sensor, heartbeat monitoring sensor, and blood sugar level monitoring sensors. All these connected to a dedicated AWS-bound service cloud using an API (Firebase) to communicate data streams. The AWS-classes servers are developed with MiniQube ADM containers for services such as listing active pods, validating request pod, action pod and protocol design pod for streamlining the services. In specific, the system has considered real-time data generated from IoMT devices and coordinated for computing under an optimized server connectivity using RSTP/HTTPs request-responding protocol for data propagation and connection request management.

6.0 RESULTS AND DISCUSSION

The proposed IAA Protocol has been successfully developed and validated on a streaming platform of real-time data processing and analysis. The protocol has included trivial mode of communication such as RTSP/HTTPs in data connection establishment and MQTT for data navigation towards server. The validating process is further streamed with multiple IoMT devices connected in series at a given active server time for communication. The outcome of this protocol is to fetch higher and improved security ratio by resultant improvisation of data channel in IOMT devices.

The channel computing and processing is relatively improved with outgoing customization protocol by significant values. The data stream propagating in the channel for active connection can be dependent on $(Conn)_t$ and IoMT devices (I_K) connected to the system in a given point of time. The relativity analysis on time computation in IoMT devices to server services time is shown in Table. 1

Table 1: Computation of TTL and RTT on various setup of communication protocol

Protocol arrangement	TTL (ms)	RTT (ms)	Packet loss (frames)	Hit-avg-time (ms)
Localhost	0.68	1.72	0.072	0.58
HTTP	0.74	1.96	0.081	0.72
HTTPs (Plugin API)	0.83	2.72	0.123	0.93
RTSP	0.73	0.42	0.009	0.43
IIA (Proposed)	0.84	1.98	0.017	0.64

Table 2: Performance estimation on connection window and TTL/RTT operations

Datasize (MB)	Connection window (ms)	RTT (ms)	TTL (ms)	Actual $(Conn)_t$ (ms)	Proposed $(Conn)_t$ (ms)
0.25	4.73	1.61	0.68	3.42	3.72
0.5	4.88	1.67	0.66	3.48	3.64
0.75	4.88	1.66	0.72	4.72	3.18
1.00	5.61	1.67	0.78	3.59	3.04
1.25	5.72	1.67	0.75	3.88	3.42
1.5	5.73	1.68	0.76	4.16	3.47
1.75	5.73	1.67	0.76	4.62	3.47
2.00	5.73	1.67	0.76	4.64	3.48

According to performance estimation in Table 2, the value of information range is incremented with 0.25MB of data with each interval of experiment to compute (ΔTTL) and (ΔRTT) resulting in computing the actual and proposed (IAA protocol) approach of data processing. According to Table 2, the resultant of proposed time computation via IAA protocol has increased the datasize and stabilized accordingly. The observation drawn from IAA protocol is relatively higher and saturated compared to the actual time. The saturation point at 1.25MB is attained with incremental value up to 2MB accordingly. The overall performance computation of proposed IAA protocol is demonstrated in Table 3.

Table 3: Performance matrix and observations

Protocol	Fragmented time (ms)	Connection Window (ms)	Accuracy (%)
HTTP	0.042	3.72	86.72
RTSP	0.017	3.11	88.11
IAA+HTTP	0.088	3.96	89.92
IAA+RTSP	0.071	3.04	91.66
$(IAA)_{Collective}$	0.049	2.78	90.72

Thus according to Table 3, the computational accuracy of proposed (IAA) is relatively higher in providing security for the data compared to HTTP and RTSP in a standalone mode. Hence the observation is proposed with 90.72% accuracy in retaining the data attributes loses compared to the generalized representation.

7.0 CONCLUSION

The proposed interdependency Attribute Authentication (IAA) protocol has been developed with an objective to improvise and analyze the security aspects of IoMT data devices communication. The technique includes an attribute validation and analysis approach for streaming the input request authentication and further justifies the relatively of request nature by classifying the connection request into a relatable or sub-relatable based attribute data extracted. The IAA protocol id first of its kind to discuss on RTT and TTL based connection authentication and security mapping. Typically, the processed IoMT data over a dedicated IAA protocol server has demonstrated higher reliability in computation with 90.72% accuracy of data extraction in generalized mode and with 91.66% accuracy in IAA+RTSP based connection request mode. In near future, IAA protocol can be expanded with File Transfer Protocol (FTP) request with Electronic Health Records (EHR) data operations in IoMT services.

REFERENCES

[1] K. K. Vaigandla, R. K. Karne, and A. S. Rao, "A Study on IoT Technologies, Standards and Protocols", *IBMRD's Journal of Management & Research,* Vol. 10 No. 2, 2021, pp. 7-14.

[2] I. Ishaq, D. Carels, G. K. Teklemariam, J. Hoebeke, F. Van den Abeele, E. De Poorter, ... , and P. Demeester, "IETF Standardization in the Field of the Internet of Things (IoT): A Survey", *Journal of Sensor and Actuator Networks*, Vol. 2 No. 2, 2013, pp. 235-287.

[3] K. Naito, "A Survey on the Internet-of-Things: Standards, Challenges and Future Prospects", *Journal of information processing*, Vol. *25*, 2017, pp. 23-31.

[4] S. Razdan, and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies", *IETE technical review*, Vol. *39* No. 4, 2022, pp. 775-788.

[5] C. Kotronis, I. Routis, E. Politi, M. Nikolaidou, G. Dimitrakopoulos, D. Anagnostopoulos, ... ,and H. Djelouat, "Evaluating Internet of Medical Things (IoMT)-Based Systems from a Human-Centric Perspective", *Internet of Things*, Vol. *8*, 2019, pp. 100125.

[6] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D.Glynos, and C. Douligeris. "Security in IoMT Communications: A Survey". *Sensors*, Vol. *20* No. 17, 2020, pp. 4828.

[7] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, . "IoMT-SAF: Internet of Medical Things Security Assessment Framework". *Internet of Things*, Vol. *8*, 2019, pp. 100123.

[8] S. T. Ahmed, V. Kumar, and J. Kim, "AITel: eHealth Augmented-Intelligence-Based Telemedicine Resource Recommendation Framework for IoT Devices in Smart Cities", *IEEE Internet of Things Journal,* Vol. 10 No. 21, 2023, pp. 18461-18468.

[9] N. K Al-Shammari, T. H. Syed, and M. B. Syed. "An Edge–IoT Framework and Prototype based on Blockchain for Smart Healthcare Applications", *Engineering,Technology & Applied Science Research*, Vol. *11* No. 4, 2021, pp. 7326-7331.

[10] B. Shanmugam, and S. Azam. "Risk Assessment of Heterogeneous IoMT Devices: A Review", *Technologies*, Vol. *11* No. 1, 2023, pp. 31.

[11] I. Ahmed, E. Balestrieri, and F. Lamonaca. "IoMT-based biomedical measurement systems for healthcare monitoring: a review", *ACTA IMEKO*, Vol. *10* No. 2, 2021, pp. 174-184.

[12] A. B. Chaaben. "A Survey of Different IoMT Protocols for Healthcare Applications", *ResearchBerg Review of Science and Technology*, Vol. *2* No. 1, 2022, pp. 41-57.

[13] N. Askar, A. Habbal, A.H Mohammed, M.S Sajat, Z. Yusupov and D. Kodirov. "Architecture, Protocols, and Applications of the Internet of Medical Things (IoMT)", *Journal of Communication*, Vol. *17* No. 11, 2022, pp. 900-918.

[14] M. Wazid, A. K. Das, J. J. Rodrigues, S. Shetty, and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges", *IEEE access*, Vol. 7, 2019, pp. 182459-182476.

[15] B. A. Mubdir, and H. M. A. Bayram, "Adopting MQTT for a multi protocols IoMT system", *International Journal of Electrical and Computer Enginerring,* Vol. 12 No. 1, 2022, pp. 834-844.

[16] Kumar, S. Sreedhar, et al. "Unstructured Oncological Image Cluster Identification Using Improved Unsupervised Clustering Techniques." *Computers, Materials & Continua*, Vol. 72, No. 1, 2022.