Secure and Energy-Efficient Smart Building Architecture with Emerging Technology IoT

Arun Kumar

Panipat Institute of Engineering and Technology, Haryana-132102, India

Sharad Sharma

Maharishi Markandeshwar (Deemed to be University), Haryana-133207, India

Nitin Goyal*

Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

Aman Singh*

Department of Computer Science and Engineering, Lovely Professional University, Punjab-144411, India

Xiaochun Cheng

Department of Computer Science, Middlesex University, London NW4 4BT, United Kingdom

Parminder Singh

Department of Computer Science and Engineering, Lovely Professional University, Punjab-144411, India

Abstract

With the advent of the Internet-of-Things (IoT), it is considered to be one of the latest innovations that offer interesting opportunities for different vertical industries. One of the most relevant IoT technology areas is smart construction. IoT operates in several sectors on a daily basis; implementation includes smart building, smart grids, smart cities, smart houses, physical defense, e-health, asset, and transportation management, but it is not restricted to this. Support

*Corresponding author

Email addresses: dr.nitingoyal30@gmail.com (Nitin Goyal), amansingh.x@gmail.com (Aman Singh)

from smart IoT buildings is an IoT-level, connected, and cost-effective system. Commercial space has major requirements in terms of comfort, accessibility, security, and energy management. Such requirements can be served organically by IoT-based systems. As the supply of energy has been exhausted and energy demand has risen, there has been a growing focus on energy usage and the maintenance of buildings.With the use of evolving IoT technology, we present a secure and energy-efficient smart building architecture.Every device is known by its unique address, and one of the key web transfer protocols is the Constrained Application Protocol (CoAP). It's an application layer protocol that doesn't use protected channels for data transfer. Automatic key management, confidentiality, authentication, and data integrity are all features of the Datagram Transport Layer Protection (DTLS).To achieve energy efficiency, we propose a smart construction architecture that, through IoT, manages the performance of all technological systems. The results of the simulation show that the energy consumption is lowered by about 30.86% with the use of the CoAP in the smart building, which is less than the Message Queuing Telemetry Transport case (MQTT). This paper also aims to observe how to integrate the DTLS protocol with the Secure Hash Algorithm (SHA-256) using optimizations from the Certificate Authority (CA) to improve security.

Keywords: Smart Infrastructure, Big Data Analytics, Internet of Things, Smart Building, Certificate Authority

1. Introduction

The increasing interest in intelligent buildings, as well as the pace of innovation in this field, has triggered several research to implement various types of applications such as energy management, build management simplification, resident comfort improvement, reactive alarm management, personal security, asset protection, intruder event management, and so on. The increase in security vulnerabilities as a result of interactions between cyber and physical entities has shifted the focus of this research [1]. The availability of IoTs in commercial

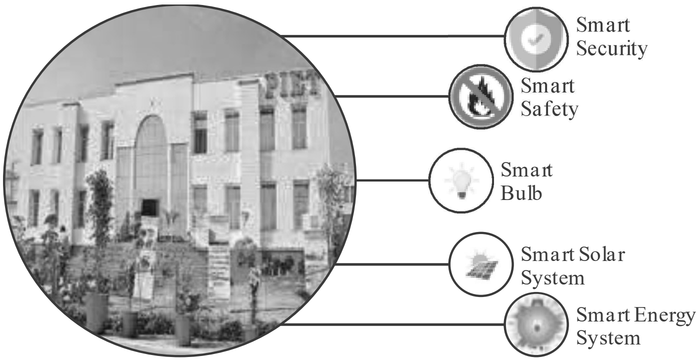


Figure 1: IoT-based smart building

buildings enables building occupants and climate to be tracked in real-time. Thus, we can access occupancy numbers in real-time and also identify several people holding a wireless gadget in different regions of the house [2]. The savvy building frameworks of things to come will, for instance, alter its vitality use by cleverly controlling the Heating, Ventilation, and Air Conditioning (HVAC) and react rapidly to potential issues that could push the structure of its course towards carbon neutrality [3]. Big Data (BD) is another idea that clarifies the gigantic volume of information that all these interconnected frameworks produce. The related advances of IoT and BD can likewise be spoken to and ought to be manufactured together [4]. Information communicated is controlled and breaks down in the cloud world. This most recent innovation for Cloud Computing (CC) or simply cloud gives improved capacity, cost-viability, adaptability, accessibility, effectiveness, toughness, and dependability [5]. Furthermore, thanks to BD technology for better user expert automation, vast data generated by connected devices and sensors can also be made into operable insights and predictions [6]. Many IoT systems and platforms are now being developed to design and deploy IoT applications (see Figure 1.

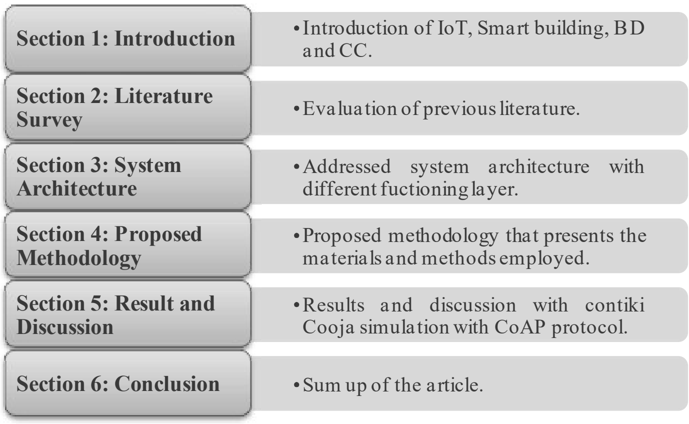
The remarkable recent developments in IoT with BD technology have provided the opportunity to broadly deploy tiny sensors for wireless communication for various applications like smart buildings, smart cities, smart healthcare, and the smart industry. In light of the increasing number of projects and innovations addressing this issue, the need for systematic characterization of energy use in buildings has gained attention. Since buildings with different functionalities have different energy use profiles, and initial characterization of the major contributors to their energy use is needed. For example, energy consumption in residential buildings is primarily due to the indoor services given to their occupants (associated with comfort), while energy consumption in industrial buildings is primarily due to the operation of industrial machinery and infrastructures dedicated to production processes. In this context, the integration and advancement of systems focused on Information and Communication Technologies (ICT) and, more precisely, IoT are vital enablers of a wide variety of applications for both industries and the general public, assisting in the realisation of smart buildings [7]. IoT enables smart things to communicate with each other as well as the efficient incorporation of real-world data and knowledge into the digital world. Smart devices with sensing and interaction capabilities, as well as recognition technologies, make it possible to collect far more knowledge about the real world than ever before.

MQTT and CoAP are two of the most promising protocols for small devices. MQTT and CoAP are both open standards that work better in constrained environments than HTTP. Both provide asynchronous communication mechanisms. IP-based and with a variety of implementations MQTT allows for a variety of communication patterns and functions solely as a binary data pipe. CoAP was created with web interoperability in mind. CoAP is being scrutinized in terms of protection because there are many problems and debates. Even though it is a modern protocol, it must be compressed and run at low power. The most difficult challenge is to maintain high performance while maintaining security and providing defence [8]. To clarify, DTLS is the official and custom application layer security protocol that can be used to provide security in CoAP, but it comes with its own set of limitations and problems, including broad message and handshake compression, and the fact that DTLS is incompatible with the CoAP proxy mode. According to a review, there is a problem with end-to-end communication because, in certain cases, an HTTP client needs to access resources from a CoAP server.

Finally, data transmission security between IoT devices refers to the prevention of unauthorised access to the IoT network. To counter these dangers, architectures have been developed [9]. As a result, a technical architecture is proposed to address those risks, namely a design that ensures scalability, application compatibility, and data transfer protection. To accomplish this, three-layer technical architectures were studied, a design was developed, and it was validated through expert judgment. In this paper, the integration of the CoAP protocol with IoT is used to minimize the power consumption of IoT devices with DTLS security. The motivation behind this contribution is that in critical situations, IoT devices can effectively provide less power consumption, deliver highly secure information, and low-cost solutions to the IoT network for smart building.This paper's contribution can be summarized as follows:

1. Discussing recent papers exploring the convergence of smart building with numerous IoT applications.
2. Investigating IoT issues in smart building and how they can be overcome by IoT incorporation.
3. Proposes DTLS protocol with SHA-256 using optimizations from the CA to improve security.
4. Non-continuous awake state of the CoAP protocol help in energy reduction in comparison to other existing schemes.

The rest of the paper is organized as follows: In Section 2, the Literature Survey is addressed in which other researchers use related proposed systems. Section 3 discussed system architecture. Section 4 discussed the Proposed Methodology. In section 5, we discussed results and discussion with Contiki Cooja simulation with CoAP protocol. The paper is eventually summarized in Section 6 and the complete workflow is shown in Figure 2.



Section 1: Introduction	• Introduction of IoT, Smart building, BD and CC.
Section 2: Literature Survey	• Evaluation of previous literature.
Section 3: System Architecture	• Addressed system architecture with different fuctioning layer.
Section 4: Proposed Methodology	• Proposed methodology that presents the materials and methods employed.
Section 5: Result and Discussion	• Results and discussion with contiki Cooja simulation with CoAP protocol.
Section 6: Conclusion	• Sum up of the article.

Figure 2: The Outline of the Paper.

2. Literature Survey

We are reviewing and evaluating previous studies on smart infrastructure and advanced sensing. The records that contributed altogether to our examination are given in the accompanying parts. Robotization frameworks are analyzed alongside analysis of a completely IoT-viable, controllable, data working in an objective and predictable methodology [10]. The arrangement for an interoperable smart structure design to make an inventive structure the board frameworks by incorporating the benefits of created computerization advancements and developments is being tended on a progressing basis. A comprehensive organization called city explorer, which offers assurance and disclosure is the bit where the recommended structure is epitomized [11]. A Graphical User Interface (GUI) that is Three-Dimensional (3D) is utilized in the arranged test system to control human action in smart homes [12]. This 3D-GUI displays dynamic and spatial sensors that behave like real sensors. Furthermore, a falsely amazing operator is given by the test system to collaborate with shrewd homes. For this, a technique for getting ready for activities is utilized. IoT-based detecting and global positioning framework that is remotely associated with taking estimations of a structure's temperature, moistness, and light. Besides, an Android framework is being created from which information is communicated to a savvy versatile interface that tracks information distantly from the Laboratory Virtual Instrument Engineering Workbench (LabVIEW), an entry and advancement condition [13, 14]. Smart buildings and smart clients are, specifically, these things. Resident information and building information gathered from savvy cell phones and sensors can be overseen and examined to make them more productive in urban communities [15].

The Localization Novel Method (LNM), a tool for recognizing walkers, creates a unique mark chronicle by utilizing the sign quality obtained by the neighbor.It also serves as the foundation for a Markov model that predicts the movement of people on foot. Furthermore, further examination of the startling sign deviation is completed utilizing the specific situation [16]. The outcomes are remarkable since, after tests, the proposed strategy is by all accounts superior to a few. However,there are consistency concerns and fluctuations in the Wireless Fidelity (Wi-Fi)signal. Specifically, the proposed framework relies upon a wearable interface that incorporates picture acknowledgment and confinement abilities, so social data identified with the works of art being watched can be consequently conveyed to clients. A design incorporates the Cloud to store interactive media content made by clients and to share occasions produced by the framework on the client's informal organization [17, 18]. An efficient rule engine for smart building systems to tackle the issues of smart structure. All the more explicitly, an extraction module for nuclear occasions is inherent to eliminate nuclear occasions from messages and afterward develop a β-organization to get nuclear conditions to parse nuclear occasions [19]. The science fiction prototyping (SFP) situation that recommends a morphogenetic plan technique for smart structures zeroed in on the advancement of drosophila melanogaster and zeroed in on contemporary innovations, computerized production, and parametric engineering of Building Information Modelling (BIM). To complete, it is prescribed to focus on an audit of the implications for the planning group for a BIM morphogenetic engineering system. Artificial Intelligent (AI) design and organization of the AI-Based Smart Building Automation Controller (AIB-

SBAC) can be insight fully receptive to shopper needs, zeroing in on better client convenience, security, and vitality proficiency.

Moreover, the plan design of AIBSBAC considers the fast establishment of adaptable attachment and play advances without a snag to establishment framework enhancements for mostapplications, including private and building computerization. Developed an IoT-based learning framework that offers a practical approach to creating detailed thermal models for future temperature controls in smart buildings. The existing state-of-the-art activities are needed for the smart growth of enhanced smart technology, parameter management, and IoT infrastructure. The principal centre is around detecting and keeping up the IoT foundation, which empowers cloud customers to utilize a virtual detecting structure utilizing correspondence conventions [20, 21, 22].

Current cutting-edge exercises necessitate astute structure with enhanced programming innovation, boundary the executives, and IoT foundation.The primary spotlight is on detecting and keeping up the IoT framework, which encourages cloud clients to utilize a PC detecting framework utilizing organizing conventions. Most of the conclusions were drawn during the SmartSantander project, aEuropean (EU) project creating a city-scale IoT and Potential Internet experimentation testbed, which offers an interactive structure for the introduction of Smart City services [23, 24]. A smart building template that, by IoT technology, regulates the performance of all physical systems to achieve energy efficiency. A new matrix called the "Laplacian IoT matrix" offers knowledge connected to a smart building graph on the IoT network. The suggestion is followed by the results of a qualitative case study. The IoT paradigm helps us to explain and use examples that are fundamental IoT principles applied to smart homes and simple use cases incorporated in a condensed Smart Home context that opens the door to potential customers' imagination. Advanced IoT architecture for monitoring continuous and real-time development. The projected result is based on a sensor node located inside the building being controlled, connected to the Internet, able to measure continuously, and send raw data to the remote server in real-time through the MQTT protocol [25, 26, 27, 28].

Table 1: Related Work Comparison

Author (s)	**Focus**	**Protocol**	**Efficiency**	**Surveillance Environment**	**Security**	**Transmission Speed**	**Quality of Service**
Alletto et al. [17]	Designed and tried an indoor area engineering that can improve client involvement with an exhibition hall.	BTLE		Indoor		X	X
Kaur et al. [18]	The proposed design incorporates with the Cloud to store interactive media content made by clients and to share occasions produced by the framework on the clients ’ informal organization.	PaaS & IaaS	X	Indoor / Outdoor			X
Sun et al. [19]	Discussed an inventive principal motor to tackle the issues of the Smart Building plan.	ZigBee	X	Indoor / Outdoor	X		
McGinley et al. [29]	Presented a science fiction prototyping (SFP) situation that recommends a morphogenetic plan technique for smart structures	SFP	X	Indoor			
Basnayake et al. [20]	Provided clarifications of the Artificial Intelligent (AI) design and organization of the AI-based smart building automation controller (AIBSBAC)	AIBSBAC		Indoor / Outdoor		X	X
Zhang et al. [21]	Developed an IoT-based learning framework that offers a practical approach to creating detailed thermal models for future temperature controls in smart buildings	Bluetooth		Indoor		X	
Verma et al. [22]	Discussed the existing state-of-the-art activities needed for the smart development of enhanced smart technology, parameter management, and IoT infrastructure.	Wi-Fi		Indoor / Outdoor			

Table 1 Continued: Related Work Comparison

Le et al. [23]	Introduced the current cutting-edgeexercises required for shrewd structure with improved programming innovation, boundary the executives, and IoT foundation.	Z-WAVE	X	Indoor / Outdoor	X		X
Evangelos Theodoridis et al. [24]	Discussed the main results, technical challenges, and socio-economic benefits in the smart city age.	SFP		Indoor		X	
Metalloid et al. [25]	Proposed a smart building template that, by IoT technology, regulates the performance of all physical systems to achieve energy efficiency.	LTE	X	Indoor / Outdoor			
Casado-Vara et al. [26]	Discussed new matrix called the "Laplacian IoT matrix" was developed which provides information on the IoT network linked to a smart building graph.	Wi-Fi		Indoor / Outdoor			X
Debauche et al. [27]	A framework was introduced that allows us to understand and use examples that are fundamental concepts of IoT applied to smart homes.	Bluetooth	X	Indoor			
Pierleoni et al. [28]	Introduced the IoT architecture for continuous and real-time building control	MQTT	X	Indoor			
Our Proposed Work	Secure and Energy-Efficient Smart Building Architecture with the Use of Emerging Technology IoT	CoAP	X	Indoor / Outdoor	X	X	X

As shown in Table 1 summarizes the related work with the following parameters like efficiency, surveillance of environmental,security transmission,speed, and quality of service (QoS). All the above solutions are planned with specific features in focus. Thus, this paper addresses the protocol known as CoAP protocol for the smart building,which will be best in security, quality of service, and transmission speed.

3. Proposed System Architecture

A smart building, whether it's an office, a home, an industrial plant, or a leisure area, provides occupants with personalised services thanks to the knowledge of its contained objects. Because the built environment has an impact on everyone's quality of life and work, buildings must be capable of not only reducing energy consumption but also improving habitability and productivity. Building sensor and actuator deployments must be optimised such that the related expense is covered by the economic benefit of energy savings. It should be noted that controlling the entire area of a large structure is neither feasible nor practical. Furthermore, real sensor data about such inputs should be considered in the final energy management framework, in addition to the activity patterns obtained after data monitoring. As a result, the device will adjust to changes in the building context as well as new conditions that were not included in the initial models. The architecture of this platform is divided into three layers that are generic enough to cover the needs of various smart environments, such as those addressed in the context of smart buildings.The three-layer structure of an IoT-based smart building is depicted in Figure 3.

Data Sensing or Perception Layer- The data from sensors is collected by the first layer. The data includes individual users' demands for appliance operation states such as temperature, humidity, and so on.This data is then stored in a dedicated BD cloud via a network gateway.

Data Processing or Network Layer- This layer organises the gathered information and then processes it. Individual users' data is required for comfort-related issues such as the HVAC system, lighting system, and temperature system.

Data Reproduction or Application Layer- Processed data is replicated as information about individual interactions between occupants and equipment in the third layer. Finally, the gathered data is used to improve device effectiveness and performance. As a result, it helps in delivering better services to the residents.

The development of vast volumes of data from Cloud Computing, Information Systems, and Emerging Technology over the past decade, with an increase in IoT device output and miniaturization. Such knowledge without analytical power, however, is not useful in any area. For the extraction of information and decision-making, concentration efforts at multiple levels are required, becoming "Big Data Analysis" an increasingly difficult field. Numerous analytical solutions incorporating BD and IoT have allowed useful information to be collected by people. BD sounds a lot like a big brotherof IoT and it could probably be interpreted that way in certain respects. The age of intelligence built into our buildings is upon us and millions upon millions of data points (IoT sensors) are generated by all that smart technology. A framework that comprises sensors that track temperature, movement, light, and humidity, to enhance building maintenance and make buildings' smart'and effective has been introduced. Furthermore, the consumer can understand if there was anyone in the house who might provide a "safe" meaning using the analysed measurements from the cloud service collected by the motion sensor. Furthermore, with a voltage stabilizer to prevent any complications, the mounted cloud server will work automatically. Both users can conveniently link to the network through their telephone services using the building's Wi-Fi connection.Intelligent

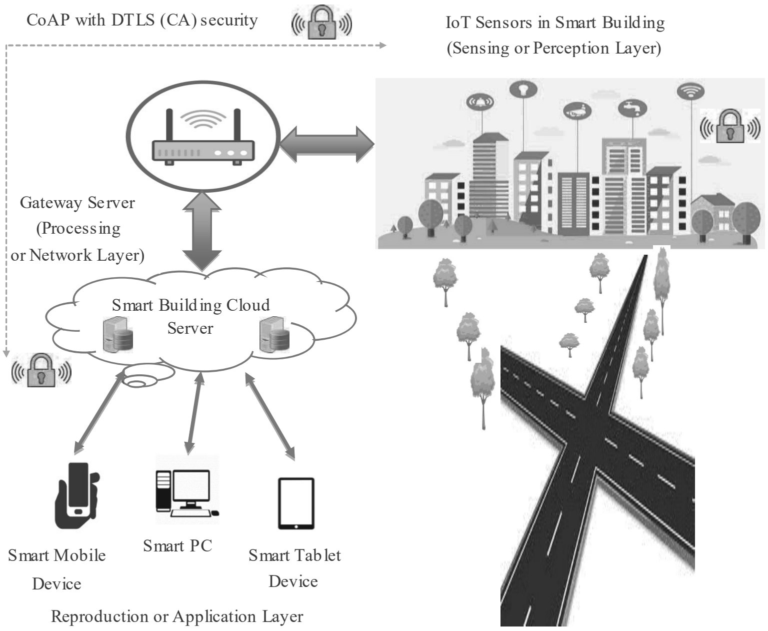

CoAP with DTLS (CA) security
IoT Sensors in Smart Building
(Sensing or Perception Layer)
Gateway Server
(Processing
or Network Layer)
Smart Building Cloud
Server
Smart Mobile
Device
Smart PC
Smart Tablet
Device
Reproduction or Application Layer

Figure 3: Proposed System Architecture.

devices allow people to create a safer building, e.g. cameras installed in the building to track the environment, from the phone or the device when necessary. Moreover, the surveillance cameras are connected to other intelligent devices to effectively monitor the building depending on occupancy. Residents will use their mobile or smart interfaces to communicate with the security system. The protection mechanism is available in communication with the building's lighting system, buzzers, alarms, the police station, etc. When an irregular movement or movement is observed or intruders are detected, the protection system responds. You can therefore see that this intelligent protection is much more reliable and competent than an emergency siren. Besides, the maintenance plan of the systems will also be provided to residents to ensure the effective and efficient operation of all devices.

Smart building systems were created to track the well-being of elderly people who live alone in their households. The built smart building system is capable of tracking an inhabitant's general physical activities as well as physiological and ambient entities at the same time. It's a multi-model, unobtrusive, non-invasive novel sensing device that's installed in strategic locations throughout the building. A single local gateway server device may provide continuous monitoring in a smart building. In a Windows software environment, the built analysis and decision-making algorithm software modules run.We can access wellness information from a remote location using an internet connection.The two wellness roles $\beta1$ and $\beta2$ describe an inhabitant's wellness based on how they use household appliances. The wellness functions aim to decide "how good" the inhabitant uses everyday objects. The first feature, $\beta1$, is derived from the appliances' non-usage as well as their inactive period. The second feature $\beta2$, on the other hand, is triggered by the improper use of a few particular appliances. The wellness index depicts a person's actions in relation to everyday object use in real-time.

$$\beta_1 = e^{\frac{-t}{T}} \tag{1}$$

Where T = Maximum inactive duration when no objects were used in the past, t = Time of Inactive duration of all appliances.

$$\beta_2 = e^{\frac{T_n - T_a}{T_n}} \tag{2}$$

Where T_n= maximum consumption time of a household object in the normal situation of the past, and T_a = current consumption time of the household object.

Thus, the following are some of the key benefits of our Smart Buildings architecture:

- Reduce energy usage,
- Boost building performance,
- Improve productivity,
- Make better use of capital with predictive maintenance.

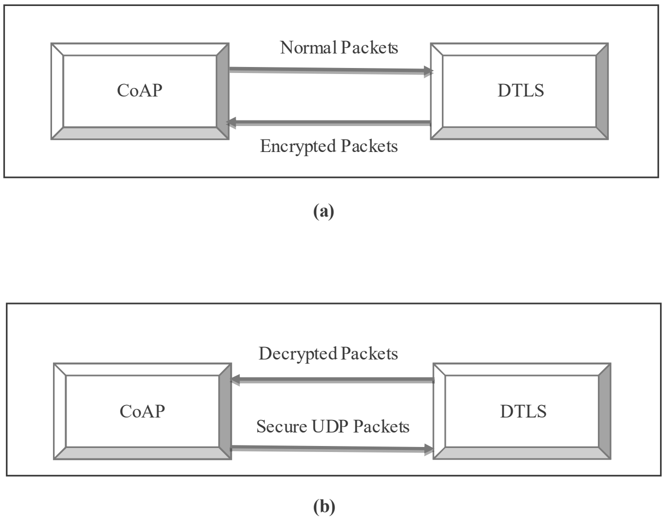


Figure 4: (a) Encryption of CoAP packets with help of DTLS, (b) DTLS decryption to CoAP

4. Proposed Methodology

Contiki is a low-power IoT operating system. Cooja is an emulator for the Contiki network. Cooja simulates Contiki's large and small networks. Contiki is a popular, freelance, and open-source IoT programming operating system with a C programming language base code, which is available under the Berkeley Software Distribution (BSD) license. Contiki is a networked, memory-constrained operating system aimed at low-power wireless Internet of Things users. Contiki can be used in wireless communications with high efficiency and protection amongst low-powered RFID chips. Contiki is programmed through the Cooja network simulator, in which RFID chips and sensors' basic libraries in C are available. The backendC programs and the associated header files can be configured and recompiled to deliver the necessary results to schedule, manage, and monitor remote IoT devices. Contiki operates with the introduction of lightweight protocols on Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks to link low power chips and radio frequency chips without performance problems [30, 31, 32, 33]. In CoAP, many resources are accommodated by a physical entity (i.e., thing) representing data obtained from sensors or activities accessible to actuators.

Figures 4(a) and 4(b) depict the general data flow interactions between DTLS and CoAP in both forward and reverse directions, respectively. CoAP packets are sent to the DTLS module in the forward direction to add protection features. This process has two interfaces: DTLS receives regular CoAP data packets and then sends encrypted data to CoAP. As shown in Figure 4(a), the encrypted packets are then sent across to UDP. As shown in Figure 4(b),

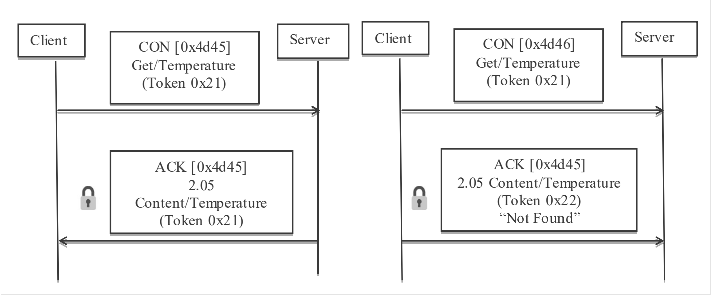


Figure 5: The success and failure response results of GET method.

the encrypted packets received from UDP are sent across to DTLS for decryption before being sent back to CoAP.DTLS supports the cipher suite based on Pre-shared keys (PSK) with SHA256: TLS PSK WITH SHA256 CCM 8. Each resource is accessible via a special Uniform Resource Identifier (URI) using GET, Place, POST, and DELETE REST methods and can be interacted with. CoAP can be considered a highly optimized variant of the Hypertext Transfer Protocol (HTTP) for use in a low-resource built-in domain [34, 35, 36]. Message Layer supports 3 types of message: CON (confirmable), ACK (Acknowledgement), RST (Reset)Maintain transmit until the same message ID (like 0x4d45 and 0x4d46in Figure 5) is issued to ACK. Usage of default time and exponentially decrease counting time as CON is transmitted. In case the receiver fails to process the message, ACK is replaced by RST for efficient transportation of communications. The client sends a request using the CON type message and automatically receives an ACK response with a conformal message. ACK contains a token response message for a good response; ACK contains a token response code for failure.

The simulation suggested for the data obtained and distributed using the Contiki Operating System (OS) and its implementations in smart buildings, is described in Figure 6. This proposed model simulates the network and derivesmeasurements from network nodes with the CoAP protocol. Such data can also be preserved in some scientific archives for future research. The Contiki OS provides an open-source framework for compact and intelligent devices that are low power consumption and not costly. It is also used for large-scale data processing. Also, rather than missing hardware equipment, we used aContiki Simulator.

We utilize the Cooja simulator system to demonstrate our organization continuously. The Power tracer, which can be found in the Tools menu under the name duty cycle of motes, is another useful application. With this technique, we can quantify the level of intensity utilized independently by every mote in the organization and the complete force utilized independently by all Sky motes. These estimations can be seen in the accompanying Table 2. Specifically, we get data on the force utilized in every hub just as the force utilized in the Transmission

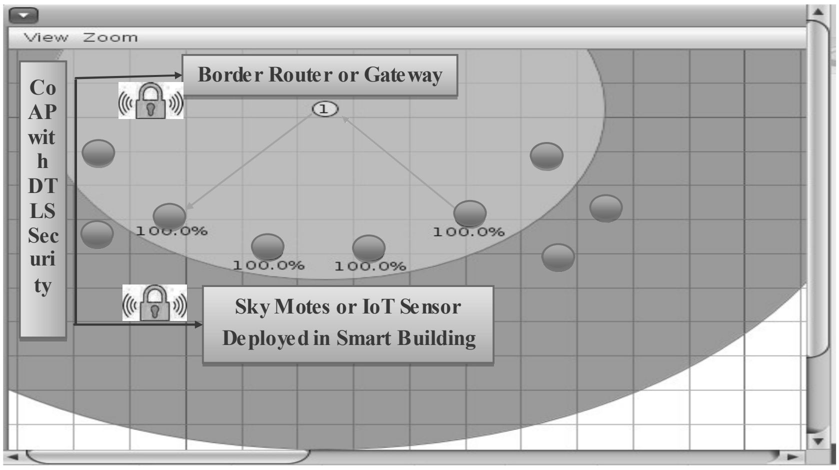


Figure 6: Proposed simulation in Contiki Cooja with Secured CoAP protocol.

Table 2: Status of all-sky motes

Motes	Radio on (%)	Radio TX (%)	Radio RX (%)
Sky Mote 1 (Border Router)	95.62%	0.65%	0.27%
Sky Mote 2	1.15%	0.30%	0.03%
Sky Mote 3	1.76%	0.55%	0.04%
Sky Mote 4	1.14%	0.28%	0.03%
Sky Mote 5	0.80%	0.05%	0.03%
Sky Mote 6	1.15%	0.64%	0.03%
Sky Mote 7	1.76%	0.31%	0.04%
Sky Mote 8	1.14%	0.55%	0.05%
Sky Mote 9	0.80%	0.22%	0.04%
Sky Mote 10	1.17%	0.05%	0.03%
AVERAGE	10.64%	0.29%	0.59%

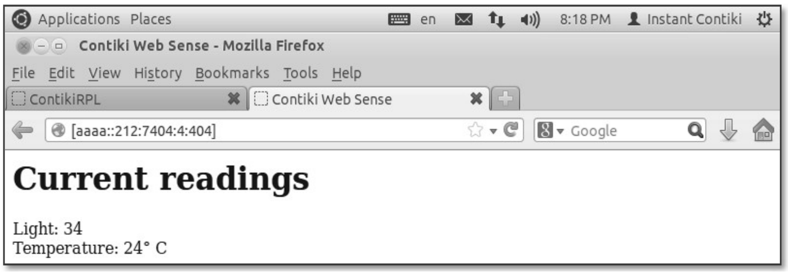
Cycle (TX) and Receiving (RX) for every mote and the normal yield. For our simulation, we utilize the low-limit bit type Sky mote, 10 KB RAM, and 48 KB ROM memory of the 8MHz MSP4300 microcontroller. This organization structure is picked because, in a general sense, it is an IPv6 Duplicated form to permit the IPv6 to run at a physical layer with low force radio frequency. The experimental results from the simulation, which we ran on Cooja, are demonstrated in the following section.

5. Result and Discussion

With the aid of Contiki Cooja with the CoAP protocol, we will explore the simulation of the proposed work. CoAP is a protocol for software that is intended to be used in very specific electronic devices that allow online interactive communication. CoAP is a protocol for use, such as IoT nodes, in resource-limited internet networks. CoAP is intended to automatically migrate to HTTP for easy incorporation into the network while retaining specific criteria including multi-casts, reasonably low overhead, and usability. With a basic binary base header format, CoAP uses two types of communications, requests, and responses. Options in an optimal Type-Length-Value format can be followed to the base header. By design, CoAP is connected to UDP and optionally to DTLS, offering a high degree of security in communications. The simulation parameters are given in Table 3.

Table 3: Simulation Parameters

Parameter	**Value**
Operating System	Contiki 2.7
Simulator	COOJA
Computer	RAM 8GB
Transmission Range	50m
Interference Range	55m
Simulation Time	90 minutes
Routing Protocol	CoAP
Number of Nodes	10
Topology	Random
MAC Layer	802.15.4
Node Type	Skymote
Packet Size	56 byte
Packet Rate	4P/s
Networking	Mesh
Node Distrubtion	Randomly



Current readings

Light: 34
Temperature: 24° C

Figure 7: Current mote reading.

Now simulation starts and ping can be performed at a new terminal for each address of a node in the network. However, a terminal window is opened and ready to enter the following commands to set the path to the Border Router. This returns a bridge, indicating that IPv6 addresses with the prefix aaaaa: :/64 have been established, and aaaa: :212:7401:1:101 is listed in the Border Router's IPv6 address. As shown in Figure 7, sensor values like temperature and light can be observed with the command "ping6 aaaa::212:7402:2:204" in the firefox browser. Thus, the value of every sensor mote can be easily observed similarly. We are now ready to begin our simulation, and ping can be performed in a new terminal for any address in the network, and the flow of each hope from each router node is expressed in "ttl" and "time (ms)."More precisely, the ttl=64 boundary router, ttl=63 a one-hop node, ttl=62 a two-hop node, and so on. The same is seen with the scatter period, which at the closest position is lower than the router, and the working flow of execution of simulation is shown below- icmp_seq=1 ttl=64 time=26.8 ms icmp_seq=2 ttl=63 time=139 ms icmp_seq=3 ttl=62 time=666 ms icmp_seq=4 ttl=61 time=308 ms icmp_seq=5ttl=60 time=481 ms Through using the collected and controlled sensor data, our proposed architecture will attain energy efficiency with high security. Contrary to previous works, we have integrated a framework that integrates sensors and has taken steps to enhance the organization of the smart building, to make the building "smart" and functional, for temperature, motion, light, and moisture. Users will have remote access to sensor data in our proposed framework and also must handle data information to take such steps. Besides, the IPv6 address of the limit router is printed as an output through opening a window, eg. Firefox. By typing the IPv6 address of each other node, the temperature and light will be printed.

$$\begin{aligned} T_{TEMP} = {} & TEMP_1 + TEMP_2 + TEMP_3 + TEMP_4 + TEMP_5 + \\ & TEMP_6 + TEMP_7 + TEMP_8 + TEMP_9 + TEMP_{10} \end{aligned} \tag{3}$$

Where T_{TEMP} is the total temperature and TEMP 1 to TEMP 10 are the temperatures of nodes 1 to 10.

For all nodes, the temperature shown in Figure 8 is equal and constant. The following

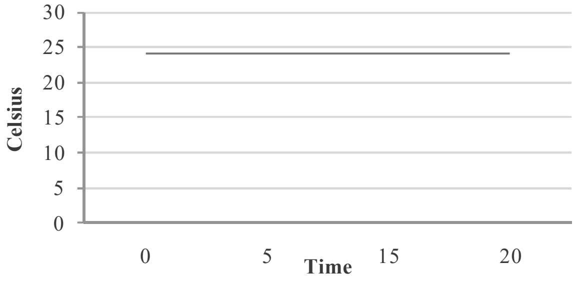


Figure 8: The temperature in all motes.

Equation 4 might explain this.

$$T_{DS} = T_{DR} + P_L \tag{4}$$

Where TDS, total data sent, TDR is total data received, and PL packet loss.

The security aspects are one significant factor when dealing with IoT protocols. CoAP uses UDP to transport information, as mentioned before. To safeguard the records, CoAP relies on UDP protection elements. As TLS over TCP is used for HTTP, CoAP uses Datagram TLS over UDP. Rivest–Shamir–Adleman (RSA), SHA, Advanced Encryption Scheme (AES), and so on are assisted by DTLS. Anyway, we should assume that some of the DTLS cipher suits might not be eligible for some restricted devices. It is important to remember that certain cipher suites are complicated and restricted devices do not have adequate resources to handle them. DTLS is a comparatively modern version of the mature protocol series SSL/TLS that offers the ability to secure link communication via the transport of alowernetwork layer such as UDP. The use of any of the techniques mentioned below may be used to implement DTLS.

1. TinyDTLS is a software library that offers a very basic datagram server that supports DTLS. It is aimed at embedded systems because it is designed to allow session multiplexing in single-threaded applications.
2. The lightweight TinyDTLS implementation is based on the open-source TinyDTLS library, which has been ported to Contiki. It supports AES-128 and SHA-256 encryption and does not fragment DTLS messages.
3. CoAP over DTLS used three libraries to implement lightweight versions of the DTLS and CoAP protocols, as well as the IPv6/6LoWPAN stack. TinyOS uses the nesC programming language to implement it. It defines the necessary interfaces for DTLS integration with CoAP and 6LowPAN.

The basic DTLS features include a Real-Time Publishing Subscription (RTPS) service. The DTLS architecture is decentralized to offer a high degree of stability and low-latency

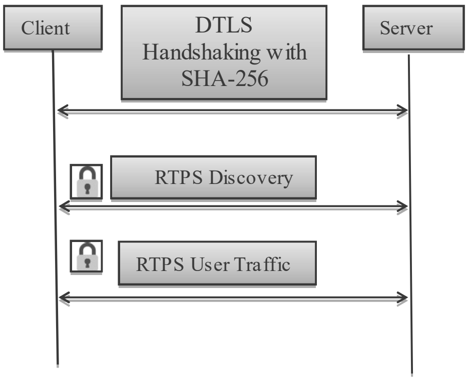


Figure 9: DTLS Handshaking Real-Time Publishing Subscription.

data access for essential IoT applications. The RTPS protocol employs discovery module data readers, data authors, and themes to reveal preconfigured QoS and security protocols, as well as current domain participant information [37]. A domain member is newly created. Definitions can also be omitted when network or system services are restricted from exploration announcements (see Figure 9). Security configurations can be achieved with common DTLS cipher suites, namely:

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_DHE_ECDSA_WITH_AES_128_GCM_SHA256

Length of bit size in SHA-1 IS 160 bit and in SHA-256 bit size is 256. Because of its smaller bit size, SHA1 is more vulnerable to attacks and SHA1 has been deprecated due to security flaws [38]. SHA256, which is more secure and reliable, uses a Public Key Infrastructure (PKI) where X.509 v3 certificates, signed by a trustworthy shared Certificate Authority (CA), are authenticated by communicating parties.

DTLS uses approvals and governance manuals defining the right of access within the entire Domain to specific themes and general security policies.Thus, the IoT technology's SHA-256 Cryptographic Hash Algorithm generates hashes for secure access, which are primarily used for verifying data and message integrity during transactions, session time, data identification, and password verification.

Sleeping End Point (SEP) is a special form of the system allowed by CoAP that spends a significant portion of its lifespan disconnected from the network, largely to conserve energy, or simply because it does not store the energy needed for its service. Nonetheless, in the same restricted RESTfull environment, it owns and hosts a collection of services and wants to

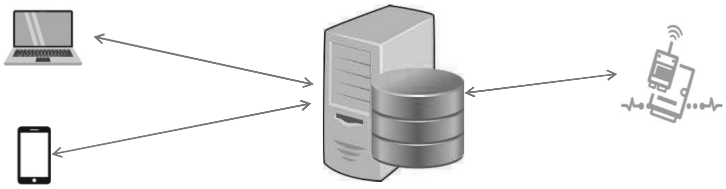


Figure 10: CoAP mirror server: clients and sleeping endpoints.

make them accessible to the other participants. In this respect, the processes that allow it to operate through its limitations must be built and enforced and its services must be accessible as if it were an ordinary, always linked, CoAP server. The Central Mirror Server (MS) is the second related CoAP mechanism. Mirror servers can often be used on behalf of mobile devices for mirror services which, due to their flexibility, often alter their Internet endpoint. Figure 10 demonstrates the configuration of a mirror server. SEP will start by registering its to-be mirrored resources with the mirror server via a POST request. From then on, sleeping endpoints will serve as clients of the CoAP. They upgrade their services to the mirror server via CoAP PUT requests and can request updates to the mirror server via CoAP POST request.

P_{trans}, the probability of successful transmission under CoAP, is calculated by adding the probabilities of successful transmission in both low and high loss states. CoAP offers a confirmable transmission mechanism, in which a packet is assumed to have been successfully transmitted once it receives an acknowledgement. The likelihood of effective transmission and acknowledgment, defined as $P_{ack,trans}$ is given by

$$P_{ack,trans} = P_{ack|trans,low}P_{trans|low}P_{low} + P_{ack|trans,high}P_{trans|high}P_{high} \tag{5}$$

where $P_{ack|trans,high}$ and $P_{ack|trans,low)}$ are the conditional probabilities of successful acknowledgment, given a successful transmission for the channel in the high and low loss states respectively; $P_{trans|high}$ and $P_{trans|low}$ are the conditional probabilities of successful transmission for the channel in the low and high loss states respectively; P_{high} and P_{low} are the steady state channel probabilities.

The overall probability of success or confirmable (P_{con}) after $R = k$ retransmissions of a packet frame follows a geometric distribution with Probability Mass Function (PMF) given by

$$P_{con}(R = K) = P_{ack,trans}(1 - P_{ack,trans})^k \tag{6}$$

Because up to N retransmission can occur before a packet is considered lost, the probability

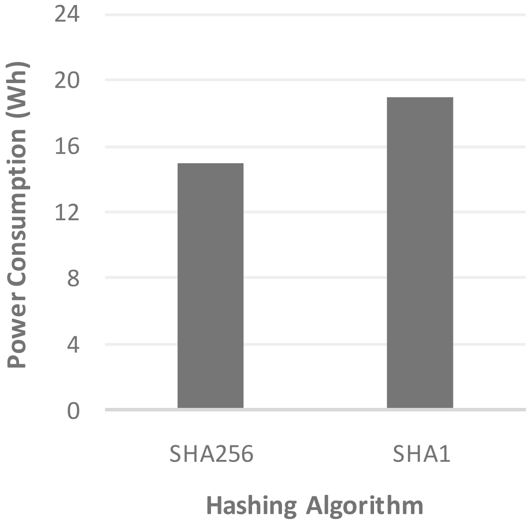


Figure 11: Power consumption in SHA256 Vs SHA1

of loss is given by

$$\begin{aligned} P_{con}(loss) &= 1 - \sum_{k=0}^{\infty} P_{con}(R = K) \\ &= 1 - P_{ack,trans} \sum_{k=0}^{N} (1 - P_{ack,trans})^k \\ &= (1 - P_{ack,trans})^{N+1} \end{aligned} \tag{7}$$

$$E(latency) = \left(min \left[\triangle \frac{(1 - P_{ack,trans}) P_{ack,trans}}{2P_{ack,trans} - 1} \right], \triangle 2^{N+1} - 1, Exchange\_Lifetime \right) \tag{8}$$

Where Exchange_lifetime is, as per CoAP conditions, the period from the beginning to send a conformable message to the time when an acceptance is no longer required and △ is the CoAP basic initial timeout is configurable and takes into account the minimum activity and if, as maximum latency is reached, all the packets are lost.The SHA-256 algorithm creates a 256-bit hash value from padded 512-bit message blocks with a maximum message size of 264-1 bits.Thus, the power consumption of SHA1 and SHA256 is shown in Figure 11. When compared to SHA1, it can be seen that SHA 256 used the least amount of power.

If all packets are dropped when the channel is in a heavy loss condition, that is = 1, and no packets are dropped when the channel is in a low loss state, that is = 0, the likelihood of

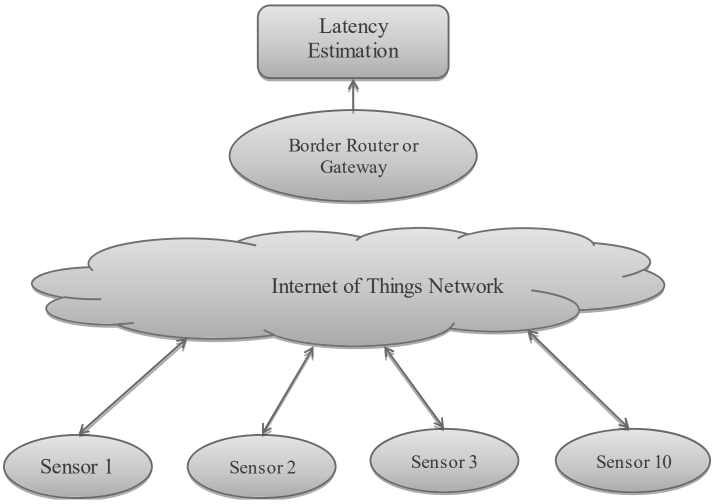


Figure 12: Power consumption in SHA256 Vs SHA1

a good transmission and acknowledgment is calculated as follows:

$$P_{ack,tran} = \frac{(1-@)(1-p)}{1-@+p} \tag{9}$$

and the non-confirmable as well as confirmable transport packet loss probabilities are given by

$$P_{non(loss)}\left(\frac{p}{1-@+p}\right) \tag{10}$$

Where, p, the probability of transitioning from a low-loss to a high-loss state β, when the channel is in a low-loss state, the packet loss probability γ, when the channel is in a high loss state, the probability of packet loss α, the probability of the channel remaining in a high-loss state

TheCoAP based experimental framework is shown in FIGURE 12 and performance analysis of the MQTT and CoAP protocols is conducted using tools from Contiki. Two parameters, Bandwidth and Packet Loss-are considered. At low bandwidth, the MQTT protocol has greater latency, and latency decreases as bandwidth increases. As shown in Figure 13, when the packet transmission bandwidth is 500 KB/s then latency in CoAP is 19ms, in MQTT is 24ms. Thus,CoAP has a lower latency compared to MQTT. The sliding window mechanism used by TCP flow control, as well as the three-way handshaking needed for initialising the communication in MQTT, are two major reasons for the difference in packet delivery latency between MQTT and CoAP. According to the sliding window characteristics, the transmitting side of a TCP-based link must avoid sending packets before the receiving device accepts all of the packets in the current sending window. Following data receipt, the receiver should send an

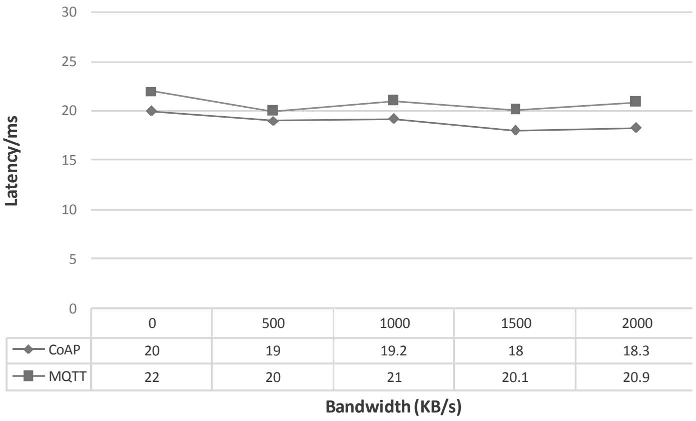
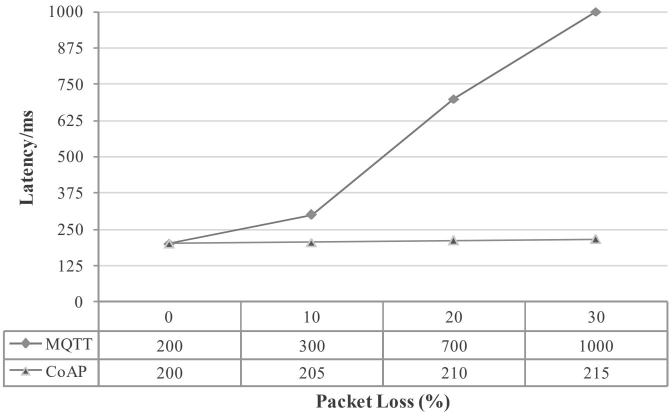


Figure 13: Analysis of protocols in terms of bandwidth and latency

acknowledgment along with a new receiving window indicating the number of bytes available in its buffer. This system would avoid congestion on the receiving side and, as a result, the receiver would not drop packets. More reliability would result, but at the expense of more power usage and a longer response time. With an increase in the rate of packet loss, the MQTT protocol increases latency exponentially. As compared to MQTT, CoAP experiences less latency (see Figure 14).

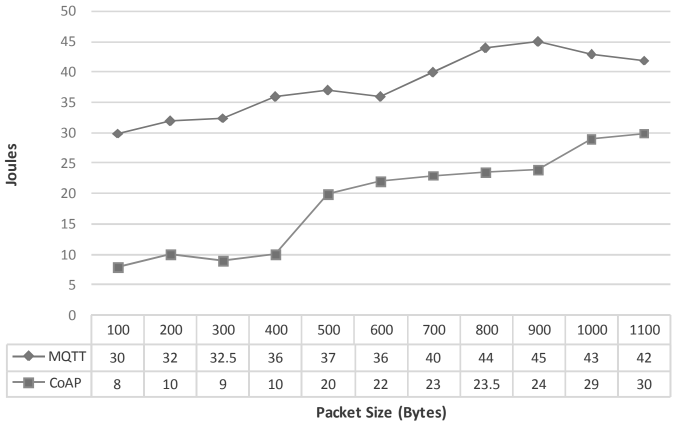
To compute the energy consumption, we trackedthe total energy consumption of all sensor Motes that generating periodically packets. The CoAP uses less energy than the MQTT, as shown in Figure 15. With nine concurrent client or sky mote requests, the average energy consumption for both protocols increases in proportion to the size of the payload, as expected.

In our proposed work, the data obtained and monitored by the sensors will help to achieve energy efficiency with the help of CoAP protocol and DTLS, offering a high degree of security in communications. We have developed, compared to past work, a system that includes IoT sensors that take action on temperature, activity, light, and humidity to achieve better control of buildings and to make the building ”intelligent” and functional. The user will have direct access to sensor data in the system we are implementing and should also comply with the device specifics to take any steps. Besides, to provide a clearer understanding, a comparative research description was tabulated in the form of Table 4 between conventional approaches and the proposed system.



	0	10	20	30
◆ MQTT	200	300	700	1000
▲ CoAP	200	205	210	215

Figure 14: Analysis of protocols in terms of packet loss and latency



	100	200	300	400	500	600	700	800	900	1000	1100
◆ MQTT	30	32	32.5	36	37	36	40	44	45	43	42
■ CoAP	8	10	9	10	20	22	23	23.5	24	29	30

Figure 15: Energy consumption of CoAP Vs MQTT

Table 4: Comparative study between the conventional approaches and the proposed scheme

Ref.	**Conventional Techniques**	**Scope of improvement**	**Proposed scheme Merits**
[20]	Proposed AIBSBAC architecture that can be appropriately adaptive to user needs, concentrating on improved user comfort, protection, and enhanced energy efficiency.	The authentication process is not done so resulting in a lack of security.	The proposed protection framework is based on the most commonly used PKI key and operates on top of regular stacks of low-power communication.
[21]	Proposed a smart building template that, by IoT technology, regulates the performance of all physical systems to achieve energy efficiency.	Only limited to the energy consumption applications, not provide high security.	Our test simulation results show that the CoAP protocol can minimize total network energy usage, dramatically boost energy balance, a well as providing high security with DTLS-CA Approaches.
[28]	The proposed solution is based on an IoT sensor node device to be examined in the smart building, connected to the Internet, capable of continuous measurement and real-time transmission of raw data through the MQTT protocol to the remote server.	Not the energy-efficient method.	CoAP experiences low power consumption, latency, and bandwidth.

6. Conclusion

In the next five years, IoT-based smart buildings areexpected to rapidly develop. Smart buildings have a huge influence on the growth of the nation. It is expected the combination of IoT, IP (IPv4 and IPv6) would improve building functions, power, energy efficiencies, and cost efficiency, transferring them into ”smart” buildings in the automation continuum. In recent years,administrations and regulators around the world, considering that buildings are major energy users, have become more focused on commercial buildings. This sector has a strong business opportunity, both because of its objective of reducing energy costs for builders and tenants and because of the efforts of energy service providers to minimize peak usage and construction of peak power plants, as well as maximizing the level of comfort for office users and residents, both in terms of temperature and lighting conditions. The development of suitable architectures and supportive specifications would be beneficial from a technology perspectiveso that both equipment cost-effectiveness and interoperability will be beneficial.

The simulation results showed that CoAP with DTLS reduces energy consumption with higher security (SHA256) when compared to MQTT. Therefore, we suggest that CoAP control be integrated into the IoT-based smart building platform to enable improved human care services. More results will be recorded in our future work.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Sedik, M. Hammad, F. E. Abd El-Samie, B. B. Gupta, A. A. Abd El-Latif, Efficient deep learning approach for augmented detection of coronavirus disease, Neural Computing and Applications (2021) 1–18.

[2] V. Adat, B. Gupta, Security in internet of things: issues, challenges, taxonomy, and architecture, Telecommunication Systems 67 (2018) 423–441.

[3] B. Miles, E.-B. Bourennane, S. Boucherkha, S. Chikhi, A study of lorawan protocol performance for iot applications in smart agriculture, Computer Communications 164 (2020) 148–157.

[4] D. Li, L. Deng, B. B. Gupta, H. Wang, C. Choi, A novel cnn based security guaranteed image watermarking generation scenario for smart city applications, Information Sciences 479 (2019) 432–447.

[5] B. Gupta, M. Quamara, An overview of internet of things (iot): Architectural aspects, challenges, and protocols, Concurrency and Computation: Practice and Experience 32 (2020) e4946.

[6] A. K. Rana, S. Sharma, Enhanced energy-efficient heterogeneous routing protocols in wsns for iot application, IJEAT 9 (2019) 4418–4425.

[7] C. L. Stergiou, K. E. Psannis, B. B. Gupta, Iot-based big data secure management in the fog over a 6g wireless network, IEEE Internet of Things Journal (2020).

[8] E. Png, S. Srinivasan, K. Bekiroglu, J. Chaoyang, R. Su, K. Poolla, An internet of things upgrade for smart and scalable heating, ventilation and air-conditioning control in commercial buildings, Applied Energy 239 (2019) 408–424.

[9] A. Kumar, A. O. Salau, S. Gupta, K. Paliwal, Recent trends in iot and its requisition with iot built engineering: A review, Advances in Signal Processing and Communication (2019) 15–25.

[10] G. Lilis, G. Conus, N. Asadi, M. Kayal, Towards the next generation of intelligent building: An assessment study of current automation and future iot based systems with a proposal for transitional design, Sustainable cities and society 28 (2017) 473–481.

[11] J. L. Hernández-Ramos, M. V. Moreno, J. B. Bernabé, D. G. Carrillo, A. F. Skarmeta, Safir: Secure access framework for iot-enabled services on smart buildings, Journal of Computer and System Sciences 81 (2015) 1452–1463.

[12] W. Lee, S. Cho, P. Chu, H. Vu, S. Helal, W. Song, Y.-S. Jeong, K. Cho, Automatic agent generation for iot-based smart house simulator, Neurocomputing 209 (2016) 14–24.

[13] M. V. Moreno, L. Dufour, A. F. Skarmeta, A. J. Jara, D. Genoud, B. Ladevie, J.-J. Bezian, Big data: the key to energy efficiency in smart buildings, Soft Computing 20 (2016) 1749–1762.

[14] J. Shah, B. Mishra, Customized iot enabled wireless sensing and monitoring platform for smart buildings, Procedia Technology 23 (2016) 256–263.

[15] L. Berntzen, M. R. Johannessen, A. Florea, Sensors and the smart city: Creating a research design for sensor-based smart city projects, in: ThinkMind//SMART 2016, The Fifth International Conference on Smart Cities, Systems, Devices and Technologies, 2016.

[16] K. Lin, M. Chen, J. Deng, M. M. Hassan, G. Fortino, Enhanced fingerprinting and trajectory prediction for iot localization in smart buildings, IEEE Transactions on Automation Science and Engineering 13 (2016) 1294–1307.

[17] S. Alletto, R. Cucchiara, G. Del Fiore, L. Mainetti, V. Mighali, L. Patrono, G. Serra, An indoor location-aware system for an iot-based smart museum, IEEE Internet of Things Journal 3 (2015) 244–253.

[18] M. J. Kaur, P. Maheshwari, Building smart cities applications using iot and cloud-based architectures, in: 2016 International Conference on Industrial Informatics and Computer Systems (CIICS), IEEE, 2016, pp. 1–5.

[19] Y. Sun, T.-Y. Wu, G. Zhao, M. Guizani, Efficient rule engine for smart building systems, IEEE Transactions on Computers 64 (2014) 1658–1669.

[20] B. Basnayake, Y. Amarasinghe, R. Attalage, T. Udayanga, A. Jayasekara, Artificial intelligence based smart building automation controller for energy efficiency improvements in existing buildings, International Journal of Advanced Automation Science and Technology 40 (2015).

[21] X. Zhang, M. Pipattanasomporn, T. Chen, S. Rahman, An iot-based thermal model learning framework for smart buildings, IEEE Internet of Things Journal 7 (2019) 518–527.

[22] A. Verma, S. Prakash, V. Srivastava, A. Kumar, S. C. Mukhopadhyay, Sensing, controlling, and iot infrastructure in smart building: a review, IEEE Sensors Journal 19 (2019) 9036–9046.

[23] D. N. Le, L. Le Tuan, M. N. D. Tuan, Smart-building management system: An internet-of-things (iot) application business model in vietnam, Technological Forecasting and Social Change 141 (2019) 22–35.

[24] E. Theodoridis, G. Mylonas, I. Chatzigiannakis, Developing an iot smart city framework, in: IISA 2013, IEEE, 2013, pp. 1–6.

[25] C. K. Metallidou, K. E. Psannis, E. A. Egyptiadou, Energy efficiency in smart buildings: Iot approaches, IEEE Access 8 (2020) 63679–63699.

[26] R. Casado-Vara, A. Martín del Rey, R. S. Alonso, S. Trabelsi, J. M. Corchado, A new stability criterion for iot systems in smart buildings: Temperature case study, Mathematics 8 (2020) 1412.

[27] O. Debauche, S. Mahmoudi, Y. Moussaoui, Internet of things learning: a practical case for smart building automation (2020).

[28] P. Pierleoni, M. Conti, A. Belli, L. Palma, L. Incipini, L. Sabbatini, S. Valenti, M. Mercuri, R. Concetti, Iot solution based on mqtt protocol for real-time building monitoring, in: 2019 IEEE 23rd International Symposium on Consumer Technologies (ISCT), IEEE, 2019, pp. 57–62.

[29] T. McGinley, A morphogenetic architecture for intelligent buildings, Intelligent Buildings International 7 (2015) 4–15.

[30] A. Mishra, N. Gupta, B. Gupta, Defense mechanisms against ddos attack based on entropy in sdn-cloud using pox controller, Telecommunication systems (2021) 1–16.

[31] A. Dahiya, B. B. Gupta, A reputation score policy and bayesian game theory based incentivized mechanism for ddos attacks mitigation and cyber defense, Future Generation Computer Systems 117 (2021) 193–204.

[32] P. Lin, L. Shen, Z. Zhao, G. Q. Huang, Graduation manufacturing system: synchronization with iot-enabled smart tickets, Journal of Intelligent Manufacturing 30 (2019) 2885–2900.

[33] D.-Y. Kim, S. D. Min, S. Kim, A dpn (delegated proof of node) mechanism for secure data transmission in iot services, CMC Comput. Mater. Cont 60 (2019) 1–14.

[34] Z. Zhang, P. Li, S. Zhao, Z. Lv, F. Du, Y. An, An adaptive vision navigation algorithm in agricultural iot system for smart agricultural robots, CMC-COMPUTERS MATERIALS & CONTINUA 66 (2021) 1043–1056.

[35] N. Kumar, V. Poonia, B. Gupta, M. K. Goyal, A novel framework for risk assessment and resilience of critical infrastructure towards climate change, Technological Forecasting and Social Change 165 (2021) 120532.

[36] C. Esposito, M. Ficco, B. B. Gupta, Blockchain-based authentication and authorization for smart city applications, Information Processing & Management 58 (2021) 102468.

[37] A. Tewari, B. Gupta, Security, privacy and trust of different layers in internet-of-things (iots) framework, Future generation computer systems 108 (2020) 909–920.

[38] R. K. Basak, R. Chatterjee, P. Dutta, K. Dasgupta, Steganography in color animated image sequence for secret data sharing using secure hash algorithm (2021).