International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Feasibility Review of DDoS Attack Mitigation on CoAP for IoT Networks

Radhika Patel*[1], Dr. Amit Nayak*[2], Raj Bhatia[3]

Submitted: 25/01/2024 **Revised**: 03/03/2024 **Accepted**: 11/03/2024

Abstract: Due to the rapid development of the Internet of Things (IoT) and the rise of linked devices, the necessity for quick and impermeable communication protocols has assumed critical importance. The Constrained Application Protocol (CoAP), which is specifically designed for IoT devices, places a high priority on compactness and energy economy. Despite its preference for these characteristics, it stands out for its vulnerability to impending Distributed Denial of Service (DDoS) attacks brought on by its weak security characteristics. This paper examines CoAP in detail and explores its suitability as a defense against DDoS attacks. Our main goal is to provide insights into the difficulties and likely directions for bolstering CoAP's security framework in order to effectively combat DDoS attacks. To achieve this, a thorough investigation into the advantages and disadvantages of CoAP will be meticulously carried out.

Keywords: *Attacks, Denial of Service attacks, Distributed Denial of Service attacks, IoT, Networks, Security, Security aspects*

1. Introduction

The Internet of Things (IoT) paradigm is a revolutionary development that has gained significant recent popularity [1]. This idea relates to the broad interconnectedness of physical objects such as equipment, vehicles, and home appliances that are all equipped with sensors, programming logic, and internet connections to gather and distribute data [2]. The realization of a cogent environment in which these artifacts may easily communicate with one another, with human agents, and with cloud-centric frameworks is the overriding goal of the Internet of Things. This connection enables automated decision-making, data-centric decision-making, and an overall improvement in ease and efficiency [3].

Various sectors have been altered by the IoT landscape's arrival, which brought forth unmatched connectedness and ease. Due to its resource-friendly architecture and lightweight design, CoAP has become a popular communication protocol for IoT devices [4]. However, because of its shoddy security measures, it might be subject to Distributed Denial of Service (DDoS) attacks. This study aims to assess the effectiveness of CoAP as a defense against such assaults and pinpoint potential directions for strengthening its security standards [4].

The Internet of Things (IoT) is significant because it has the potential to dramatically revolutionize a variety of sectors and facets of daily life [5]. The following are some significant fields where IoT has a significant impact:

a. Smart houses: The IoT enables the development of intelligent houses with linked and remote-managed appliances, lighting controls, security cameras, and thermostats. As a consequence, energy efficiency, home security, and general comfort all increase [6].

b. Industrial IoT (IIoT): In industrial environments, IoT devices are useful for asset tracking, predictive maintenance, and process optimization, which boost productivity and reduce downtime [7].

c. Healthcare**:** IoT-driven medical devices may remotely monitor patient health, promote adherence to treatment programs, and speed up reactions to urgent situations, all of which improve patient outcomes [8].

d. Smart Cities: Through the integration of data from diverse sources, including traffic sensors, waste management systems, and energy grids, the IoT plays a crucial role in forming smart cities [9]. The administration of resources, citizen services, and urban planning are all improved by this data-centric approach.

e. Agriculture: By monitoring soil conditions, weather patterns, and crop health, IoT sensors can optimize agricultural practices, boosting crop yields while minimizing resource waste [10].

f. Transportation: The Internet of Things (IoT) enables the creation of intelligent transportation systems that include linked cars, traffic management tools, and autonomous driving systems. The main objectives are to increase road safety and reduce traffic congestion [11].

1.1 CoAP as a Communication Protocol for IoT Devices

An application-layer protocol designed especially for Internet of Things (IoT) deployment and networks with resource constraints is called Constrained Application Protocol (CoAP). IoT networks frequently have limitations including low bandwidth, limited computing power, and energy limits [12]. Because CoAP is designed to provide simple, lightweight, and energy-efficient communication, it is an excellent choice for Internet of Things applications, especially in resource-constrained contexts [13].

a. Resource-Centered Design: CoAP follows a resource-centered design that is comparable to the architecture of the Hypertext Transfer Protocol (HTTP). The CoAP framework uses Uniform Resource Identifiers (URIs) to identify resources, and clients may communicate with these resources using well-known HTTP-like operations like GET, POST, PUT, and DELETE. The ability to display their capabilities and data as resources that other devices and apps may easily access and alter gives IoT devices this ability [14].

b. Minimal Communication Overhead: CoAP uses the User Datagram Protocol (UDP) as its primary transport protocol, which reduces communication overhead in comparison to HTTP's use of the Transmission Control Protocol (TCP) For devices with limited resources, such as processing speed and memory, this decreased overhead is crucial [15].

c. Built-in qualities: CoAP has built-in qualities necessary for IoT configurations. One way to do this is to enable multicast communication, which encourages both one-to-many and many-to-many interactions. Real-time updates and the effective management of asynchronous processes are also made possible by CoAP's intrinsic support for asynchronous communication and event alerts [16].

d. Support for Proxy and Caching: CoAP has support for proxying and caching, which are essential for effective communication in large-scale IoT installations [17]. While caching helps reduce duplicate data transfers and mediates communication between devices, proxies also mediate communication between devices.

e. Security Thoughts: To protect inter-device communication, CoAP provides simple security elements such as Datagram Transport Layer Security (DTLS). It is crucial to recognize that the default security procedures in CoAP may not be adequate for really sensitive IoT applications, which may call for additional security precautions [18].

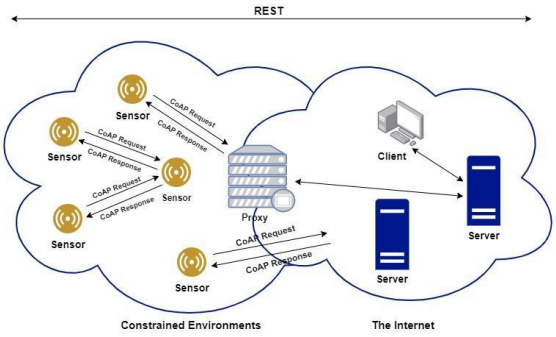

Fig. 1. IoT Devices and the CoAP Communication Protocol

A. ***CoAP vs. HTTP for IoT Communication***

In the context of the internet, CoAP and HTTP are frequently compared since they both serve as application-layer protocols. But there are a few noticeable differences that set them apart [19].

a. Overhead in Communications: CoAP is better suited for devices and networks with limited resources because of the reduced overhead caused by the use of UDP.

b. Request-Response Structure: Similar to HTTP, CoAP's request-response structure encourages simple communication patterns between servers and clients.

c. Asynchronous Interaction: CoAP naturally supports asynchronous interaction, which is essential for Internet of Things (IoT) applications characterized by patchy connectivity or inconsistent device response times.

d. Multicast Support: CoAP includes built-in support for multicast communication, enabling effective group collaboration in IoT environments.

e. Resource Discovery: CoAP has built-in methods for resource discovery that speed up the process by which clients locate resources across networks or devices.

f. Security: Both protocols have security precautions, but CoAP's use of Datagram Transport Layer Security (DTLS) for protected communication is particularly well-suited for contexts with constraints.

TABLE I. A COMPARISON OF THE RESOURCE USAGE OF HTTP AND COAP

Protocol	Transactional bytes	Life span (days)	Power (in mW)
HTTP	1451	84	1.333
CoAP	154	151	0.744

As per the [20] conducted a comparison of the CoAP and HTTP protocols in terms of battery life, power consumption, and the amount of bytes exchanged each transaction. The outcomes are displayed as follows in Table I.

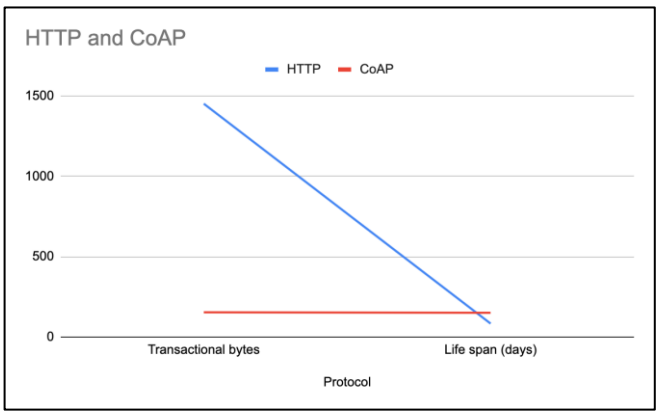

Fig. 2. Line graphs compare HTTP and CoAP resource consumption.

As a result, we decide to use the CoAP protocol to facilitate communication between the IoT server, which provides data to the observer, and the IoT client, which must monitor the resources.

2. Ddos Attack Vectors on Coap

1.1 Protocol Exploitation

The Internet of Things (IoT) environment's resource-constrained devices and networks are catered to by CoAP, a lightweight and energy-efficient protocol. However, because of its lack of robust security measures, it is vulnerable to possible flaws that bad actors may use to plan Distributed Denial of Service (DDoS) attacks. The following are significant CoAP flaws that might be used for DDoS attacks [21].

TABLE II. Attack Vectors for DDoS on CoAP

Attack Type	Description
UDP-based DDoS Attacks	Flooding the target device or server with a huge amount of CoAP packets, overloading its resources and resulting in a denial of service [22].
Amplification Attacks	Exploiting CoAP's multicast communication feature to send short CoAP requests with fake source addresses to a multicast group, causing all devices in the group to respond to the victim, significantly amplifying the traffic towards the target [23].
Manipulation of URI Paths and Query Options	URI path abuse, often referred to as query abuse, is the practice of creating malicious requests with needlessly lengthy or complex URIs, requiring the target server to use unnecessary resources and time in interpreting the request, ultimately leading to resource exhaustion [24].
Exhaustion of CoAP Tokens	Flooding the target server with multiple CoAP requests, each carrying a different token, leading to the exhaustion of the server's token table and the rejection of legitimate requests [25].
Resource Depletion	Sending a large stream of CoAP requests directed at specific server resources, depleting the target device's limited memory, computing power, and network bandwidth, rendering it unable to fulfill legitimate requests [26].
ACK Storm Attacks	Sending an excessive amount of token-containing CoAP requests to the target server, which results in the server's token database running out and the rejection of legitimate requests [27].
Manipulation of the "Observe" Option	Modifying the target server by generating an extensive range of pointless Observe subscriptions, which might result in wasteful resource use and the server's inability to manage legitimate subscribers [28].
Proxy CoAP Exploitation	Using the proxying capabilities of CoAP to send malicious requests through proxies, conceal the attackers' true source, and increase the impact of the assault. [29]

To address vulnerabilities and protect CoAP-based IoT devices against DDoS attacks, it is crucial to make sure that the controls in Table II above—filtering, request validation, rate restriction, and access control—are applied successfully. Furthermore, identifying and blocking anomalous traffic patterns indicative of DDoS assaults can be facilitated by the use of intrusion detection and prevention systems specifically designed for CoAP. Ensuring the durability and security of IoT ecosystems requires proactive updates of CoAP implementations and ongoing security risk monitoring.

3. Analysis of Ddos Flooding Attacks that Target Coap Servers and Endpoints

A common and effective method used by bad actors to obstruct internet services, including CoAP servers and endpoints within the Internet of Things (IoT) architecture, is DDoS flooding [30]. These attacks flood the target systems with an excessive amount of traffic, exhausting their resources and denying genuine users of their services. Let's examine DDoS flooding assaults in detail, paying particular attention to how CoAP servers and endpoints were targeted [31].

a. UDP Flood Attacks: UDP flood attacks are among the most popular DDoS tactics used against CoAP servers since UDP is the transport protocol that CoAP relies on as a basis. Attackers launch a massive avalanche of CoAP packets in the direction of the target server, frequently using fake or randomly created source IP addresses. The server's capacity to distinguish between legitimate requests and the flood of malicious traffic is hampered by this practice. The server is exposed to a massive inflow because UDP runs without establishing a connection before processing a packet [32].

b. Attacks on resource discovery: CoAP has techniques for resource discovery, allowing clients to find accessible resources on the server. Attackers take advantage of this feature to carry out resource discovery attacks, in which a large number of discovery requests are sent to the

server. This depletes the server's resources and causes service interruptions [33].

c. Request Flooding: Request flooding is a type of assault activity that CoAP encounters in a surge. In this scenario, attackers overload the server with excessive CoAP requests for a single resource or even a set of resources. The server cannot react to legitimate customers because of this flood of requests, which exhausts its processing power. Although the methods of the requests might vary, their sheer number is enough to prevent the server from operating normally [34].

d. Attacks that Reflect and magnify: Reflection and amplification attacks reflect and magnify attack traffic by tricking intermediate services. Attackers can use unsecured or improperly configured CoAP proxies for amplification in the context of CoAP. The traffic directed at the target CoAP server or endpoint is amplified by sending a small number of requests to a proxy with a fake source IP address, which causes the proxy to respond with a bigger response [35].

e. Token Exhaustion Attacks: CoAP is vulnerable to token fatigue attacks because it relies on tokens to correlate requests and answers. Attackers use this strategy by flooding the server with several CoAP requests, each carrying a unique token [36]. As a consequence, the server's token database fills up and valid requests are turned down, causing an interruption in service.

f. Abuse of Proxy Requests: Because CoAP supports proxying, intermediaries can send CoAP requests to other servers. Malicious organizations make use of this capability by sending a large number of CoAP requests through unreliable proxies. By using this tactic, the attack's impact on the target server is increased while the attack's true source remains hidden [37].

Adopting strong security measures is essential to reducing the danger presented by these DDoS flooding assaults and enhancing the resilience of CoAP-based IoT systems. Implementing traffic shaping, access restrictions, request validation, and traffic filtering are required for this. The identification and prevention of abnormal traffic patterns typical of DDoS assaults can be facilitated by the use of intrusion detection and prevention systems designed for CoAP. To maintain the integrity and security of IoT ecosystems, CoAP deployments must be continuously monitored and updated to address new security vulnerabilities [38].

2.1 Mitigation Strategies:

Certainly, you've provided a thorough list of efficient mitigation techniques to thwart DDoS flooding assaults on CoAP servers and endpoints in IoT networks. Collectively, these actions can increase the resistance of CoAP-based systems to such attacks.

TABLE III. Strategies for Mitigation

Technique	Description
Traffic Filtering	Recognise and stop anomalous traffic patterns linked to DDoS assaults [39].
Rate Limiting	To lessen the impact of request flooding attacks, limit the number of requests made by a single client [40].
Server and Proxy Hardening	Set up CoAP proxies and servers securely to stop weaknesses from being used in reflection and amplification attacks [41].
Load Balancing	To manage traffic spikes and fix vulnerabilities in the system, load balancers should be used to split up incoming CoAP requests across several servers [42].
Anomaly Detection	Install systems that keep an eye on CoAP traffic and spot unusual patterns that point to DDoS assaults so that countermeasures and early detection may be taken [43].
Router Blackhole	Reduce the effect of the attack by employing blackhole routing techniques to divert malicious traffic away from the target server [44].
Cloud-based DDoS Protection	To prevent strong assaults from reaching CoAP servers, use cloud-based DDoS protection solutions. These systems take use of the scalability and threat mitigation experience of the cloud [45].
Frequent Patches and Updates	To stop known vulnerabilities from being exploited, keep your CoAP implementations up to speed with the newest security patches and updates [46].

Administrators may reduce the likelihood and severity of DDoS flooding attacks against CoAP servers and endpoints by combining these strategies into a single security plan and continuously keeping an eye on the Internet of Things, as shown in Table III above.

4. Feasibility Study for Coap-Based Ddos Mitigation

The Constrained Application Protocol (CoAP)-adopting devices and services on the Internet of Things (IoT) are particularly vulnerable to Distributed Denial of Service (DDoS) assaults [47]. Because CoAP is primarily made for confined devices and networks, its security features are limited, making it vulnerable to DDoS assaults. This study intends to evaluate CoAP's potential efficacy and

performance as a mitigation approach since the notion of using it for DDoS mitigation holds promise [48].

3.1 CoAP-based DDoS mitigation's efficacy

The low processing cost of CoAP's architecture makes it possible to handle large request volumes effectively, which helps to identify and filter DDoS attack traffic. IoT devices may actively contribute to DDoS mitigation efforts despite resource limits since CoAP is aligned with such limitations. CoAP enables real-time DDoS attack detection and mitigation by utilising asynchronous communication and event notifications. This reduces the effect of DDoS assaults by expediting reaction times. Furthermore, by allowing the interception and filtering of harmful traffic prior to it reaching target servers, CoAP's proxy and cache functions lessen the burden on backend infrastructure and lessen the impact of DDoS attacks [49].

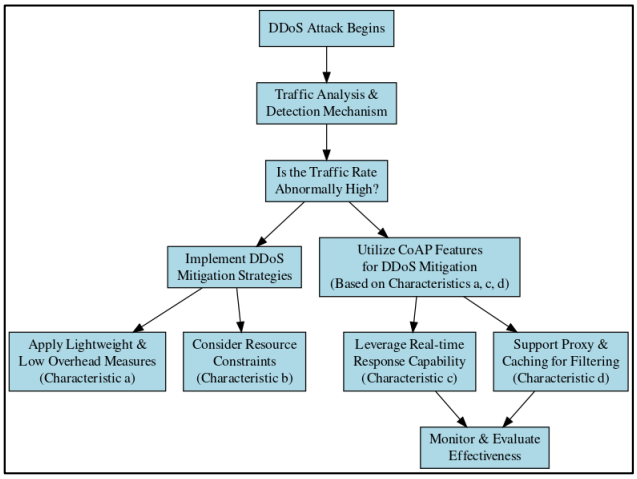

Fig. 3. CoAP-based DDoS mitigation workflow

The following figure 3 illustrates the steps that a DDoS attack goes through in order. After the DDoS attack is launched, the procedure switches to traffic analysis and detection. When the flowchart notices an abnormally high traffic rate, it suggests putting DDoS mitigation measures in place. These countermeasures take into account a number of attack characteristics, such as resource constraints, instantaneous response times, and the use of proxy and caching systems for filtration. The final step in the process is to monitor and evaluate how well the mitigation methods that have been implemented are working.

3.2 Performance Considerations:

The efficacy of utilizing CoAP for DDoS mitigation in IoT contexts will be decisively determined by this thorough examination of performance issues. It emphasizes the need for systems that can successfully defend against attacks while maintaining the integrity of legal traffic processing, all while adjusting for the resource constraints present in CoAP-enabled devices [50].

a. Scalability: Strict scalability testing should be done to determine the effectiveness of CoAP-based DDoS mitigation. This test confirms the solution's capacity to successfully defend against widespread assaults while maintaining the competence to control lawful network flow. Scalability is crucial for the system to be practical in actual assault scenarios [51].

b. Resource Utilization: A thorough examination is required to determine the impact of DDoS mitigation strategies on the total resource consumption of IoT devices given the resource limits present in CoAP devices. The mitigation techniques need to be carefully planned in order to provide a light and effective appearance while avoiding the risk of resource depletion [51].

c. Latency and Response Times: Quick detection and action are required for real-time DDoS mitigation using CoAP. In order to prevent the intervention from excessively delaying the treatment of legal traffic, the research should examine the latency that is imposed by these mitigation methods. To provide the best user experience, a balance must be struck between quick response and low latency [51].

d. False Positives and Negatives: A crucial component of CoAP-based DDoS mitigation is accurate differentiation between genuine and malicious data. The ability of the solution to discriminate between the two groups should be thoroughly evaluated in the feasibility study. The success of the system depends critically on reducing instances of false positives (blocking real users) and false negatives (allowing malicious traffic) [51].

3.3 Improved security measures

a. Secure Communication Using DTLS: The effectiveness of DTLS (Datagram Transport Layer Security) in strengthening CoAP communication should be thoroughly evaluated in the feasibility study. To prevent possible attackers from interfering with DDoS mitigation operations, this examination is essential [52].

b. Finding anomalies: It has potential to include anomaly detection methods into CoAP-based DDoS mitigation. The effectiveness of these strategies in identifying and intercepting traffic patterns suggestive of DDoS assaults should be the focus of the investigation [52].

c. Access Management: Access control features included in CoAP devices offer a way to prevent unauthorized access and lessen the effect of DDoS assaults. The usefulness and benefits of such systems should be covered in the feasibility study [52].

3.4 Tests of performance and simulations:

The feasibility study should include thorough simulations and performance testing. The effectiveness and efficiency of CoAP-based DDoS mitigation are evaluated through these

activities. The simulation of several DDoS attack types under controlled circumstances enables the evaluation of the responsiveness and efficacy of the mitigation systems [53].

3.5 Resource and Cost Analysis:

The research must broaden its scope to include a cost-benefit analysis of the adoption of CoAP-based DDoS mitigation. Costs for maintenance, software, and hardware should all be included in this evaluation. The analysis should also take into account the resources required for managing and deploying the mitigation solution [54].

3.6 Analysis of Current CoAP-based DDoS Mitigation Techniques:

It is the responsibility of the feasibility study to evaluate any CoAP-based DDoS mitigation technologies that are already available on the market or are developing inside research circles. Such an assessment offers priceless insights into the health of the industry today and possible directions for growth and innovation [55].

5. Enhancing Coap Security for Ddos Mitigation

A complete foundation for creating secure CoAP communication inside IoT ecosystems is provided by the practices and guidelines you've presented, without a doubt. Organizations may greatly improve the security of their IoT devices and networks by following these principles [56], [57].

TABLE IV. Improving CoAP Security to Reduce DDoS Attacks

Security Measure	Description
Use of DTLS for Secure Communication	DTLS is used to protect data integrity and secrecy during CoAP transmission.
Authentication of Users and Devices	Mutual authentication is being used to prevent unwanted access and guarantee that only reliable people and devices are able to connect to the Internet of Things.
Secure Management of Passwords and Keys	Putting strong key management processes in place to stop illegal access and man-in-the-middle attacks.
Access Control Measures	Implementing access control protocols to restrict unapproved interaction and minimise the possible attack area.
Verification of CoAP Messages	Verifying incoming messages in accordance with the CoAP protocol specifications to stop protocol flaws from being exploited.
Request Throttling and Rate Limiting	Reducing the amount of messages transmitted in a second using strategies like rate limitation to reduce DDoS assaults.
Monitoring and Detection of Anomalies	Real-time monitoring and anomaly detection are used to identify unusual activity and take quick action in response.
Encryption of Sensitive Data	Enhancing encryption to better safeguard sensitive data, including PII and information about IoT devices.
Regular Firmware Updates	The frequent application of firmware upgrades to safeguard devices against known defects and vulnerabilities.
Secure Boot and Device Integrity	To avoid unauthorised firmware alteration and preserve device integrity, secure boot processes should be implemented.
Secure Bootstrapping	Implementing safe bootstrapping techniques to build a foundation of confidence during device setup.
Secure Proxy and Gateway Deployment	Implementing proxy and gateway configurations safely to guarantee the privacy and integrity of the traffic that passes through.
Implementation of Privacy Considerations	Putting user privacy first by using techniques for data minimization and anonymization to build confidence.
Regular Security Audits and Penetration Testing	Identifying vulnerabilities and weaknesses through regular examinations that allow for proactive correction.

Companies may create a secure CoAP communication environment in the Internet of Things by referring to Table IV. The continuous implementation of these controls and monitoring of newly emerging threats as the threat environment evolves are necessary to maintain the integrity and security of IoT ecosystems.

6. Case Studies

The use of CoAP as a defense against Distributed Denial of Service (DDoS) assaults in the real world has shown successful results in some cases. Instead of being regarded exclusively as a specialized DDoS mitigation solution, CoAP is mostly known for its role in promoting Internet of Things (IoT) connectivity. However, its resource-constrained limits and simplified design have been looked into as possible benefits for efficiently tackling particular DDoS attack types in IoT scenarios. Let's examine a case study that demonstrates

how CoAP's advantages might be used to lessen DDoS threats:

Mitigation Using a CoAP Proxy-Based Approach:

CoAP proxies are used as an intermediary layer in an IoT deployment where CoAP is the selected communication protocol for linked devices as a strategic countermeasure against DDoS assaults. These proxies operate as a first line of defense by coordinating operations like traffic screening, rate capping, and access control, all of which are intended to protect the central CoAP servers and endpoints from the damaging effects of DDoS assaults. In order to clarify the practical effects of using CoAP proxies for DDoS mitigation, the following hypothetical scenario is provided:

Scenario:

A large number of CoAP-capable devices that are connected to backend servers through the CoAP protocol make up an Internet of Things (IoT) ecosystem. Unfavorably, a malicious actor turns their focus to this ecosystem and launches a DDoS flooding assault with the intention of overloading the CoAP servers with a deluge of nefarious CoAP requests.

DDoS Protection Using a CoAP Proxy:

a. Traffic Filtering: At the gateway, CoAP proxies act as sentinels, intercepting and closely examining incoming traffic. The proxy identifies and distinguishes harmful traffic by examining traffic patterns typical of DDoS assaults, effectively blocking requests with known malicious sources or suspicious behavior.

b. Rate Limiting: The CoAP proxies are capable of implementing responsible rate-limiting procedures. These policies place limits on the number of CoAP queries that are allowed from specific clients or IP addresses. As a result, the backend servers are shielded from an onslaught of requests from a single attacker.

a. Access Control: By zealously implementing access control policies, CoAP proxies assume the role of guardians. The right to interact with certain resources is only granted to devices that have the required authorization. Requests from unauthorized impenetrable barrier, which effectively reduces the possible target surface.

c. Load balancing: CoAP proxies cleverly distribute incoming CoAP requests over a variety of backend servers by utilizing load balancing techniques. This intelligent distribution prevents a heavy burden on any one server by ensuring an equitable dispersion of the assault load.

d. Anomaly Detection: CoAP proxies that are adept at spotting anomalies act as vigilant sentinels. They have the ability to spot irregularities in traffic patterns that depart from accepted standards. The proxies are equipped to preventively identify and mitigate DDoS attacks thanks to their keen perception.

Positive Outcomes:

The IoT ecosystem benefits from the use of CoAP proxies as a strong DDoS mitigation layer in a variety of ways:

a. Diminished Impact: The ecosystem successfully reduces the direct impact of the DDoS onslaught by placing CoAP proxies at the forefront in a planned manner. As a result, endpoints and backend servers are shielded from the attack's full-fledged savagery. By protecting resources, legitimate CoAP traffic is protected and is able to continue flowing unhindered.

b. Scalability: CoAP proxies come with built-in scaling capabilities. This versatility includes supporting a sizable number of devices as well as the constant influx of DDoS traffic. The IoT environment thus exhibits its resilience by successfully reacting to varying degrees of assault intensity.

c. Real-time response: Attempts to mitigate DDoS make use of CoAP's intrinsic inclination for asynchronous communication. The CoAP attribute on the proxies makes it easier to quickly identify and stop malicious traffic in real time, enabling an immediate response against DDoS attacks.

d. The fictitious example highlights how CoAP proxies may be used to protect an IoT environment from the dangers posed by DDoS assaults. This illustration should be viewed as a hypothetical situation that has to be empirically validated and tested in actual deployments.

Limitations and Failures

Situations where CoAP's deployment failed to effectively prevent DDoS attacks and any lessons that may have been applied.

The implementation of CoAP has several limitations that may make it difficult to effectively prevent some types of DDoS assaults. The following are some situations where CoAP's implementation has trouble managing DDoS mitigation:

a. Amplification Vulnerabilities: Attackers may use CoAP's use of multicast communication to launch amplification attacks. Attackers communicate with a CoAP multicast group by sending brief CoAP requests with bogus source addresses. As a result, the victim becomes the focus of attention for all group members' answers, amplifying the attack traffic.

- Lesson Learned: CoAP deployments must enact strict access controls and filtering procedures to prevent unauthorized devices from joining multicast groups. Additionally, using CoAP proxy servers can make it

easier to analyze and filter any potentially harmful multicast traffic before it gets to the designated server.

b. Attacks based on token exhaustion: Attackers take advantage of CoAP's use of tokens to link requests and responses. They send a ton of CoAP requests, each with a different token, to the server. This massive surge of requests causes the server's token database to run out, perhaps leading to the denial of valid requests.

- Lesson Learned: Implementing token management strategies like expiry and recycling can stop token depletion attacks. The use of tokens with a short lifespan and effective token storage techniques might further reduce the effects of such assaults.

c. Limited Security Features: When compared to protocols like HTTPS, CoAP's security features, which are mostly rooted in Datagram Transport Layer Security (DTLS), are somewhat underwhelming. Although DTLS offers encryption and authentication, it cannot provide complete defense against sophisticated DDoS assaults.

- Lesson Learned: CoAP implementations should include other security mechanisms like rate restriction, comprehensive request validation, and strict access controls in addition to DTLS to increase its effectiveness. Integrating intrusion detection systems (IDS) with anomaly detection systems can increase the capacity to recognize and respond to potential DDoS attacks.

d. Inadequate Resource Management: Because CoAP servers and devices must deal with limited resources, they are vulnerable to DDoS assaults that take advantage of these restrictions and might leave the device unable to respond to valid requests.

- Lesson Learned: Resource management techniques like request throttling and resource prioritization can prevent resource depletion during DDoS attacks. CoAP devices are capable of navigating unanticipated traffic spikes efficiently because of thorough capacity planning and load testing.

e. Scalability Issues: Due to scalability limitations, managing DDoS assaults in sizable IoT settings with a large number of CoAP devices can be challenging.

- Lesson Learned: The distribution of load across different servers should be considered during CoAP installations to avoid single points of failure and improve the overall robustness of the IoT ecosystem. Utilizing edge gateways and load balancers makes it possible to handle traffic effectively.

f. Lack of Immediate Response: In some circumstances, especially when dealing with complex and extensive DDoS attacks, CoAP's ability to respond quickly may be jeopardized.

- Lesson Learned: To improve CoAP's agility in identifying and thwarting DDoS assaults, it is essential to set up real-time traffic monitoring and analysis tools. Automated response mechanisms and human involvement lessen the consequences of complicated assaults.

7. Results and Discussion

We describe our approach together with its implementation and performance analysis in an effort to strengthen the security of the CoAP protocol by incorporating the Third Party (TP) concept into DTLS according to [58]. Creating the improved DTLS protocol in MATLAB, utilising specialised libraries to manipulate the CoAP protocol, and simulating the system at the system level with SIMULINK are all part of the implementation process. The main idea behind the implementation is to strengthen CoAP communication by combining DTLS with Internet Protocol (IP) concepts. The suggested improved protocol employs TP to decrease DoS concerns by establishing a shared secret key between trustworthy peers (TP and server) for client and server authentication. TP authenticates the client for server access after first confirming the validity of incoming traffic using specified IP address lists. The improved DTLS protocol implementation incorporates traffic behaviour analysis (traffic behaviour analysis) to filter incoming CoAP packets and classify IP addresses into Blocked, Suspicious, and Trusted lists. In order to verify consistency with prior encounters from the same IP, comparisons with a predetermined Payload threshold (PLT) and careful examination of traffic patterns are required. Three machines—trusted, suspect, and blocked—transmit packets to a host server as part of the implementation model. The enhanced DTLS protocol filters traffic and updates IP address lists in the SIMULINK environment for further analysis.

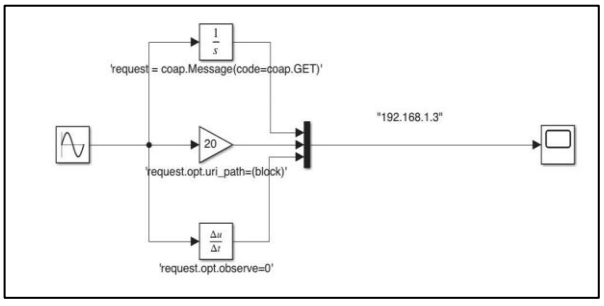

Fig. 4. The proposed model in Simulink

Important insights were obtained from running simulations in the MATLAB Simulink framework. The results are shown in Figures 2 and 3, where the three user types—trusted, suspect, and blocked—are denoted by yellow, blue, and red traffic, respectively. Figure 2 shows that the suggested approach was notably effective when one user per type was used. In order to effectively prevent traffic from suspicious and blocked machines, the TP server updated the Suspicious List (SL) and avoided communication from the machine with the blocked

IP. The trustworthy machine's traffic was successfully allowed, and its IP was added to the trusted list. The color-coded traffic classification remained in Figure 3, with 30 users per type, highlighting the TP server's capability to distinguish between trustworthy, suspect, and prohibited data. Traffic classification was made easier by using a database that had the IP addresses of 90 individuals from each of the three groups. This allowed the server to allow traffic from trustworthy users and certain users who displayed suspicious behaviour, but it blocked traffic from known malicious sources.

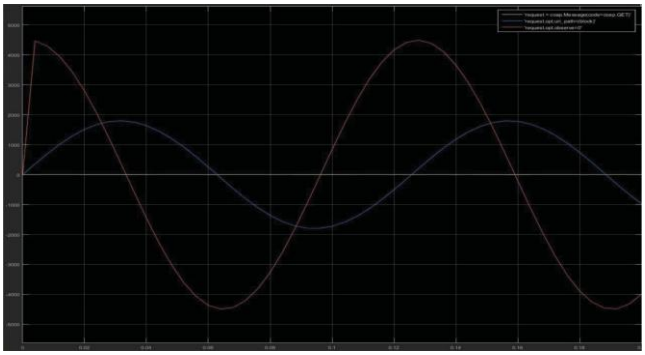

Fig 2. Simulation results (1 user, X axis : Number of Packets, Y-axis : Efficiency in bits/second)

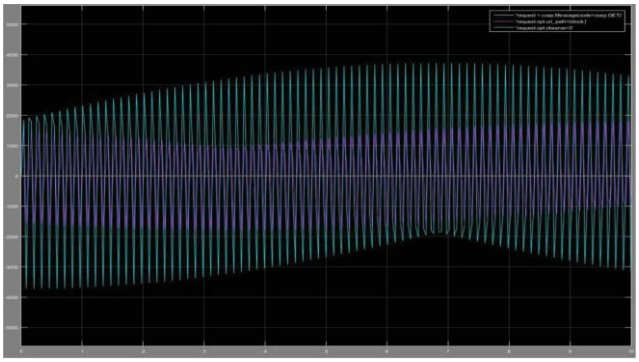

Fig. 5. Simulation results (30 users, X axis : Number of packets, Y axis : Number of users)

Figure 4 and Table 1 provided further details on these outcomes, showcasing the TP server's profidfs iency with traffic filtering and categorization.

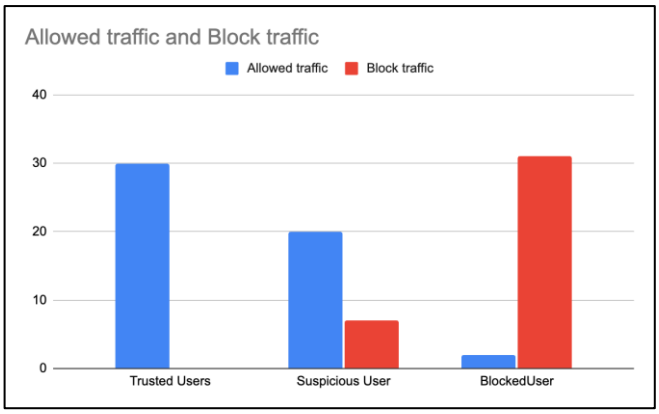

Fig. 6.FTP server-blocked and permitted traffic

Additionally, very infrequent instances of false positives and false negatives are revealed by the study. In particular, the server successfully recognised all 30 trustworthy users, with just a slight disparity of 3 individuals between the suspicious organizations that were discovered. Still, the algorithm remained resilient since the server correctly categorized them as prohibited users. As shown in the accompanying data, the resultant false positive percentage in the categorization of suspicious and blocked users was around 7%. Furthermore, a false negative rate of 6.45% was recorded for traffic filtering.

TABLE V. Results of TP server detection

	Trusted users	**Suspicious users**	**Blocked users**	**Total**
Defined	30	30	30	90
Server classification	30	27	33	90
Classification false positives	0%	0%	10%	6.66%
Classification false negative	0%	10%	0%	6.66%
Allowed traffic	30	20	2	52
Blocked traffic	0	7	31	38
False negative	0%	0%	0%	0%
False positive	0%	0%	6.45%	6%

8. Future Directions

CoAP Developments: Predicting Future Trends and Their Effect on DDoS Mitigation.

In order to improve CoAP's effectiveness in reducing DDoS assaults inside IoT ecosystems, it is possible to anticipate CoAP's future and provide prospective remedies to its current

limits [59]. Real-time updates are not possible, although it is possible to speculate about potential CoAP developments that could impact DDoS mitigation [60].

- Enhanced Security Mechanisms: CoAP's future versions may focus on bolstering its security features so they can better fend off DDoS assaults. To strengthen the protocol's resistance to several DDoS attack routes, this might include strong authentication, improved access control mechanisms, enhanced token management, and further security enhancements.
- CoAP-based DDoS mitigation approaches standardization: As the IoT environment develops, efforts may be made to standardize CoAP-based DDoS mitigation methods. This might lead to the creation of the best procedures and guidelines for establishing CoAP gateways, proxies, and other middlemen as specific DDoS mitigation strata.
- Prototyping for Enhanced Resilience: Future versions of CoAP may include improvements aimed at bolstering the protocol's resistance to DDoS attacks. This might entail strategies to reduce amplification vulnerabilities, improve management of scenarios involving resource depletion, and enable improved control of large-scale CoAP request inundations.
- Adaptive Traffic Management: Future CoAP implementations may include adaptive traffic management components that dynamically adjust the processing of incoming requests in accordance with the volume of traffic that is currently present. This flexibility could increase the ability of IoT ecosystems to deal with different DDoS assault intensities.
- Integration with machine learning and artificial intelligence: As CoAP develops, it may include methods from both fields to stop DDoS attacks. CoAP devices and proxies might be given the tools they need to more effectively detect and mitigate emerging DDoS attacks with the help of AI-guided anomaly detection and behavioral analysis.
- Cloud-Based DDoS Protection Service Integration: Cloud-based DDoS protection services may be used in the future by IoT installations managed by CoAP for more intricate attack detection and mitigation. This combination might relieve the resource-intensive duty of DDoS mitigation from IoT devices by offloading it to specialized suppliers.
- DDoS mitigation profiles standardization: Imagine standardization organizations and IoT industry associations creating DDoS mitigation profiles that are particular to CoAP. These profiles would detail the necessary security configurations and protocols required for a reliable defense of CoAP deployments.
- Industry Synergy and Research: Industry stakeholders, cybersecurity researchers, and standardization bodies will probably collaborate to make the anticipated advancements in CoAP and its integration with DDoS mitigation. Cohesive initiatives should result in increasingly effective and widely used CoAP-based DDoS mitigation techniques.

9. Conclusion

Overall, this study highlights CoAP's potential as a Distributed Denial of Service (DDoS) mitigation paradigm in the context of Internet of Things (IoT) ecosystems. While CoAP's simplified architectural characteristics provide inherent benefits for devices with limited resources, the corresponding limitation in its security mechanisms makes it vulnerable to possible flaws. In order to strengthen its security defenses against the wide range of DDoS attacks, CoAP's security mechanisms must be continuously explored and innovatively engaged. The CoAP protocol's robust and impermeable properties play a crucial role in protecting and strengthening linked devices and networks against the serious threat of DDoS onslaughts as the IoT development trajectory advances.

Acknowledgements

This research was supported/partially supported by Charotar University of Science and Technology. We thank our colleagues from Devang Patel Institute of Advance Technology and Research who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. We thank Dr. Amit Nayak for assistance with IoT networks, and for comments that greatly improved the manuscript.

Author contributions

Radhika Patel: Data curation, Writing-Original draft preparation, Software, Validation., Field study

Dr Amit Nayak: Conceptualization, Methodology, Software, Field study

Raj Bhatia: Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Matta, P., & Pant, B. (2019). Internet of things: Genesis, challenges and applications. Journal of Engineering Science and Technology, 14(3), 1717-1750.

[2] Vermesan, O., Friess, P., Guillemin, P., Sundmaeker, H., Eisenhauer, M., Moessner, K., ... & Cousin, P. (2022). Internet of things strategic research and

innovation agenda. In Internet of things (pp. 7-151). River Publishers.

[3] Babayigit, B., & Abubaker, M. (2023). Industrial internet of things: A review of improvements over traditional scada systems for industrial automation. IEEE Systems Journal.

[4] Hao, X., Ren, W., Fei, Y., Zhu, T., & Choo, K. K. R. (2022). A blockchain-based cross-domain and autonomous access control scheme for internet of things. IEEE Transactions on Services Computing, 16(2), 773-786.

[5] Greengard, S. (2021). The internet of things. MIT press.

[6] Cvitić, I., Peraković, D., Periša, M., & Botica, M. (2018, December). Smart home IoT traffic characteristics as a basis for DDoS traffic detection. In 3rd EAI International Conference on Management of Manufacturing Systems.

[7] Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. Internet of Things and Cyber-Physical Systems.

[8] Margam, R. (2024). SMART INHALERS: HARNESSING IOT FOR PRECISE ASTHMA MANAGEMENT. International Education and Research Journal, 10.

[9] Bibri, S. E., Krogstie, J., Kaboli, A., & Alahi, A. (2024). Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. Environmental Science and Ecotechnology, 19, 100330.

[10] Khan, A., Hassan, M., & Shahriyar, A. K. (2023). Optimizing onion crop management: A smart agriculture framework with iot sensors and cloud technology. Applied Research in Artificial Intelligence and Cloud Computing, 6(1), 49-67.

[11] Oladimeji, D., Gupta, K., Kose, N. A., Gundogan, K., Ge, L., & Liang, F. (2023). Smart transportation: an overview of technologies and applications. Sensors, 23(8), 3880.

[12] Gunnarsson, M. (2023). Efficient Security Protocols for Constrained Devices. Department of Electridal and Information Technology, Faculty of Engineering,? LTH, Lund University.

[13] Rana, B., Singh, Y., & Singh, P. K. (2021). A systematic survey on internet of things: Energy efficiency and interoperability perspective. Transactions on Emerging Telecommunications Technologies, 32(8), e4166.

[14] Chiu, Y. H., Liao, C. F., & Chen, K. (2021, August). Transparent web of things discovery in constrained networks based on mDNS/DNS-SD. In 2021 International Conference on Platform Technology and Service (PlatCon) (pp. 1-6). IEEE.

[15] Bayılmış, C., Ebleme, M. A., Çavuşoğlu, Ü., Kücük, K., & Sevin, A. (2022). A survey on communication protocols and performance evaluations for Internet of Things. Digital Communications and Networks, 8(6), 1094-1104.

[16] Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). A survey on IoT platforms: Communication, security, and privacy perspectives. Computer Networks, 192, 108040.

[17] Valdovinos, I. A., Millán, P. E. F., Guerrero-Ibáñez, J. A., & Valdez, R. E. C. (2024). Design, Implementation and Evaluation of an Embedded CoAP Proxy Server for 6LoWPAN. IEEE Access.

[18] Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. Security and Privacy, 6(6), e318.

[19] Al-Masri, E., Kalyanam, K. R., Batts, J., Kim, J., Singh, S., Vo, T., & Yan, C. (2020). Investigating messaging protocols for the Internet of Things (IoT). IEEE Access, 8, 94880-94911.

[20] Oliver, S. G., & Purusothaman, T. (2022). Lightweight and Secure Mutual Authentication Scheme for IoT Devices Using CoAP Protocol. Computer Systems Science & Engineering, 41(2).

[21] Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors, 22(3), 1094.

[22] Syaifuddin, S., Kusumawardani, S. S., & Widyawan, W. (2024). Tackling DDOS Attacks in IoT: Asynthesis of Literature 2018 to 2022. International Journal of Intelligent Systems and Applications in Engineering, 12(1), 802-809.

[23] Using a multicast group and short CoAP requests with fictitious source addresses, the attackers leverages CoAP's multicast communication feature to send traffic towards the target that is amplified significantly because all devices in the group respond to the victim.

[24] Al-Masri, E., Kalyanam, K. R., Batts, J., Kim, J., Singh, S., Vo, T., & Yan, C. (2020). Investigating messaging protocols for the Internet of Things (IoT). IEEE Access, 8, 94880-94911.

[25] Zhao, Q., Shu, L., Li, K., Ferrag, M. A., Liu, X., & Li, Y. (2024). Security and Privacy in Solar Insecticidal

Lamps Internet of Things: Requirements and Challenges. IEEE/CAA Journal of Automatica Sinica, 11(1), 58-73.

[26] Mengistu, T. M., Kim, T., & Lin, J. W. (2024). A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning. Sensors, 24(3), 968.

[27] Salas, J. (2021). IoTFC: A Secure and Privacy Preserving Architecture for Smart Buildings.

[28] Gill, S. S., Wu, H., Patros, P., Ottaviani, C., Arora, P., Pujol, V. C., ... & Buyya, R. (2024). Modern computing: Vision and challenges. Telematics and Informatics Reports, 100116.

[29] Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. R. (2024). A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. Future Internet, 16(2), 40.

[30] Hintaw, A. J., Manickam, S., Aboalmaaly, M. F., & Karuppayah, S. (2023). MQTT vulnerabilities, attack vectors and solutions in the internet of things (IoT). IETE Journal of Research, 69(6), 3368-3397.

[31] Gupta, B. B., & Dahiya, A. (2021). Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures. CRC press.

[32] Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. The Journal of Supercomputing, 76, 5320-5363.

[33] Batmaz, B., & Doğan, A. (2021). CoAP acceleration on FPSoC for resource constrained Internet of Things devices. IEEE Internet of Things Journal, 8(24), 17790-17801.

[34] Bhardwaj, A., Mangat, V., Vig, R., Halder, S., & Conti, M. (2021). Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. Computer Science Review, 39, 100332.

[35] Trajanovski, T., & Zhang, N. (2021). An automated and comprehensive framework for IoT botnet detection and analysis (IoT-BDA). IEEE Access, 9, 124360-124383.

[36] Ahvanooey, M. T., Zhu, M. X., Li, Q., Mazurczyk, W., Choo, K. K. R., Gupta, B. B., & Conti, M. (2021). Modern authentication schemes in smartphones and IoT devices: An empirical survey. IEEE Internet of Things Journal, 9(10), 7639-7663.

[37] Bhattacharjya, A., Zhong, X., Wang, J., & Li, X. (2020). CoAP—application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP. Digital twin technologies and smart cities, 151-175.

[38] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors, 23(8), 4117.

[39] Abubakar, R., Aldegheishem, A., Majeed, M. F., Mehmood, A., Maryam, H., Alrajeh, N. A., ... & Jawad, M. (2020). An effective mechanism to mitigate real-time DDoS attack. IEEE Access, 8, 126215-126227.

[40] MAHRACH, S., & HAQIQ, A. (2020). DDoS flooding attack mitigation in software defined networks. International Journal of Advanced Computer Science and Applications, 11(1).

[41] Uwaezuoke, E. C. (2022). Analysis of power line communication network vulnerabilities using cyber security techniques (Doctoral dissertation, University of Johannesburg).

[42] Belgaum, M. R., Musa, S., Alam, M. M., & Su'ud, M. M. (2020). A systematic review of load balancing techniques in software-defined networking. IEEE Access, 8, 98612-98636.

[43] Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal, 7(8), 6882-6897.

[44] Yang, N., Chen, K., & Wang, M. (2021). SmartDetour: Defending blackhole and content poisoning attacks in IoT NDN networks. IEEE Internet of Things Journal, 8(15), 12119-12136.

[45] El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering, 29(1), 223-246.

[46] Husnain, M., Hayat, K., Cambiaso, E., Fayyaz, U. U., Mongelli, M., Akram, H., ... & Shah, G. A. (2022). Preventing mqtt vulnerabilities using iot-enabled intrusion detection system. Sensors, 22(2), 567.

[47] Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors, 22(3), 1094.

[48] Chaganti, R., Bhushan, B., & Ravi, V. (2023). A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions. Computer Communications, 197, 96-112.

[49] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors, 23(8), 4117.

[50] Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. IEEE Internet of things Journal, 1(3), 265-275.

[51] Dutta, M., & Granjal, J. (2020). Towards a secure Internet of Things: A comprehensive study of second line defense mechanisms. IEEE Access, 8, 127272-127312.

[52] Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., ... & Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET communications, 16(5), 421-432.

[53] Kumar, A., Sharma, S., Goyal, N., Singh, A., Cheng, X., & Singh, P. (2021). Secure and energy-efficient smart building architecture with emerging technology IoT. Computer Communications, 176, 207-217.

[54] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. Sensors, 23(8), 4117.

[55] Khalil, K., Elgazzar, K., Abdelgawad, A., & Bayoumi, M. (2020, June). A security approach for CoAP-based internet of things resource discovery. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT) (pp. 1-6). IEEE.

[56] Kumar, P. M., & Gandhi, U. D. (2020). Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. The Journal of Supercomputing, 76, 3963-3983.

[57] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., & Watsen, K. (2021). Bootstrapping remote secure key infrastructures (BRSKI). RFC 8995.

[58] Sara, A., & Randa, J. (2024, February). Data protection in IoT using CoAP based on enhanced DTLS. In AIP Conference Proceedings (Vol. 2729, No. 1). AIP Publishing.

[59] Swamy, S. N., & Kota, S. R. (2020). An empirical study on system level aspects of Internet of Things (IoT). IEEE Access, 8, 188082-188134.

[60] Rehman, S. U., Manickam, S., & Firdous, N. F. (2023, June). Impact of DoS/DDoS attacks in IoT environment: A study. In AIP Conference Proceedings (Vol. 2760, No. 1). AIP Publishing.