Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

5th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2024)

SEPTEMBER 5-6th, 2024

Role of PKI in Securing AMQP Communication

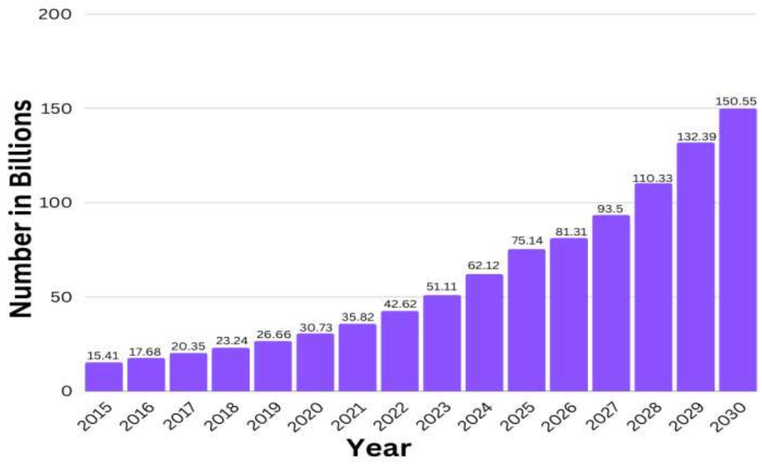
Dr. Sanjay Adiwal, S Shuaib Ahmed, Dr. Balaji Rajendran, Dr. Mohammed Misbahuddin, and Dr. S D Sudarsan

AGENDA

- Introduction
- Security Threats in AMQP
  - Dictionary Attack
  - DoS Attack
  - MitM Attack
- Role of PKI for AMQP Security
- Challenges in Security of IoT with AMQP
- Conclusion

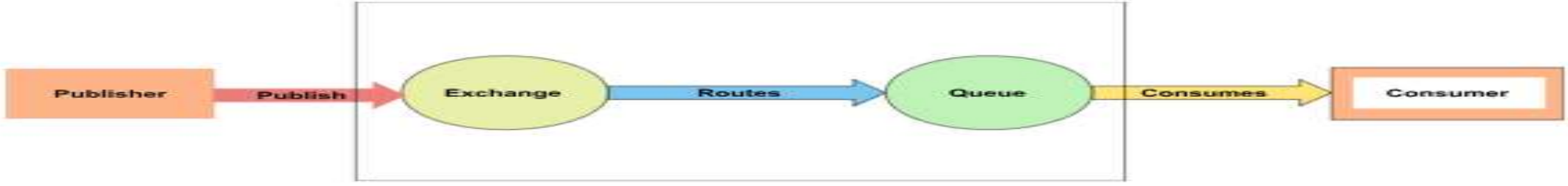
Introduction – IoT

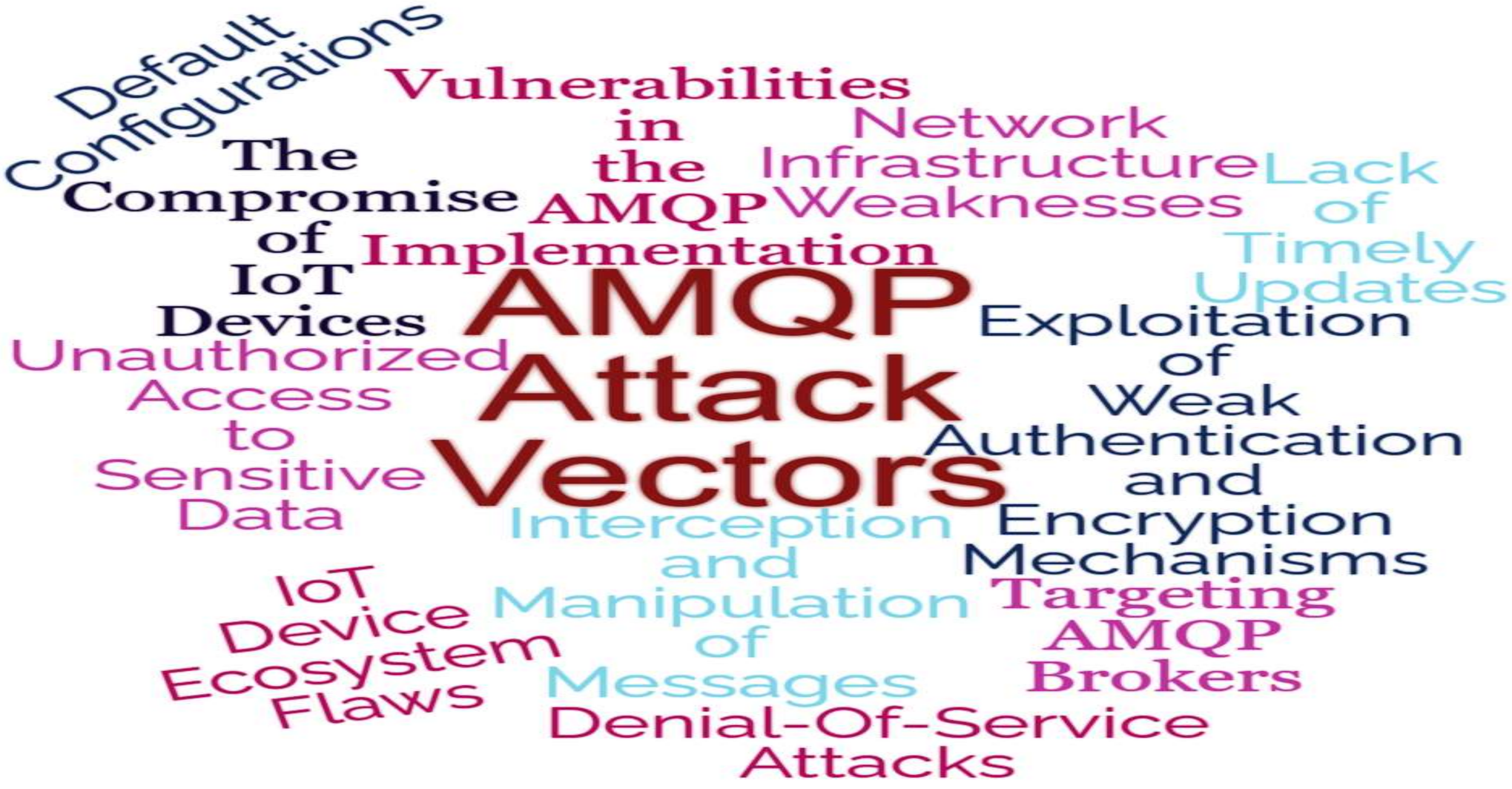
- The way Internet has reformed the world, we can hardly envisage our lives without it.
- We are living in the era where various objects across the globe are connected to the Internet.
- These objects are uniquely identifiable and can sense, actuate, and communicate without human intercession.
- According to recent estimates, there are approximately 62 billion IoT devices in the world today, outnumbering humans.
- By some estimates, the number of connected devices in the world will surpass 150 billion by the year 2030.
- Approximately 30 years after the birth of IoT, society is confronted with significant challenges regarding IoT security.



Advanced Messaging Queueing Protocol - AMQP

- Application Layer Protocols - Device to Device Communication
- HTTP, CoAP, MQTT, AMQP etc.
- AMQP is also a communication protocol designed specifically for IoT, which uses Publish/Subscribe massaging as its core.
- Publisher emits massages to Exchange
- Consumer receives massages from the queue
- Binding connects an exchange with a queue using binding key
- Exchange compares the routing key with binding key



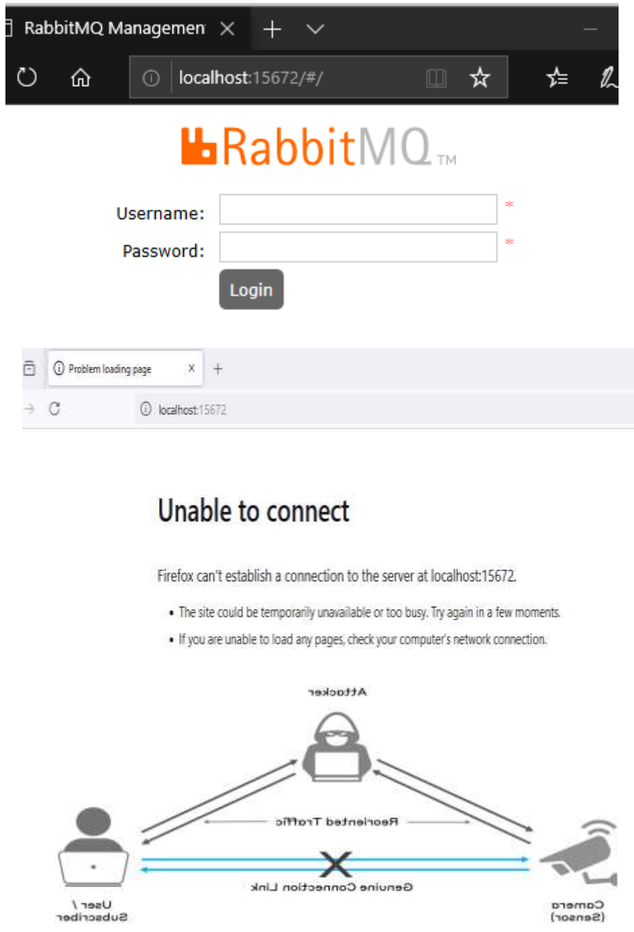

Default Configurations
Vulnerabilities in the AMQP Implementation
Network Infrastructure Weaknesses
Lack of Timely Updates
The Compromise of IoT Devices
AMQP
Attack
Vectors
Exploitation of Weak Authentication and Encryption Mechanisms
Unauthorized Access to Sensitive Data
Interception and Manipulation of Messages
Targeting AMQP Brokers
IoT Device Ecosystem Flaws
Denial-Of-Service Attacks

Attacks on AMQP

- **Dictionary Attack**
  - **Involves systematically trying of potential credentials from a pre-defined list to gain unauthorized access to the messaging broker. This type of attack exploits weak or default passwords to compromise the RabbitMQ server and potentially intercept or manipulate messages.**

- **Denial of Service – DoS**
  - **Targets the messaging broker by overwhelming it with excessive traffic or resource-intensive operations, causing it to become unresponsive or crash.**

- **Man in the Middle – MitM**
  - **Involves intercepting and potentially altering messages exchanged between Broker and the Publisher, compromising data integrity and confidentiality.**



Dictionary Attack

- Scanning of AMQP on connected device
- Version grabbing of RabbitMQ Server

```
PORT     STATE SERVICE VERSION
5672/tcp open  amqp    RabbitMQ 3.9.13 (0-9)
```

- Generate a Dictionary and perform an attack

```
└─$ sudo python dictionaryAttack.py
[+] Success: User: sammy ── Password: sammy
[+] Success: User: user ── Password: user
[+] Success: User: kali ── Password: kali
[+] Success: User: user ── Password: user
Dictionary Attack finished
```

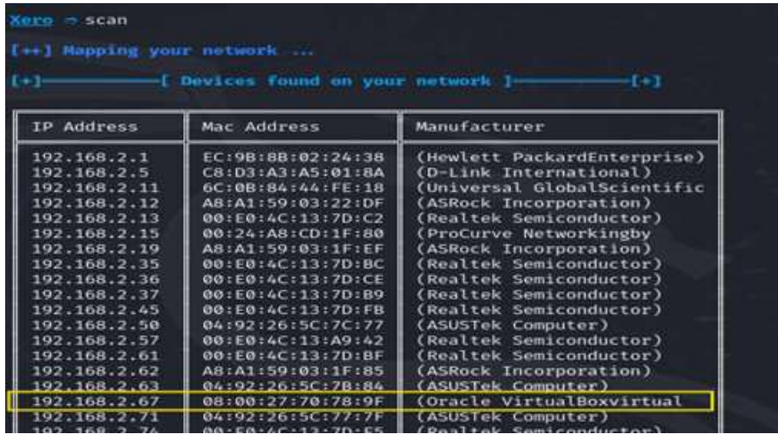
```
└─$ nmap -p- 192.168.2.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 20
Nmap scan report for 192.168.2.67
Host is up (0.00017s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE
1883/tcp  open  mqtt
4369/tcp  open  epmd
5672/tcp  open  amqp
15672/tcp open  unknown
25672/tcp open  unknown
```

```python
import pika

target = "192.168.2.67"
user_list = "/home/kali/userlist.txt"
pass_list = "/home/kali/passwd.txt"

with open(user_list, "r") as ins:
    for username in ins:
        with open(pass_list, "r") as ins:
            for password in ins:
                username = username.rstrip()
                password = password.rstrip()
                credentials = pika.PlainCredentials(username, password)
                parameters = pika.ConnectionParameters(target, 5672, '/', credentials)
                try:
                    connection = pika.BlockingConnection(parameters)
                    print("[+] Success: User: " + username + " ── Password: " + password)
                except Exception as e:
                    continue

print("Dictionary Attack finished")
```

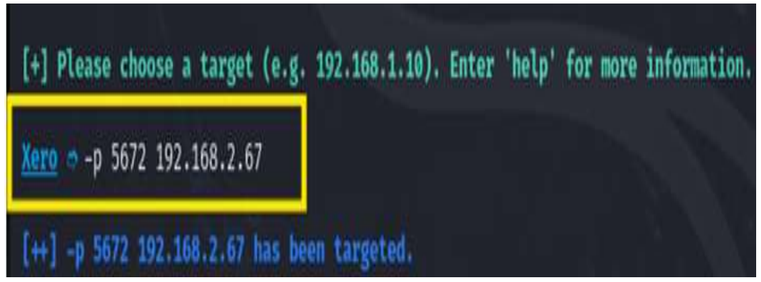
DoS Attack on AMQP

- Launch Xerosploit Tool

- Scan for Devices in the Network



- Set the Target

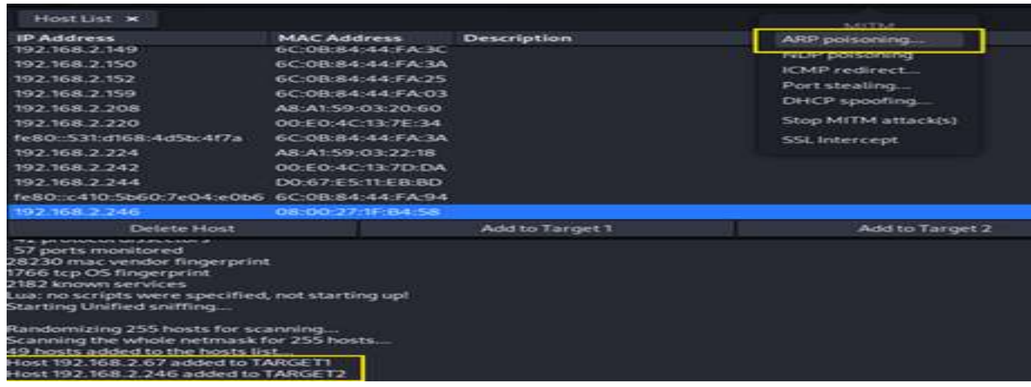


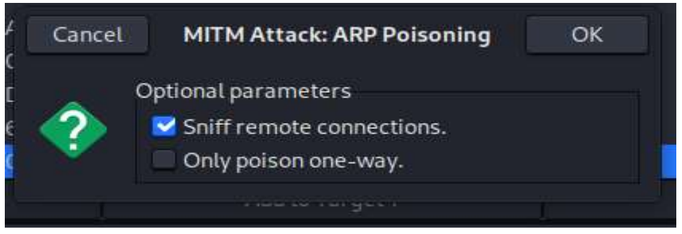
- Access module information and select the DoS module

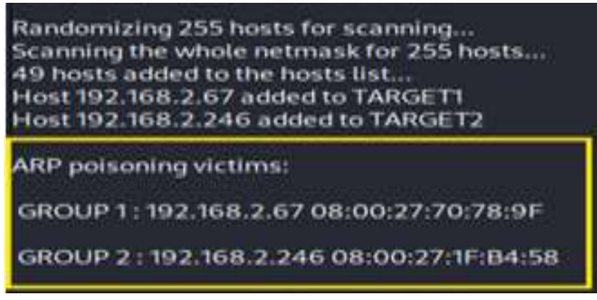
- The RabbitMQ server has stopped responding. A total of 1,91,00,189 packets were transmitted to the targeted IP address. The DoS attack was successfully executed.

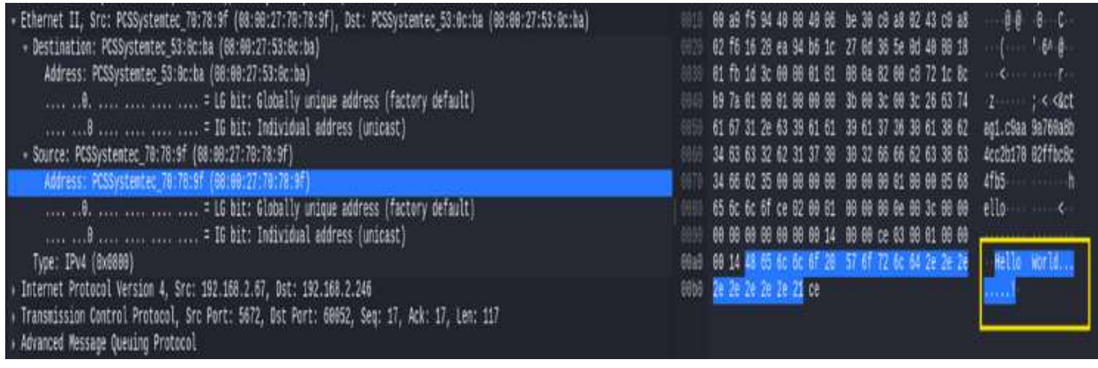
Man in the Middle Attack

- Man-in-the-Middle through ARP Poisoning on AMQP – Ettercap Tool on Kali Linux
- Target 1 and Target 2 are set to IP addresses 192.168.2.67 (AMQP server - Broker) and 192.168.2.24 (Publisher), respectively
- Adjust the optional parameters to "sniff remote connections" and click OK
- the ARP cache poisoning attack is successfully launched using the Ettercap tool. This attack intercepts all network traffic between the AMQP server (the Broker) and the Publisher.
- the Publisher's message to the Broker is seen, which says, "Hello World", compromising the integrity of the AMQP communication.









Role of PKI in AMQP Security

- Integrating PKI into the AMQP protocol significantly strengthens its authentication mechanisms, such as SASL and TLS.
- By incorporating digital certificates and cryptographic protocols, PKI provides a robust framework for verifying the identities of communicating entities.
- This ensures that only trusted parties can establish connections, thereby enhancing the overall security of the messaging system and safeguarding data integrity and confidentiality during transmission.
- Certificate-based authentication, where X.509 digital certificates verify the identities of brokers and clients, enhancing overall system security.
- TLS encrypts data exchanged between clients and servers, preventing unauthorized access and eavesdropping.
- SASL adds a layer of security by providing additional authentication mechanisms (such as Kerberos, NTLM, etc) that validate user credentials securely.

CHALLENGES IN SECURING IOT COMMUNICATION WITH AMQP

- Securing IoT communication using the AMQP presents several challenges due to the unique characteristics and requirements of IoT devices and networks.
- These devices often have limited processing power, memory, and battery life, making it hard to use strong security features like encryption and authentication without slowing down the device or draining the battery.
- Used in different and sometimes risky environments, which makes them more vulnerable to physical tampering or unauthorized access.
- Different devices from various manufacturers, each with its own level of capabilities and security. Managing security tasks like firmware updates, patching, and access control across this mix of devices can be challenging.

Conclusion

- This paper emphasizes the critical role of PKI in securing AMQP-based IoT communication.
- We have identified the attack vectors associated with AMQP, demonstrated several key attacks, and outlined how PKI can effectively mitigate these threats.
- Our analysis highlights how PKI is essential for safeguarding AMQP-based IoT communication against evolving threats, thereby strengthening the overall security and reliability of IoT ecosystems.

References

- [1] McAteer, Ian Noel, Muhammad Imran Malik, Zubair Baig, and Peter Hannay. "Security vulnerabilities and cyber threat analysis of the AMQP protocol for the internet of things." (2017).
- [2] Mabrouk, Tamer F. "An agent based approach to create an intelligent and autonomous operational con-cept for the internet of things." theme is: Humanitarian ICT (2018): 37.
- [3] Sethi, Pallavi, and Smruti R. Sarangi. "Internet of things: architectures, protocols, and applications." Journal of electrical and computer engineering 2017, no. 1 (2017): 9324035.
- [4] Rathod, Vishal J., and Mohit P. Tahiliani. "Geometric sequence technique for effective rto estimation in coap." In 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6. IEEE, 2020.
- [5] Rathod, Vishal J., Sanjana Krishnam, Ayush Kumar, Gauri Baraskar, and Mohit P. Tahiliani. "Effective RTO estimation using EIFEL retransmission timer in COAP." In 2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), pp. 1-6. IEEE, 2020.

References

- [6]Rathod, Vishal, and Mohit P. Tahiliani. "Geometric Series based effective RTO estimation Technique for CoCoA." Ad Hoc Networks 130 (2022): 102801.
- [7]Rizzardi, Alessandra, Sabrina Sicari, and Alberto Coen-Porisini. "Analysis on functionalities and security features of Internet of Things related protocols." Wireless Networks 28, no. 7 (2022): 2857-2887.
- [8]Altulaihan, Esra, Mohammed Amin Almaiah, and Ahmed Aljughaiman. "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions." Electronics 11, no. 20 (2022): 3330.
- [9]Nebbione, Giuseppe, and Maria Carla Calzarossa. "Security of IoT application layer protocols: Challenges and findings." Future Internet 12, no. 3 (2020): 55.
- [10] Xiong, Xuandong, and Jiandan Fu. "Active status certificate publish and subscribe based on AMQP." In 2011 International Conference on Computational and Information Sciences, pp. 725-728. IEEE, 2011.
- [11] Quadar, Nordine, Abdellah Chehri, Gwanggil Jeon, Mohammad Mehedi Hassan, and Giancarlo Fortino. "Cybersecurity issues of IoT in ambient intelligence (AmI) environment." IEEE Internet of Things Magazine 5, no. 3 (2022): 140-145.

THANK YOU