Encrypted Virtual Private Network in Secure Internet of Things Technology

- NIVETHITHA SUBASCHANDRA BOSE

- PRASHANT KRISHNAN IYER

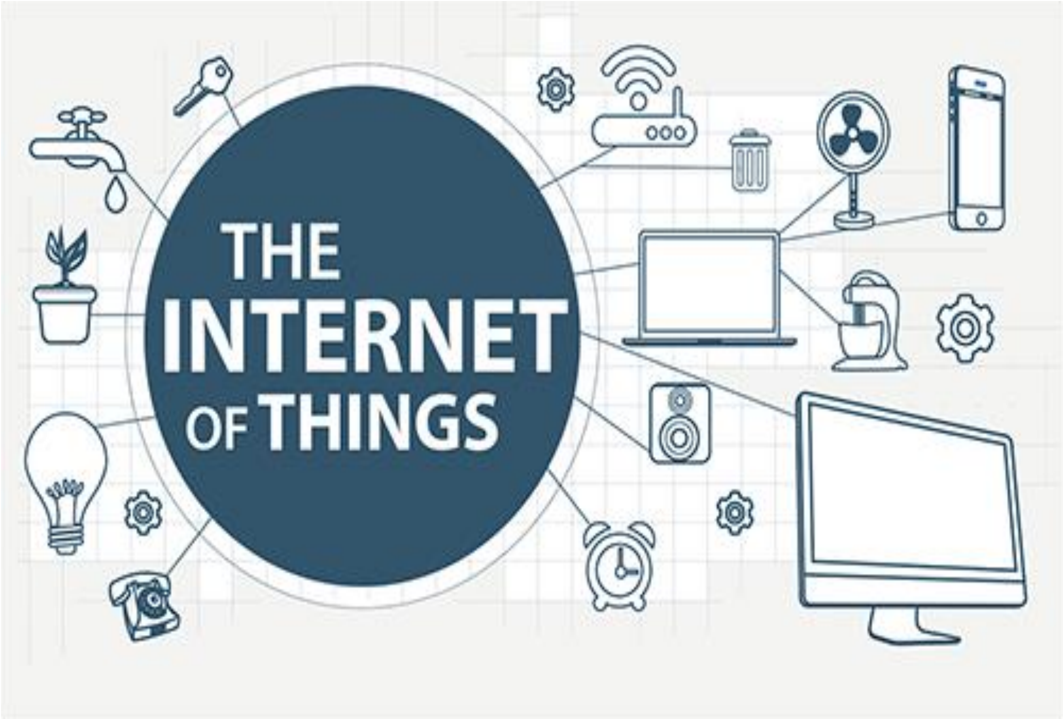
- RAJAPUTHRI MAHARAJA

WHAT IS IOT ???

INTERNET OF THINGS..

INTERNET OF THINGS !!!

- The Internet of Things introduces a vision of a future Internet where users, computing systems, and everyday objects cooperate seamlessly.
- IoT for short, is a new interconnection of technology heralded as the next industrial revolution—implying radical change, disruption, and an entirely new paradigm for the planet



Advantages

- **Safety, Comfort, Efficiency**

  Measuring and managing hazardous environments without putting people at risk, and optimizing all physical environments for comfort and productivity while controlling energy costs.

- **Better Decision Making**

  Analysing larger trends from empirical data, can make smarter decisions.

- **Revenue Generation**

  At first, the above benefits from the IoT will impact your bottom line simply by reducing expenses and improving efficiency.

  The IoT may be the "X factor" that gives many organizations a strategic advantage over the competitors in the next decade.

Challenges in IOT:

- **Sensing a complex environment:**

  Innovative ways to sense and deliver information from the physical world to the cloud.

- **Connectivity:**

  Variety of wired and wireless connectivity standards are required to enable different application needs.

- **Power:**

  Many IOT applications need to run for years over batteries and reduce the overall energy consumption.

- **Security is vital:**

  Protecting users privacy and manufacturers IP detecting and blocking malicious activity.

M2M Communication

- It forms the base of IoT Architecture.
- The end-devices usually form **Machine to Machine** (M2M) networks using various radio technologies, such as **ZigBee**, **Wi-Fi** and many more.
- **Advantages** :
  - Low Bandwidth
  - Low Upload biased traffic

MQTT

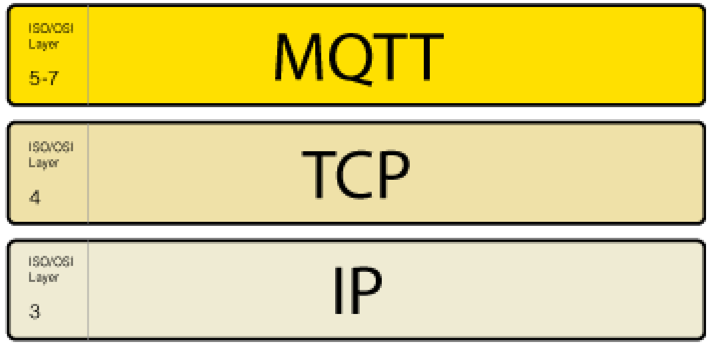
- What is **MQTT** ?
- **Message Queue Telemetry Transport** (MQTT) protocol is an extremely lightweight communication protocol that forms the base of M2M communicational architecture.
- It is a **publish/subscribe** messaging protocol unlike the request/response since messages need not be responded, thereby **reducing the network bandwidth**. MQTT ensures **high reliability** by providing Quality of Service at all levels.
- **Decoupling** of publisher and subscriber.

Advantages :

Low Latency

High Reliability

Reduced Network Bandwidth



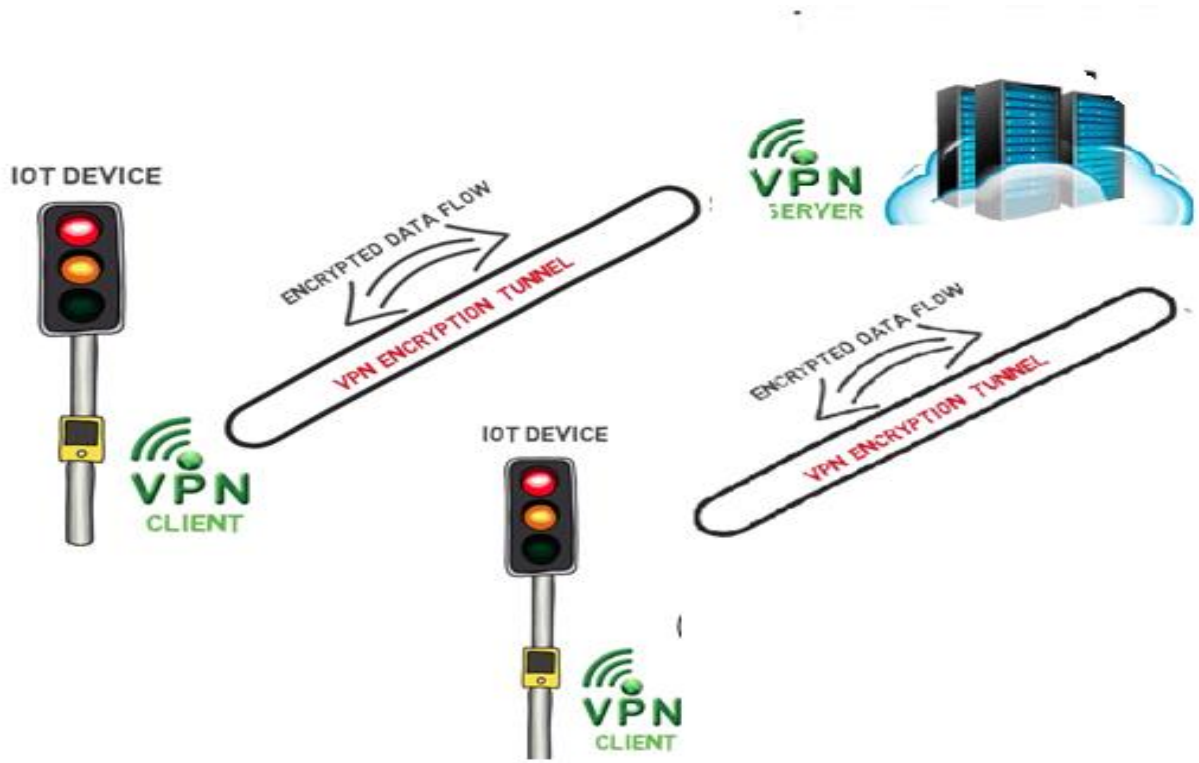
Virtual Private Networks (VPN):

- A **Virtual Private Networks** (VPN) allows you to connect to the internet via a server run by a VPN provider.
- In a VPN, the computers at each end of the tunnel encrypt the data entering the tunnel and decrypt it at the other end.
- However, a VPN needs more than just a pair of keys to apply encryption.
- The basic idea is to configure a “TLS/SSL” TCP port for the MQTT clients to use when connecting to the VPN.

Research Problem:

- Security In IoT Is Vital
- Some of the common techniques for security include
    - Encryption of data
    - Combination of different protocols.
    - Attacks possible are Man in the middle attack or Evesdropping.

Proposed Solution:

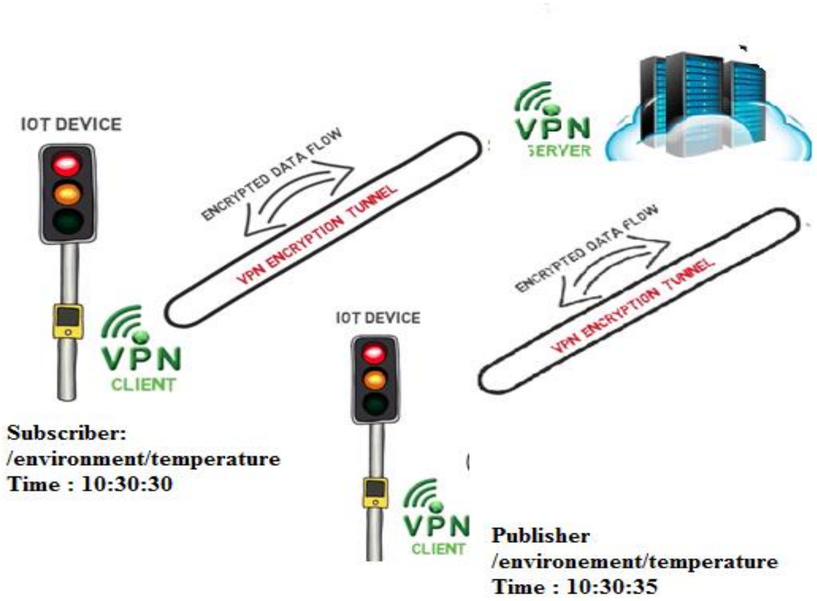


Proposed Solution:

- Setting up an **Encrypted VPN channelled infrastructure** for IoT.
- Our research aims in providing a detailed summary of the difference in Latency for the requests to get processed when the VPN server is set on the Raspberry-Pi versus on the cloud.
- The proposed system also aims in building up three models
  - A local MQTT server setup on a Raspberry-Pi.
  - A cloud MQTT server.
  - An Hybrid model in which higher order(in terms of processing speed and complexity) requests to be processed on the Raspberry-Pi and the requests with less overhead on the cloud.

Latency Calculation:

- Our Proposed System calculates **end-to-end Latency** (i.e.) the delay before a transfer of data begins following an instruction for its transfer.

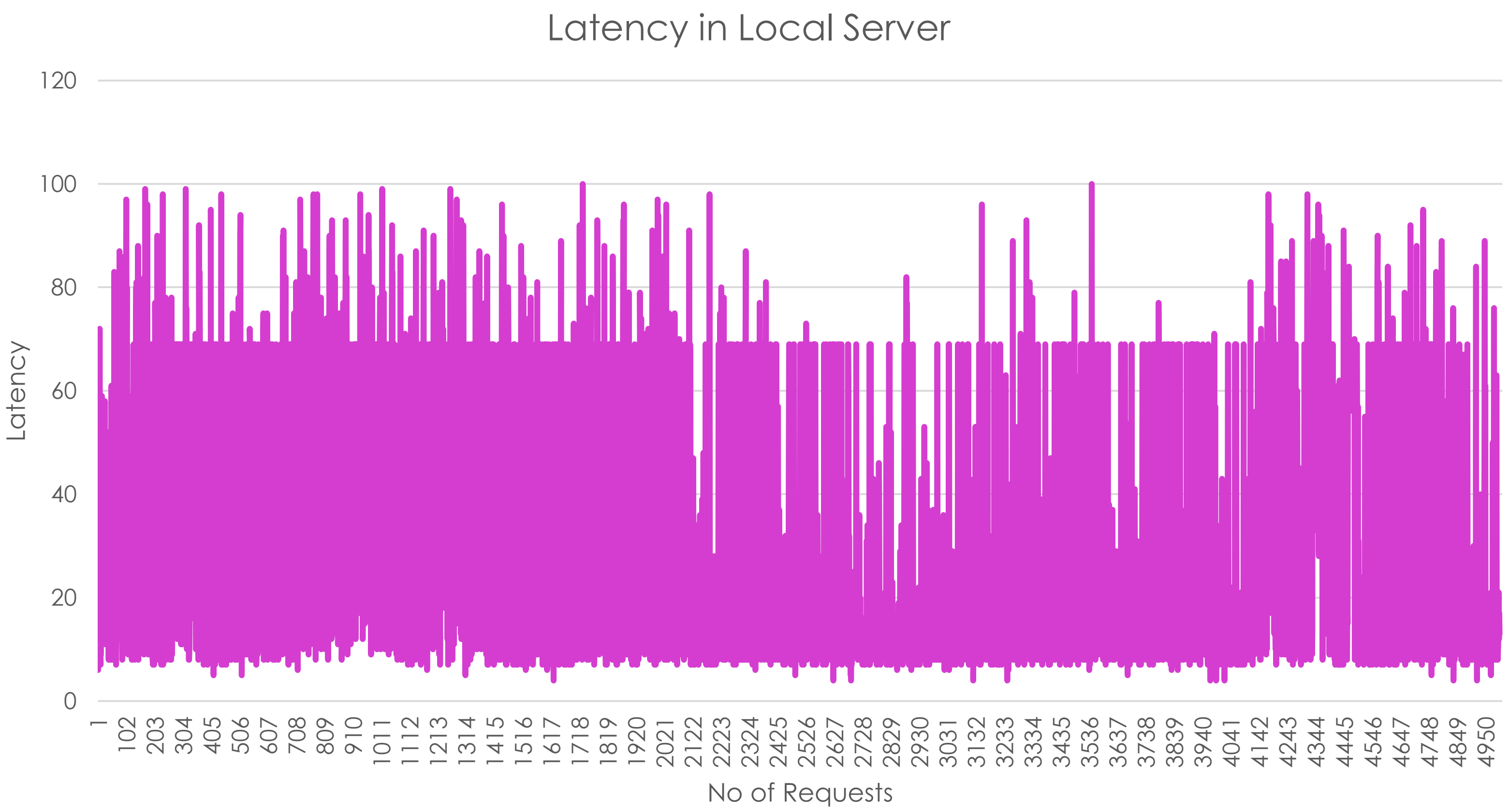


Subscriber:
/environment/temperature
Time : 10:30:30

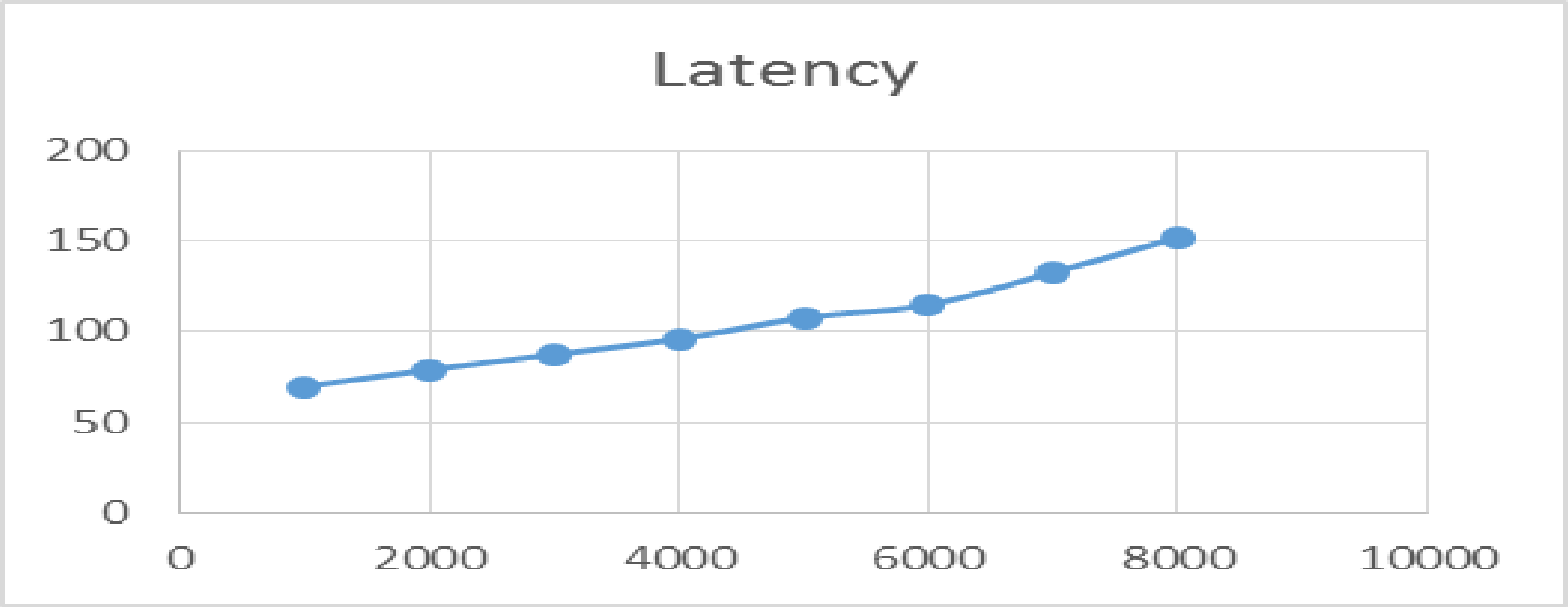
Publisher
/environement/temperature
Time : 10:30:35

```
{
    message_id = m
    topic = temperature
    temp
    {
        Celsius = c
        Fahrenheit = f
        publisher_time = t
    }
}
```

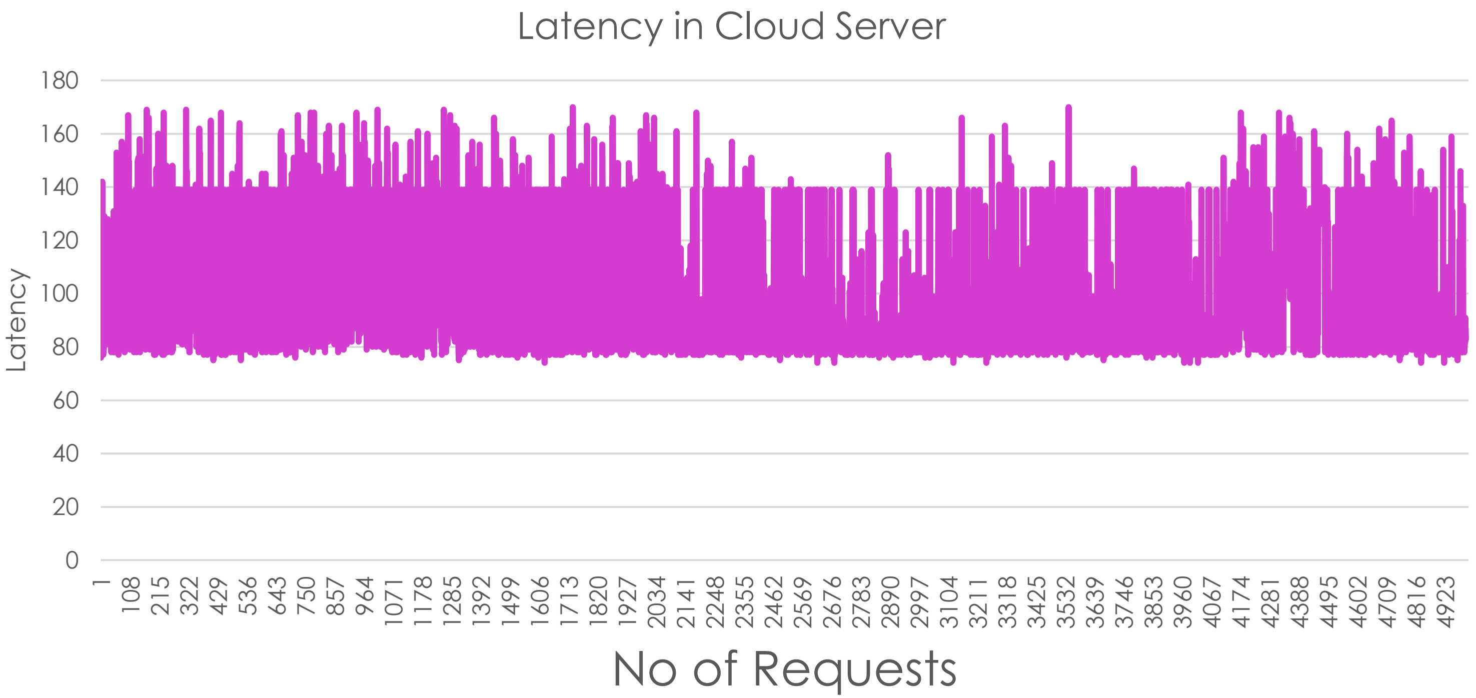
Latency Calculation in local server:



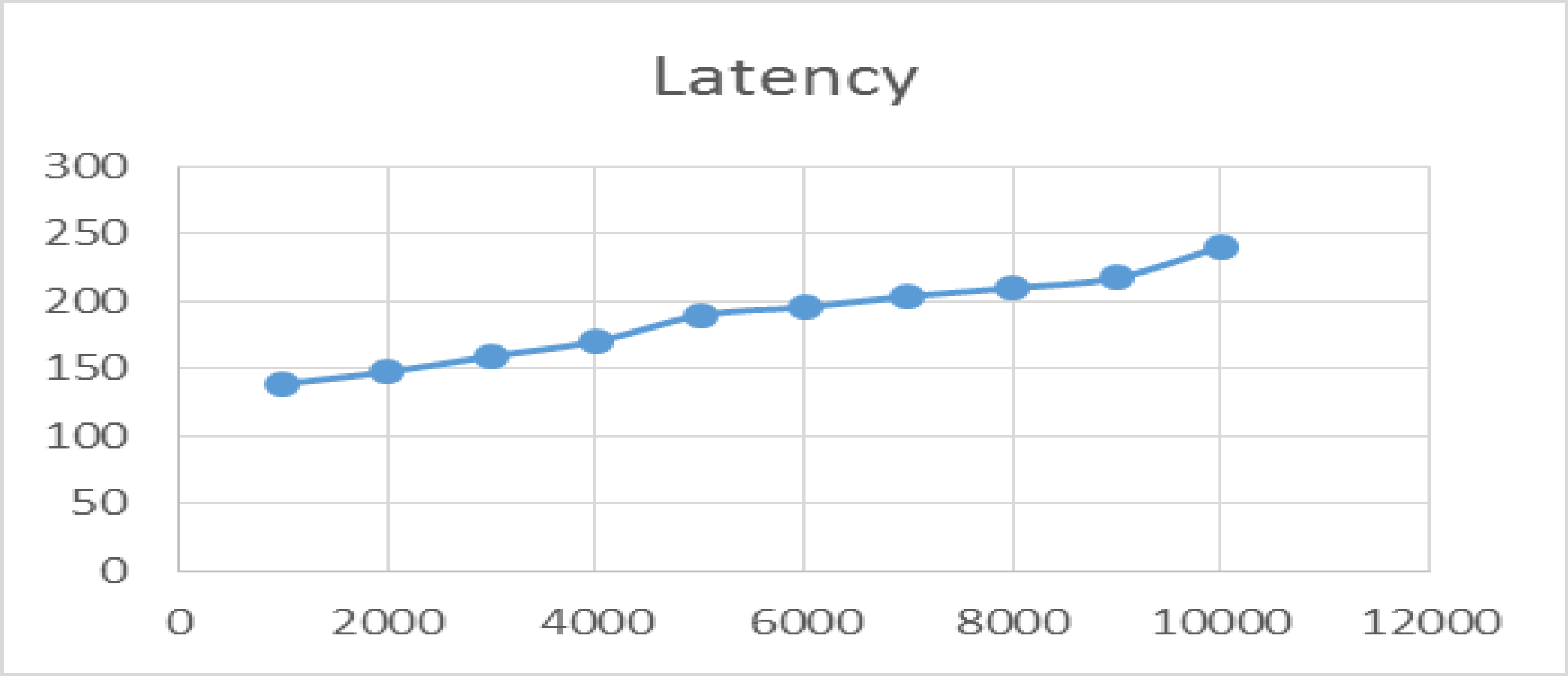
Latency Calculation in Local Server



Latency Calculation in cloud server:



Latency Calculation In Cloud Server



Bandwidth Calculation:

- Bandwidth is defined as the **ability to transfer data** (like Json, VOIP call) **from one point to another in a fixed amount of time**.
- The Bandwidth needed for data transmission in M2M communication depends on a few factors namely
  - Packet overhead.
  - Network Protocol used. (In this case MQTT,TCP-IP)
  - Overhead due to compression technologies if any used.

For Ex: If latency = 10ms (For one data packet request),100 such data packet requests are required to be transmitted every second. Each packet carries network protocol overheads.

Bandwidth Calculation:

- For Bandwidth calculation in M2M communication we also need to keep into account , the overhead of
  - MQTT of the data to be sent.
  - TCP to the MQTT packet.
  - TCP to the data sent.

And not taking into account , the connectivity, keep alive and many more aspects.

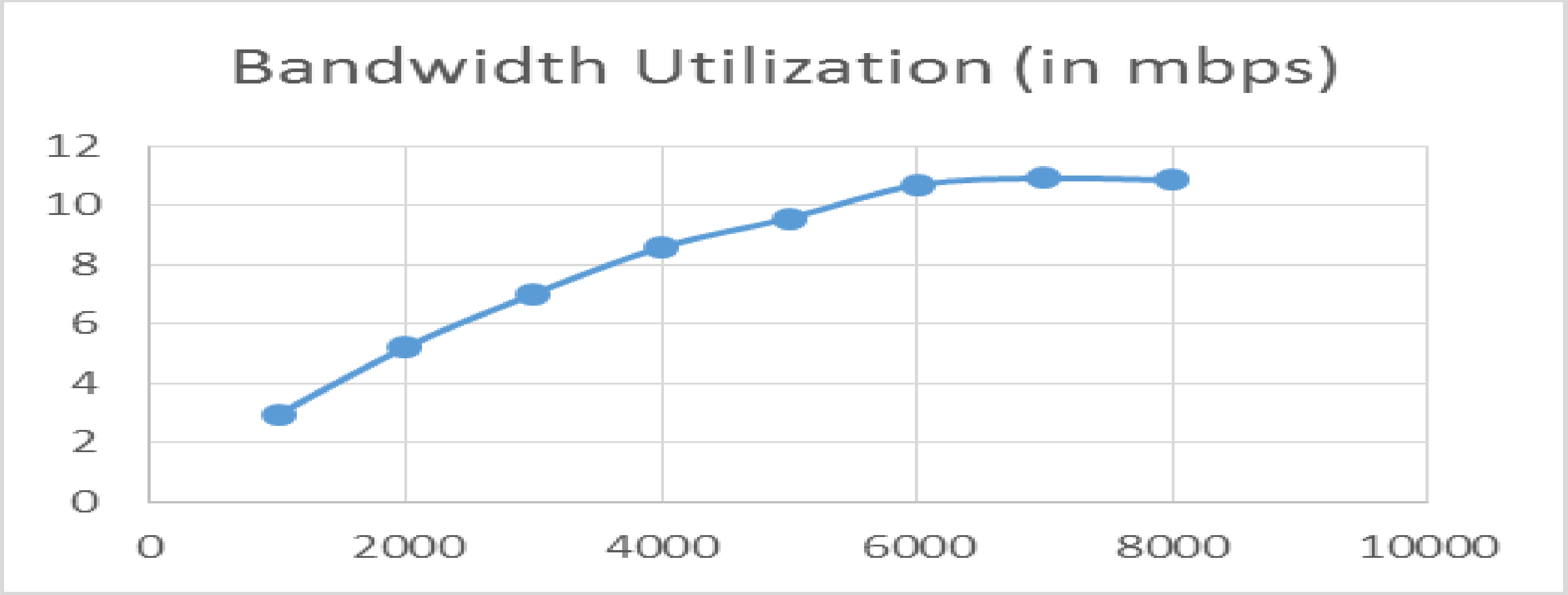
TCP/IP header size = 40 bytes.

For Instance 1) Data size = 1Byte

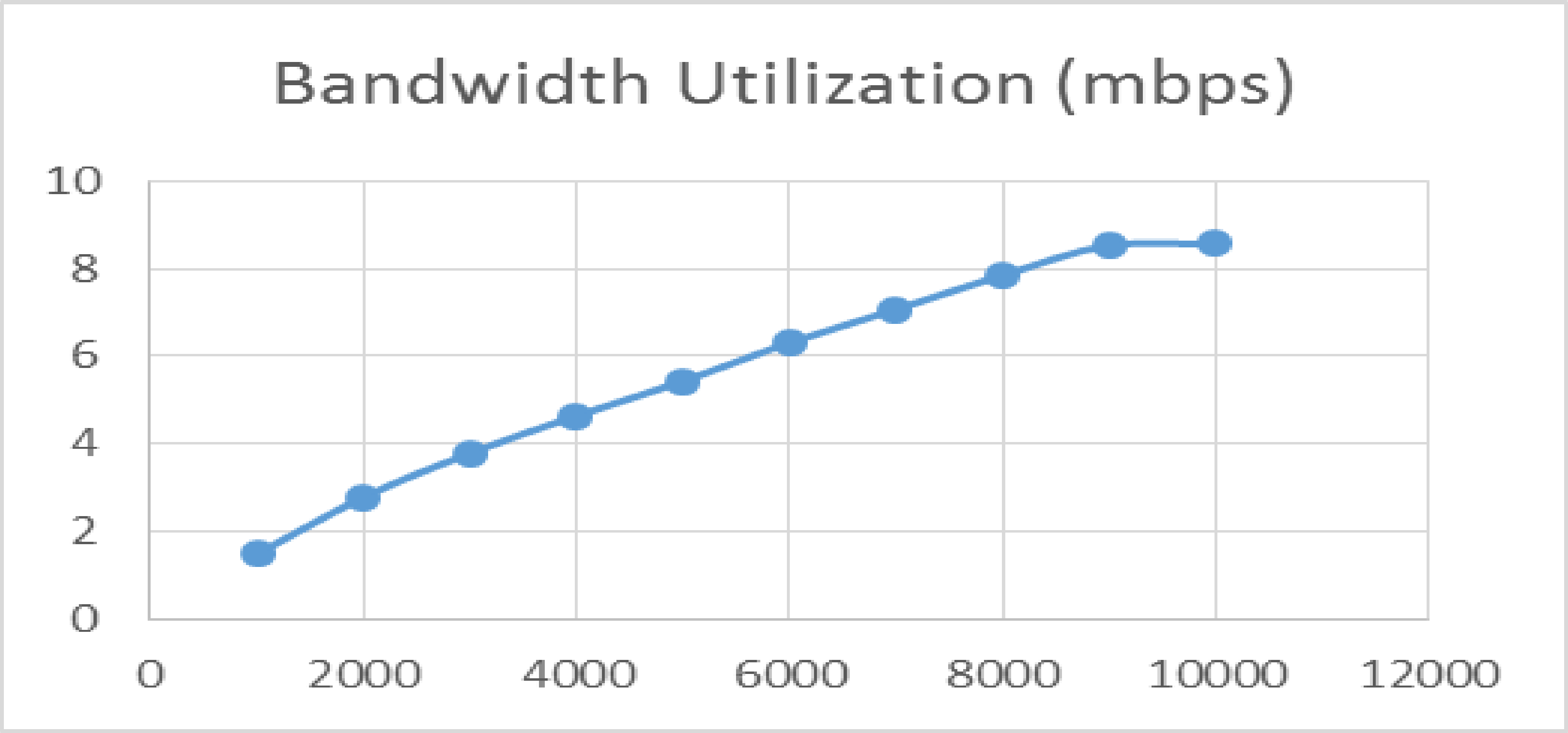
1Bytes * 40Bytes = 40Bytes = 4100% TCP/IP overhead

i.e **41Bytes** of data is actually transmitted ….

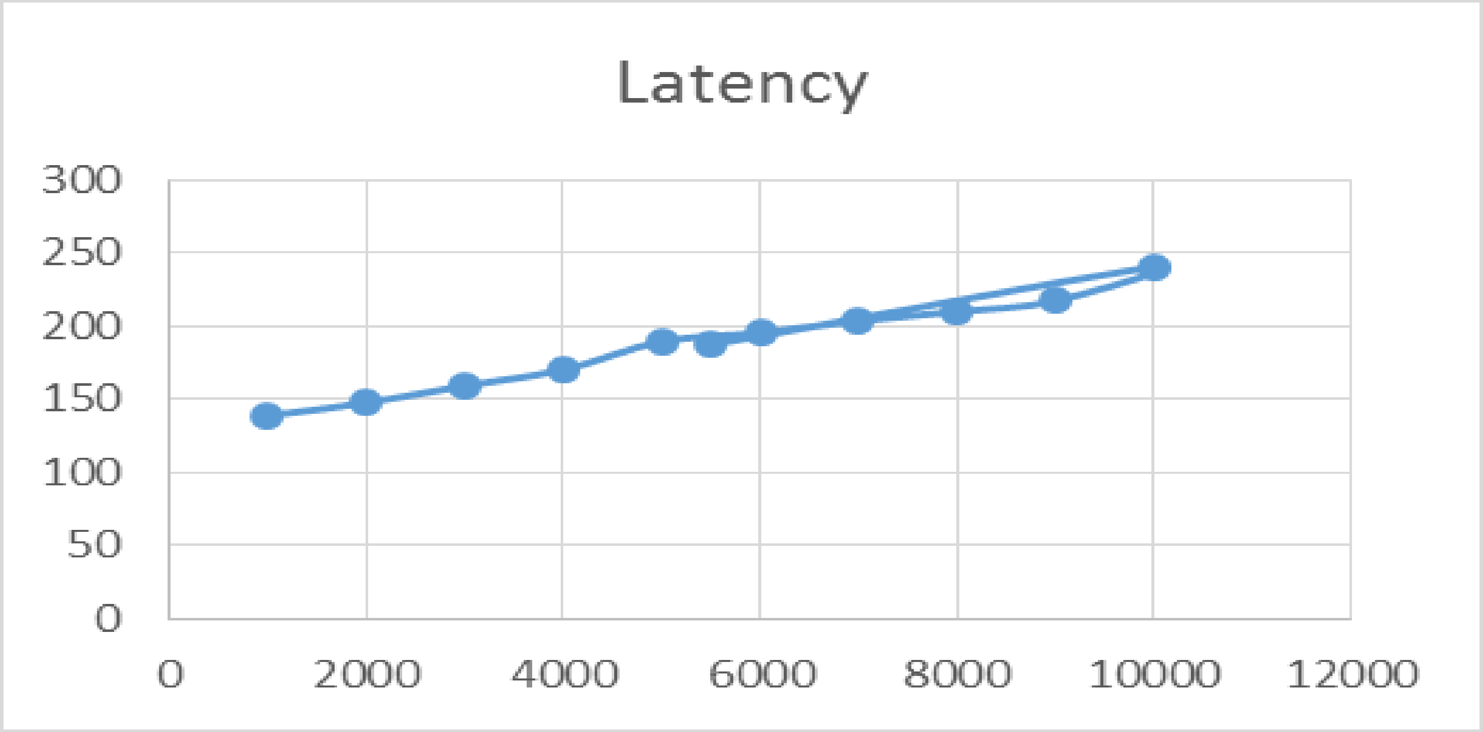
Bandwidth Utilization in Local Server



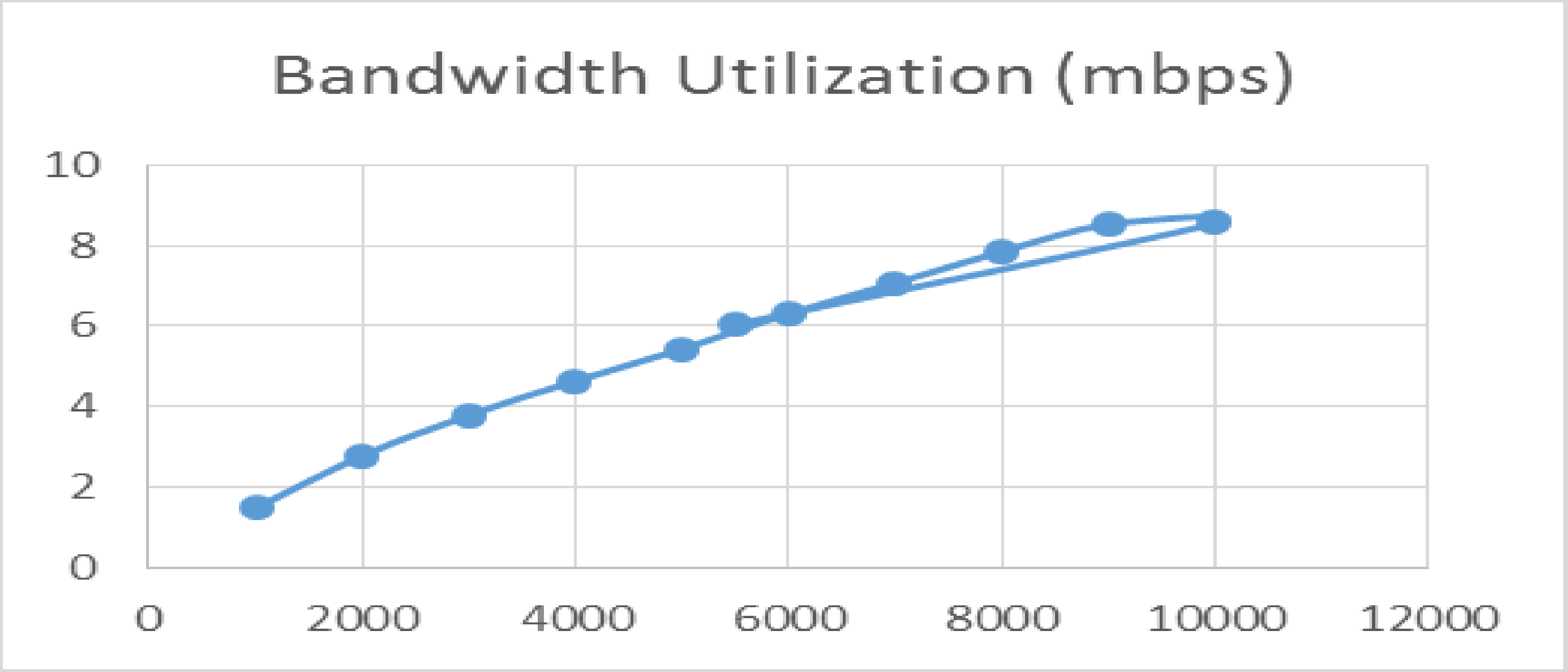
Bandwidth Calculation in Cloud Server



Latency Calculation in Hybrid Mode



Bandwidth Utilization In Hybrid Mode



CONCLUSION

- The model that our team has proposed is one of the best alternatives to
  - Existing security challenges
  - Secure IoT M2M communication
  - Bring in standardization of security principles to be implemented
  - Authentication of the clients participating in the communication
  - Cost effective security
  - Is Standalone executable on Windows, Mac OS X, Linux, Android and IOS
  - Support for simultaneous users
  - Provides Network access control
    - Authenticating a client-side digital certificate

FUTURE WORK

- It includes :
  - Designing a **cross-platform, secure and an highly configurable VPN solution** that considers certain potential factors for increasing the performance (like reducing network overhead and having efficient bandwidth), such as

    payload length, encryption key size, encryption digest, TLS digest, etc.

FUTURE WORK

- Also in addition to the tests performed, the results should be verified using some **analytical modelling** of data.
  - This will help us understand how each of these factors affects the performance and why.

Thank You !!!