INDIAN INSTITUTE OF TECHNOLOGY PALAKKAD

Software Stack for IoT devices

Under guidance of Dr. Vivek Chaturvedi

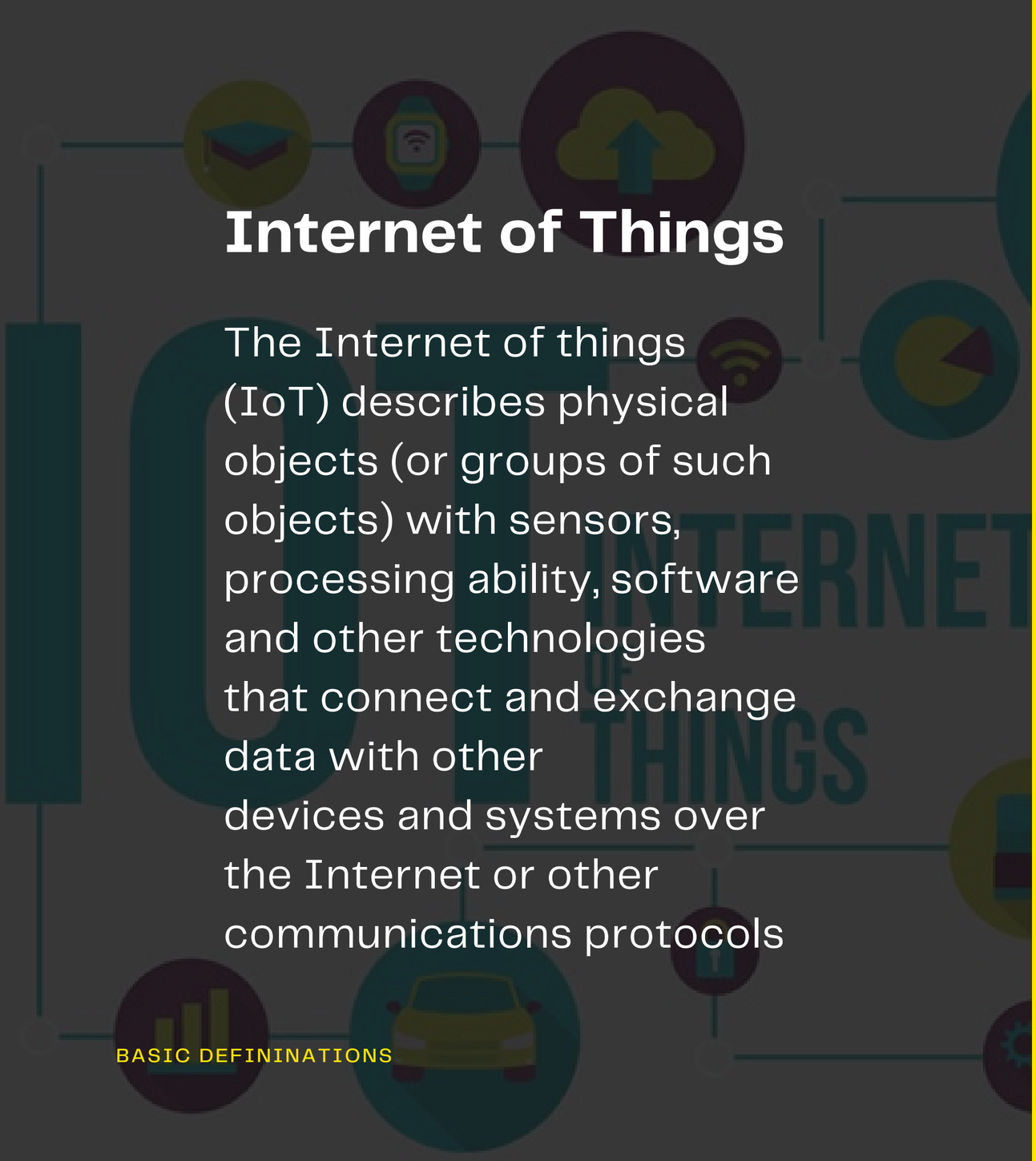
Presentation by:
Garima Ranjan (122101011)
Kshitij M. (112101025)

Things to discuss

- Objective
- Basic definations
- Introduction to AES and Twine
- Comparision
- Conclusion
- Future goals

Objective:

Work on a software that can communicate with all the connected IoT nodes without risking the security of the data.
One major task in the communication layer is encryption.
We need a light weight but secure crypto algorithm.

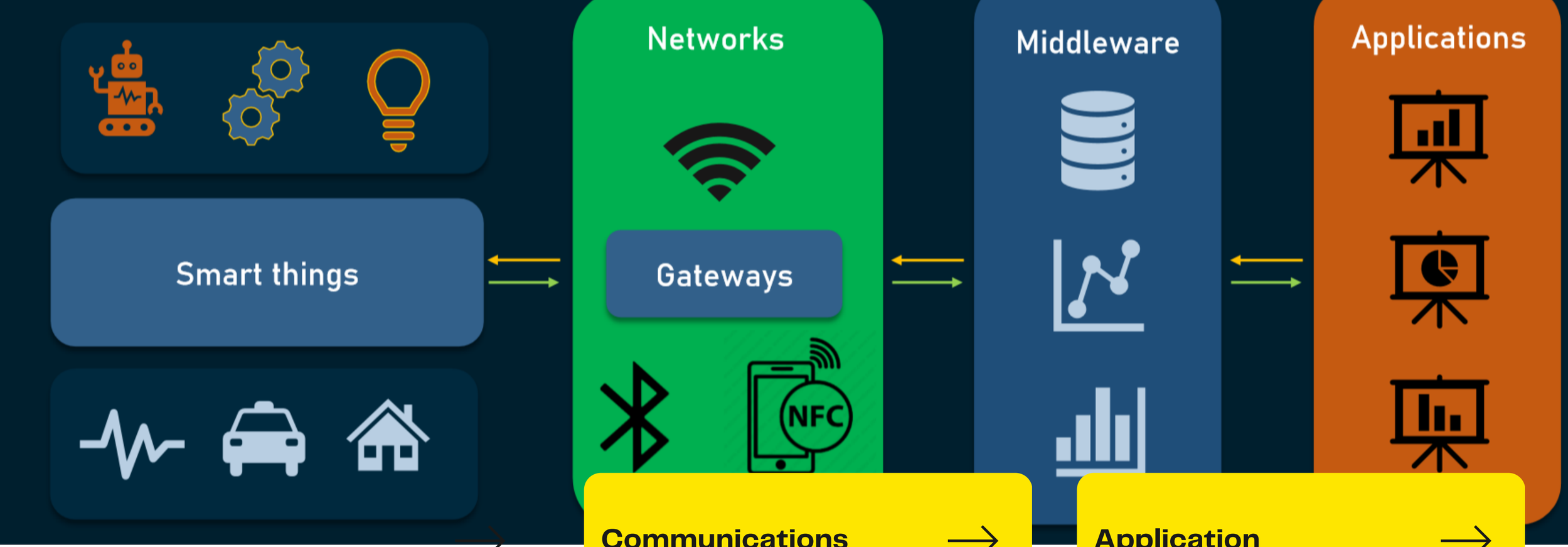


Internet of Things

The Internet of things (IoT) describes physical objects (or groups of such objects) with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications protocols

Software Stack

- A software stack is a collection of independent components that work together to support the execution of an application.
- The components, which may include an operating system, architectural layers, protocols, runtime environments, databases and function calls, are stacked one on top of eachother in a hierarchy.



Layers of Software Stack

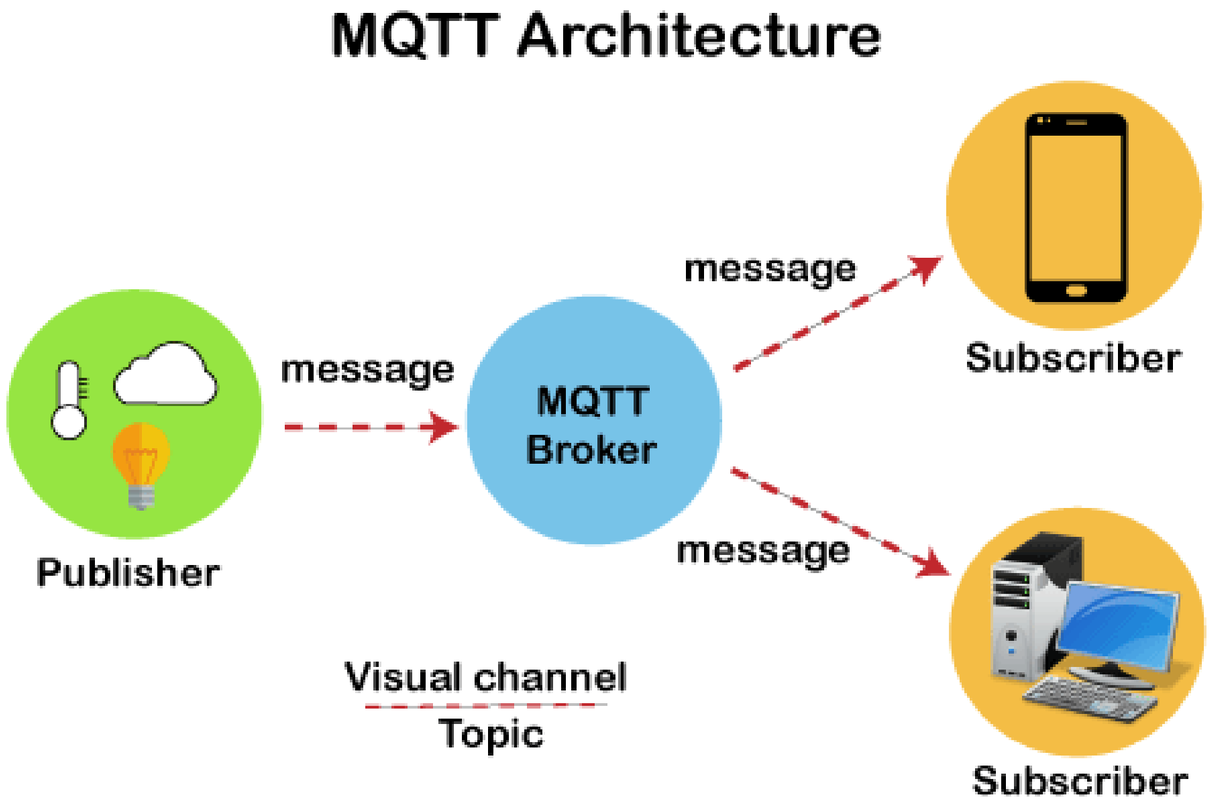
BASIC DEFINATIONS

Communications

We are interested in the secure communication between IoT devices and the Cloud. Also, a secure and healthy communication between application and the cloud for sending and storing data.

Application

Desigining an applcation to communicate with cloud for giving instructions to the IoT devices.



Message Queue Telemetry Transport(MQTT)

What is MQTT protocol?

MQTT is a standards-based messaging protocol, or set of rules, used for machine-to-machine communication OASIS standard messaging protocol for Internet of Things(IoTs).

Why MQTT?

Lighweight and ”publish” and ”subscribe” actions are easier to implement.
Takes care of the privacy of the nodes, as there is no exchange of IP addresses or ports.
Better scalability compared to the traditional client-server approach, addition of newer nodes is easier.

Encryption in MQTT

Payload security
SSL/TLS encryption

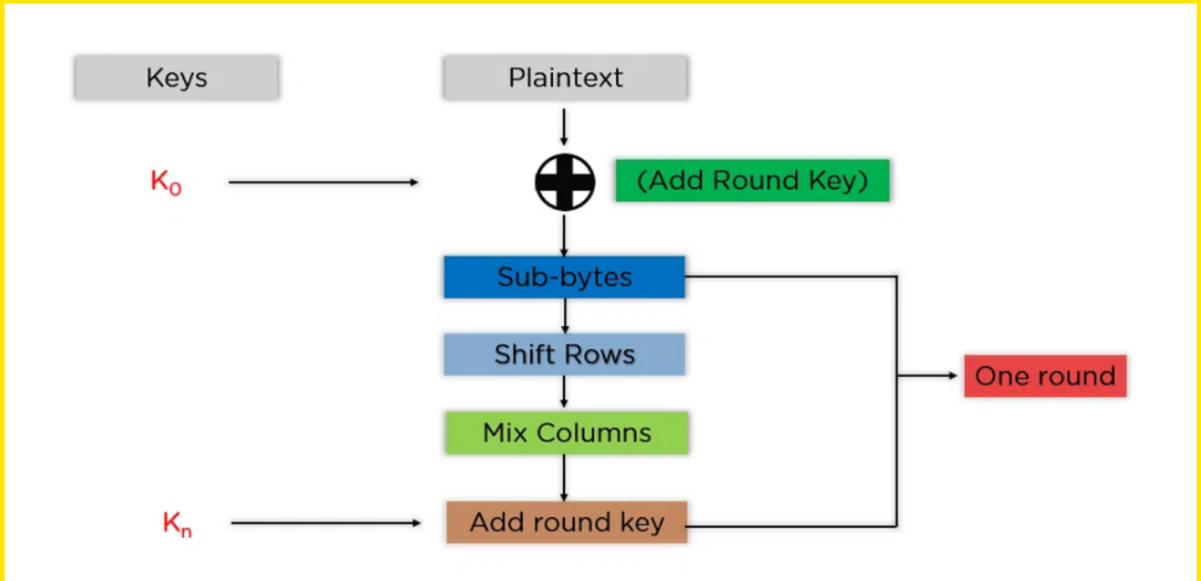
ENCRYPTION

TWINE

It is a 64-bit block cipher.
It supports 80 and 128-bit keys.
Main feature: achieve hardware efficiency while minimizing the hardware-oriented design choices.

AES

AES is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Symmetric key algorithm means the same key is used for both encrypting and decrypting the data.



Final Comparision and Conclusion

Which is better AES or Twine?

Twine

Features:
(1) no bit permutation,
(2) generalized Feistelbased, and
(3) no Galois–Field matrix
(4)only one 4–bit S–box
(5)only one 4–bit XOR
(6)no fixed key setting, hence keys can be updated

AES

AES is a symmetric encryption algorithm, meaning that the same key is used for both encrypting and decrypting data. This makes it faster and more efficient

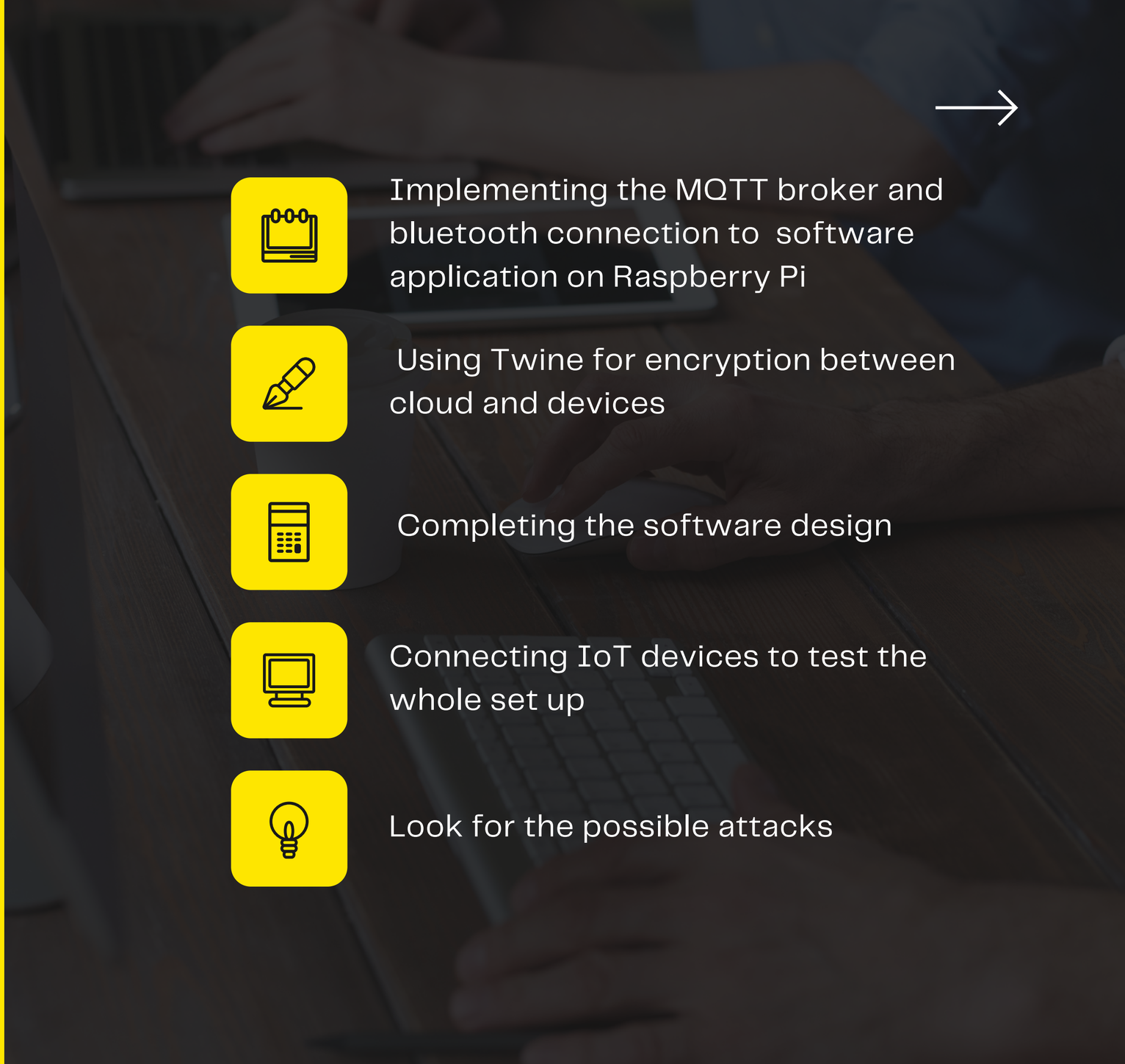
What is good for our project?

Twine is better option for our purpose as it is light weight and easier to implement.

Future Plans

Combining all objectives

FUTURE SCOPE OF PROJECT



- Implementing the MQTT broker and bluetooth connection to software application on Raspberry Pi
- Using Twine for encryption between cloud and devices
- Completing the software design
- Connecting IoT devices to test the whole set up
- Look for the possible attacks

Resource Page

Biblography

About MQTT:

https://mqtt.org/
https://www.hivemq.com/mqtt-essentials/

About Twine:

https://www.nec.com/en/global/rd/tg/code/symenc/pdf/twine_LC11.pdf

About IoT:

https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT
https://en.wikipedia.org/wiki/Internet_of_things

About AES:

Source:https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption
https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard
https://ieeexplore.ieee.org/document/6304791
https://www.ijert.org/research/area-optimized-architecture-for-aes-mix-column-operation-IJERTV4IS090602.pdf

About Tkinter:

https://youtu.be/Iv_dECet_oM
https://youtube.com/playlist?list=PLu0W_9lII9ajLcqRcj4PoEihkukF_OTzA

Images:

https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.dreamstime.com%2Fstock-illustration-smart-phone-to-connect-to-social-network-connected-devices-people-as-illustration-icons-image62213270&psig=AOvVaw2gswZ8u9J7qsOejL8DDMh9&ust=1684057796464000&source=images&cd=vfe&ved=0CBEQjRxqFwoTCKjj-amC8v4CFQAAAAAdAAAAABAQ
https://www.altexsoft.com/media/2020/08/iot-architecture-building-blocks.png https://cheapsslsecurity.com/blog/wp-content/uploads/2017/10/iot-device-security.jpg
https://www.researchgate.net/profile/Je-Sen-Teh/publication/316569426/figure/fig2/AS:699926145142784@1543886805054/Memory-bound-Example-of-block-cipher-TWINE_Q640.jpg

THANK YOU

Link to codes

Tkinter Login Page

Algorithms in python