



# IOT AND CYBERSECURITY

ASHUTOSH SRIVASTAVA



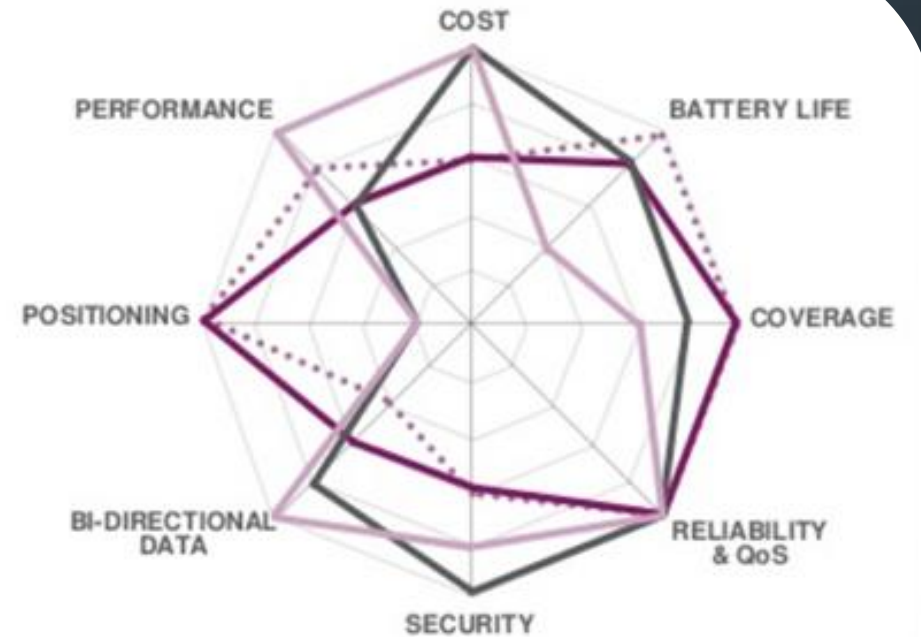
# AGENDA

- Overview
  - Current State of IoT
  - Security Challenges
  - Threat Spectrum
  - How do we protect ourselves
  - What's Next
- 
- 
- 

# OVERVIEW

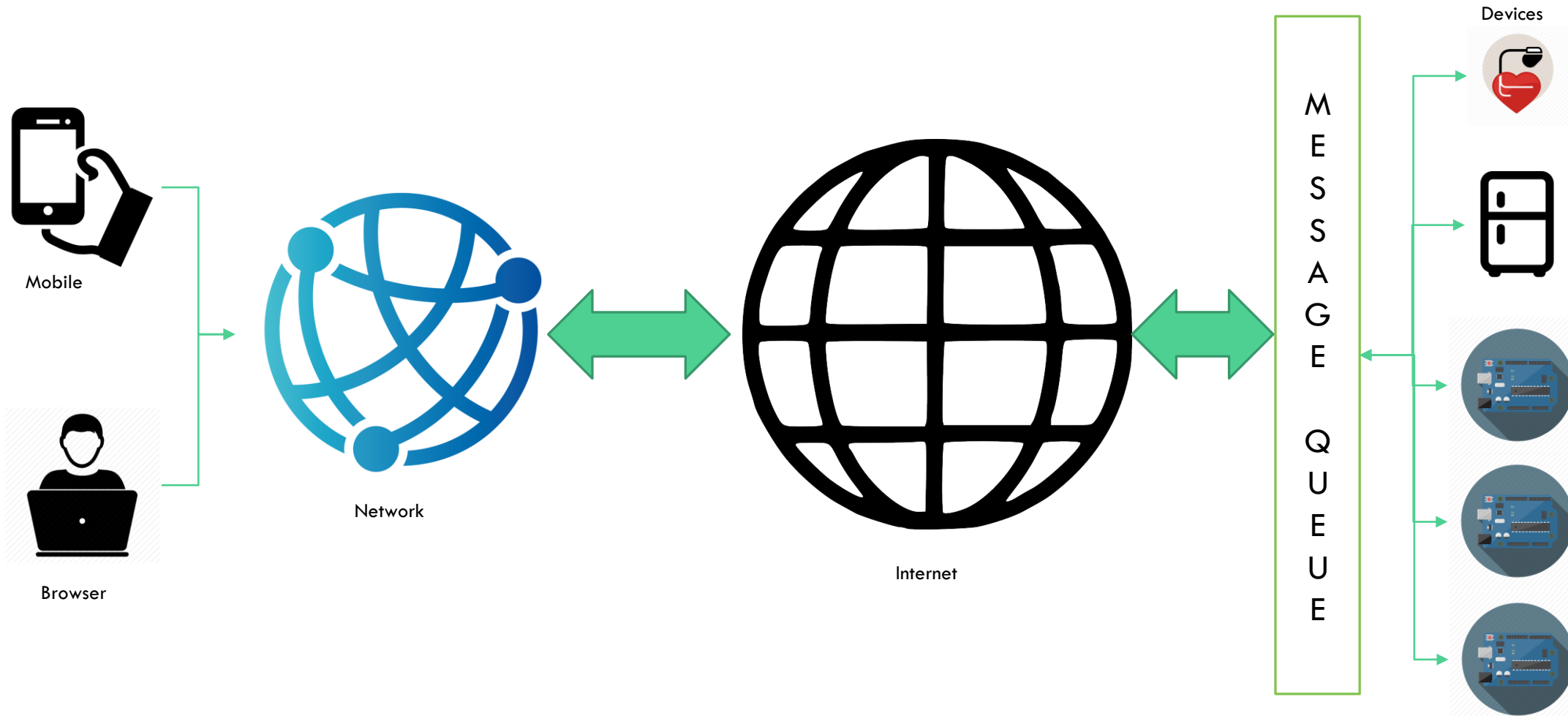
- Connected Devices are now everywhere
- IoT is all about scalability of Connected Devices
- A Gartner report predicts over 20 billion connected things by 2020
- Security of IoT is at:
  - Macro level: security of complex system with User management
  - Micro level: At the device level, network

# CURRENT STATE OF IOT



- ..... TRANSPORT & LOGISTICS: Goods tracking
- SMART CITIES: Smart bicycles
- INDUSTRIAL: Process monitoring & Control
- SMART BUILDINGS: Home automation

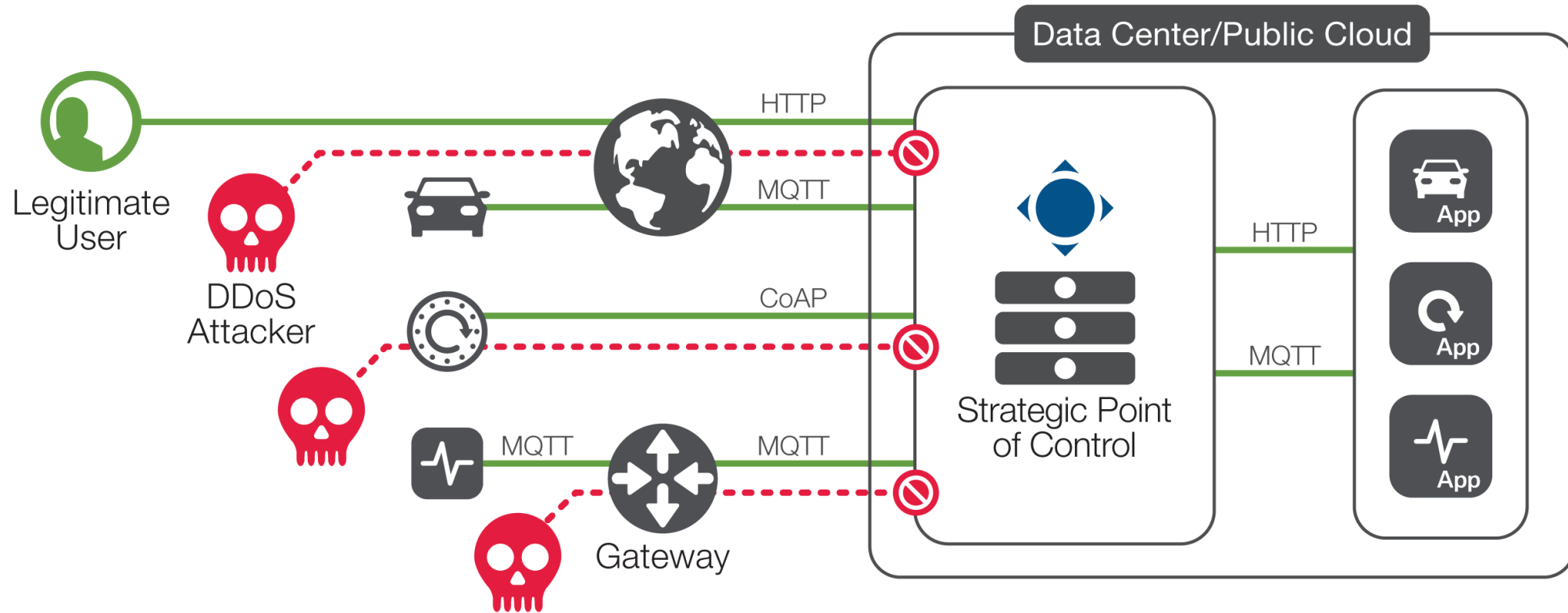
# SECURITY CHALLENGES (CURRENT LANDSCAPE)



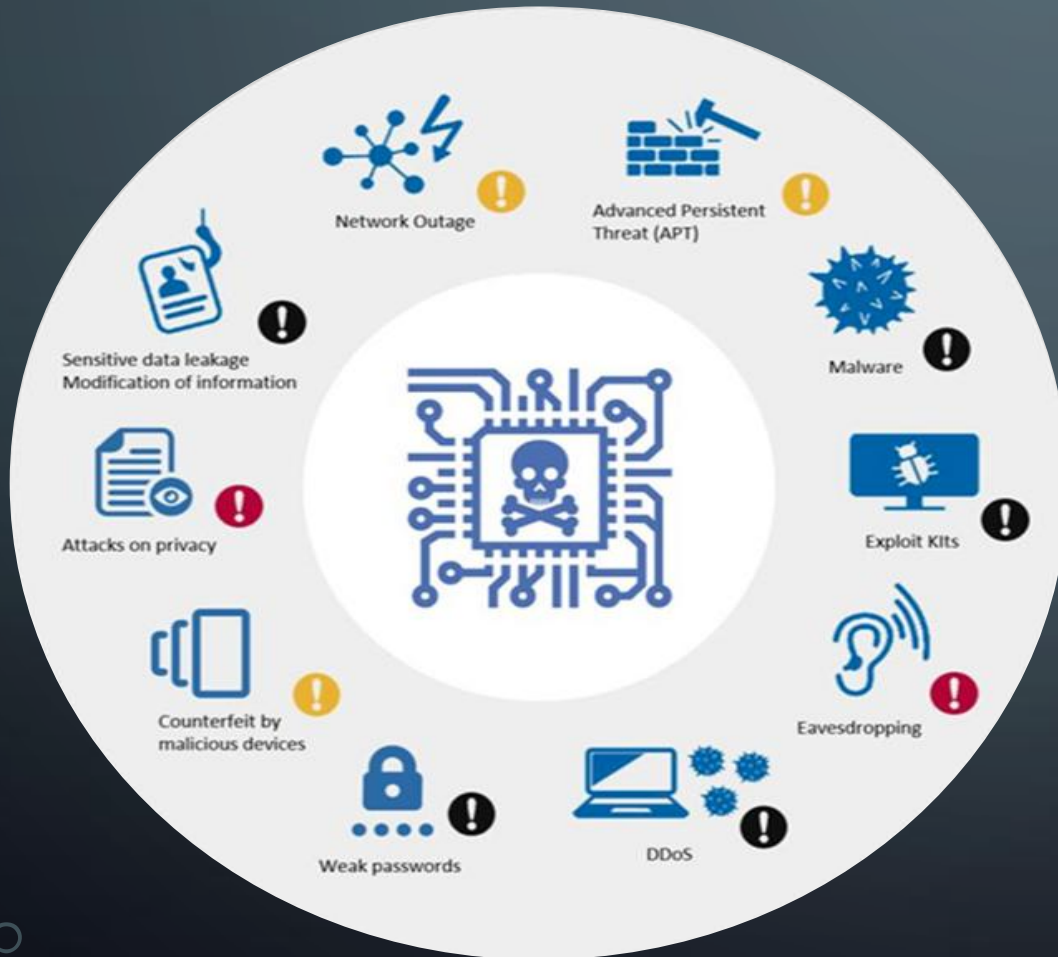
# SECURITY CHALLENGES (USER LEVEL)



# SECURITY CHALLENGER (NETWORK)



# THREAT SPECTRUM



- 70% of IoT devices contain vulnerabilities
- Product design does not consider security
- Adding security during scaling is challenging
- “Edge” device connection an issue
- Devices themselves are insecure due to low processing capability
- Changing protocol landscape also presents challenges
- User credentials also pose a threat
- Low security at home router and gateway levels also worrisome
- Easy to compromise mobile devices



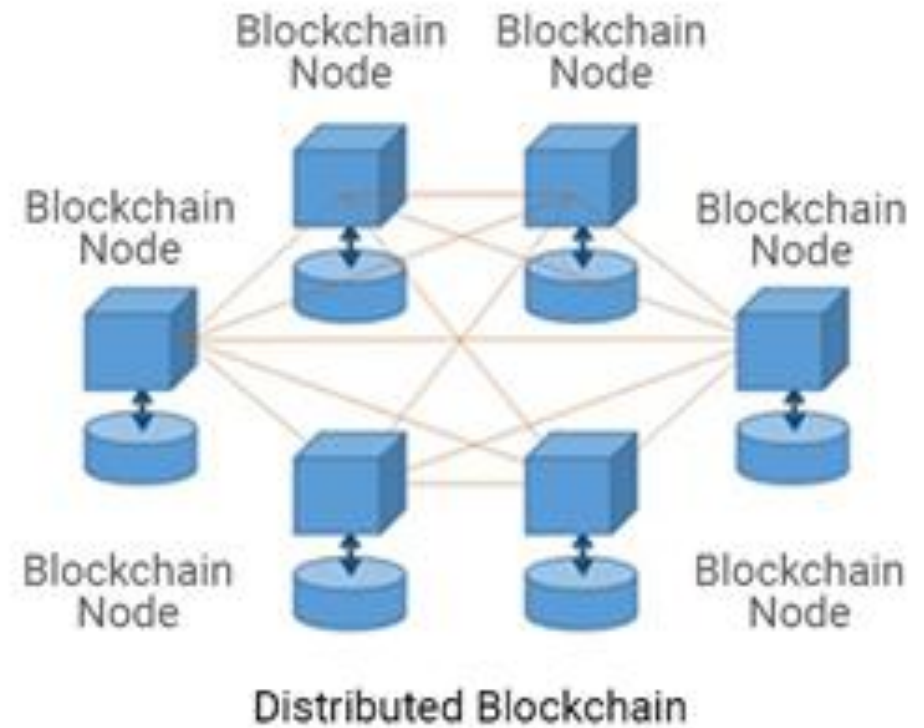
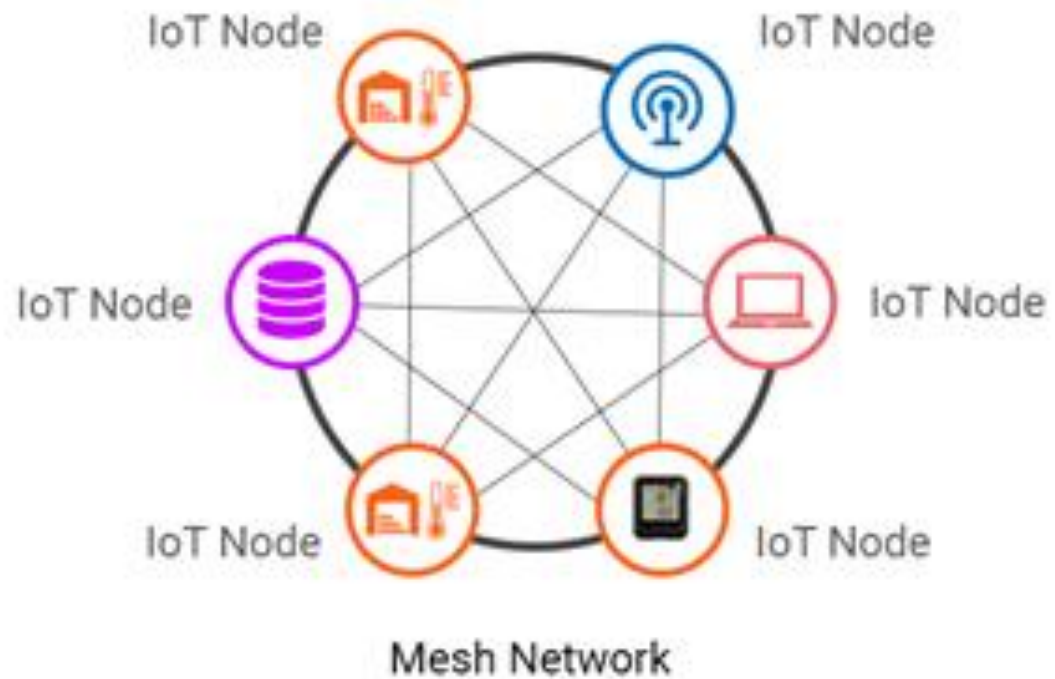
# HOW DO WE PROTECT OURSELVES

- Devices need to meet a minimum industry standard
  - US senate passed “Internet of Things (IoT) Cybersecurity Improvement Act of 2017” to define the minimum standard
- With the advent of Beagleboard & Raspberry Pi etc., it is possible to get device level security
- TLS security to secure communication with message server
- Role based access to restrict user entry
- 2 Factor authentication/OAuth based logins

# WHAT'S NEXT (OWASP)

- Open Web Application Security Project's Internet of Things Top 10 Project
  - Injection
  - Broken Authentication
  - Sensitive Data Exposure
  - External Entities
  - Broken Access Control
  - Security Misconfiguration
  - Cross-Site Scripting
  - Insecure Deserialization
  - Using Components with Known Vulnerabilities
  - Insufficient Logging & Monitoring

# WHAT'S NEXT (BLOCKCHAIN)



# REFERENCES

- OWASP top 10 projects: [https://www.owasp.org/images/7/72/OWASP\\_Top\\_10-2017\\_%28en%29.pdf.pdf](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)
- Atos blockchain and IoT: <https://atos.net/en/blog/blockchain-iot-re-architecting-core-edges>
- What blockchain can do for IoT: <https://dzone.com/articles/what-blockchain-can-do-for-the-internet-of-things>
- IIoT and Network Security: <https://f5.com/resources/white-papers/the-industrial-internet-of-things-and-network-security-27421>
- Defining and securing IoT: <https://www.helpnetsecurity.com/2017/11/22/defining-securing-iot/>

The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines of varying lengths and angles, ending in small white circles, resembling electronic components or nodes on a board. The traces are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

QUESTIONS ?

The background is a dark blue gradient. In the four corners, there are white, stylized circuit board traces. These traces consist of straight lines of varying lengths and angles, ending in small white circles, resembling electronic components or nodes on a board.

**THANK YOU**

ASHUTOSH@EVENIONSOLUTIONS.COM