SANDHYA B R
Cyber Security Researcher Industry 4.0-Security

Accenture India

“ Everyday brings new challenges to protect your privacy and data from the ever-growing threats which motivates in finding new ways for staying safe , defending against cyber attacks. ”

- A Certified Ethical Hacker (CEH) from EC Council
- Bachelor of Computer Science and Engineering
- Hackathons - Attack to protect ,Security Innovation, Nullcon etc.
- Brown Bag Sessions - Data Privacy and Protection , Android Application Development and Security , IoT Device Security.
- Trainings / Workshops - Application Security Testing hands on workshop , KSIT , Bangalore. Cyber Security Awareness Fest at EWIT , Bangalore. A trainer for GFT – Green Field Training conducted by Accenture for the New-Joiners
- Nullcon-Bangalore chapter , Infosec Women in Cyber Security
- IISc, Bangalore (CXC), IEEE to gain knowledge on IoT, its uses and security.


PRIVACY
PROTECTION
THE BIGGEST CHALLENGE OF THE IoT ERA

TAKEAWAYS

- Growth of IoT Devices
- Need for privacy and data protection
- Major data privacy breaches
- Challenges faced by IoT Device Manufacturers
- Privacy measures
- Stay Safe

THE IoT ERA

By 2025, there will be as many as 75 billion connected IoT devices. Privacy is the biggest area of concern in this IoT Era.

The global IoT market is forecast to be worth $1.7T in 2020.

By 2022, 100% of the global population is expected to have LPWAN coverage.

The IoT in Banking and Financial Services market size is expected to grow to $2.03B by 2023.

Enterprise and automotive IoT market will grow to 5.8 billion endpoints in 2020, a 21% increase from 2019.

References:https://techjury.net/stats-about/internet-of-things-statistics/ [1]
https://securityboulevard.com/2019/09/20-surprising-iot-statistics-you-dont-already-know/
https://www2.deloitte.com
https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-a

IS YOUR DATA SAFE ?

Device tracking

Logging

Data Breach

Confidentiality

DDOS

Authorization

Alerts

Social Media Data

MITM

GDP

Every 5 Minutes

Monitoring

DATA PROTECTION POLICY

FLOOD

HTTP

Usability

PCI DSS

OWASP

Firewalls

Passwords

$330,000 B

Data Storage

Authentication

Permissions

Compliance

Data Leak

PHISHING

Smart Devices

Open Ports

Unique Device Information

2 Billion Records Exposed In Massive Smart Home Device Breach

- User database exposed to internet without any password.
- 2 billion logs
- User passwords, reset codes, smart camera recorded conversations, emails addresses, IP Address, geolocation etc.
- Passwords/password reset codes logged areMD5 Hashed.
- Hashed but not salted.
- With reset codes-lock the user account

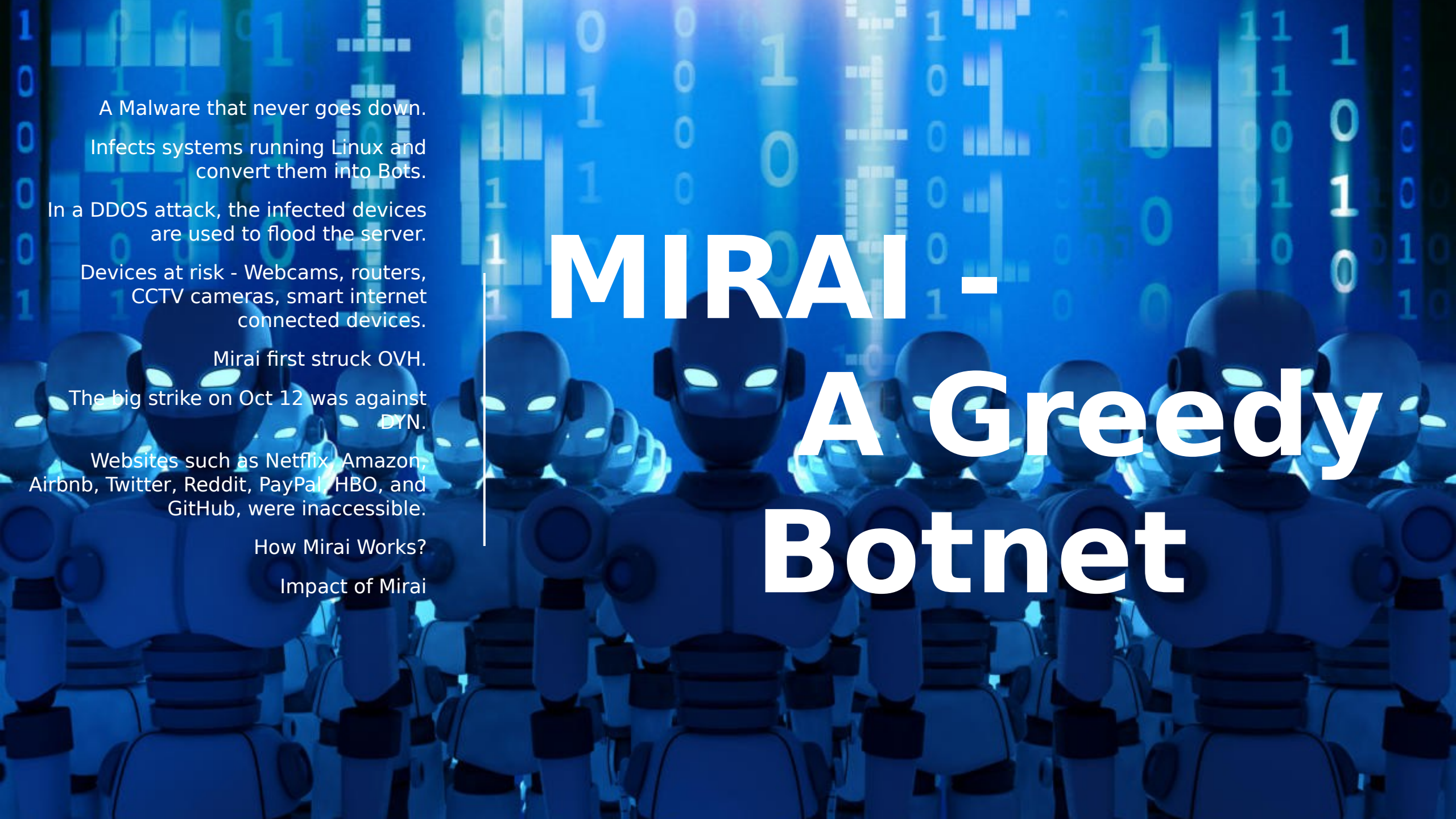
Are privacy concerns halting smart cities?

Smart Cities – Future of IoT

- Individual Privacy is a concern
- Insecure being surveillance on constant camera
- Data collected is utilized
- Educate consumers to gain confidence

PRIVACY MEASURES

- Public Awareness
- Government Measures
- Data Contracts
- Anonymized and categorized data



MIRAI - A Greedy Botnet

A Malware that never goes down.

Infects systems running Linux and convert them into Bots.

In a DDOS attack, the infected devices are used to flood the server.

Devices at risk - Webcams, routers, CCTV cameras, smart internet connected devices.

Mirai first struck OVH.

The big strike on Oct 12 was against DYN.

Websites such as Netflix, Amazon, Airbnb, Twitter, Reddit, PayPal, HBO, and GitHub, were inaccessible.

How Mirai Works?

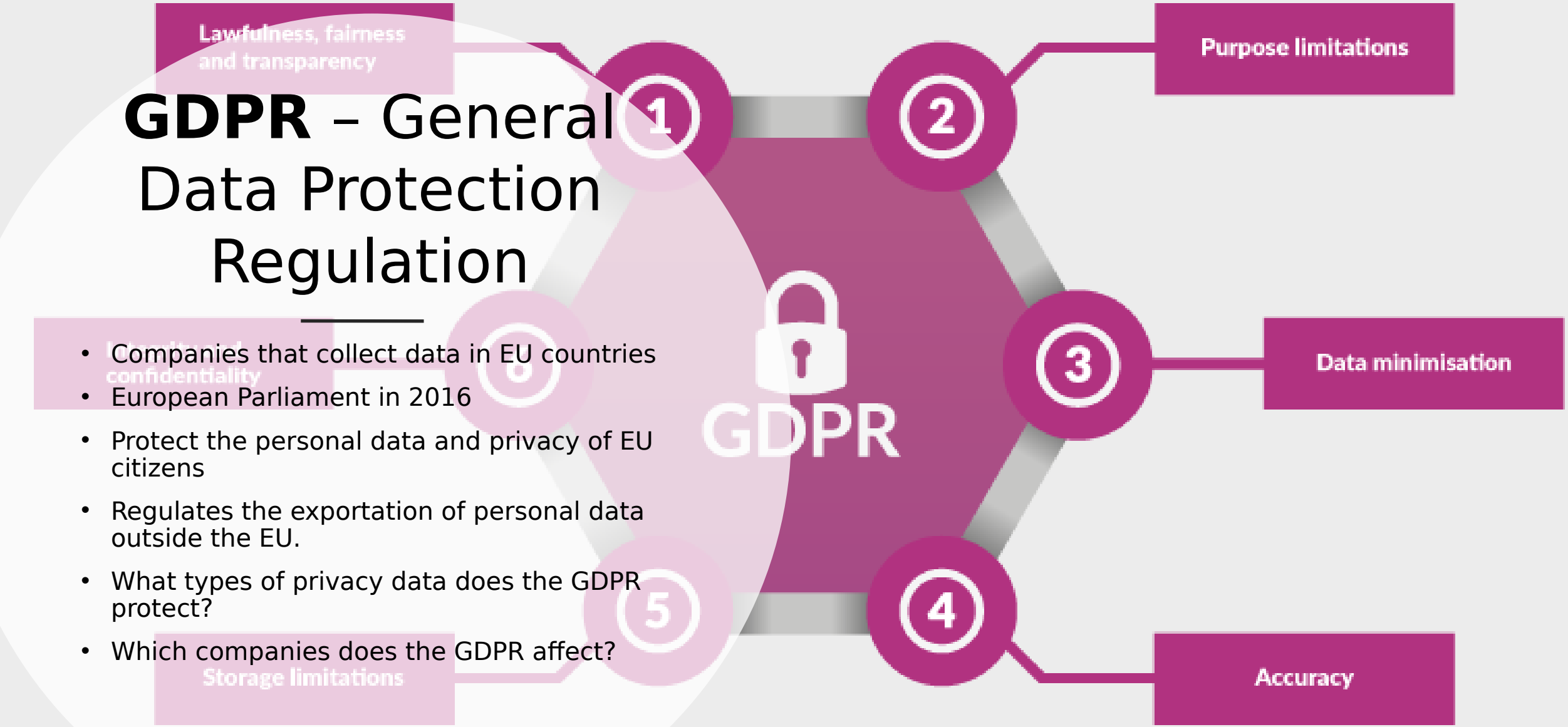
Impact of Mirai

Team of hackers take remote control of Tesla Model S from 12 miles away

- The hack targeted the car’s controller area network, or Can bus.
- Hackers could move the seats back and forth, trigger the indicators, wing mirrors and windscreen wipers, and open the sunroof and boot while the car was driving and in parking mode.
- Control the car’s brakes.
- Phone connected to car’s infotainment systems , could reveal information about the driver’s location , contact details, messages etc.

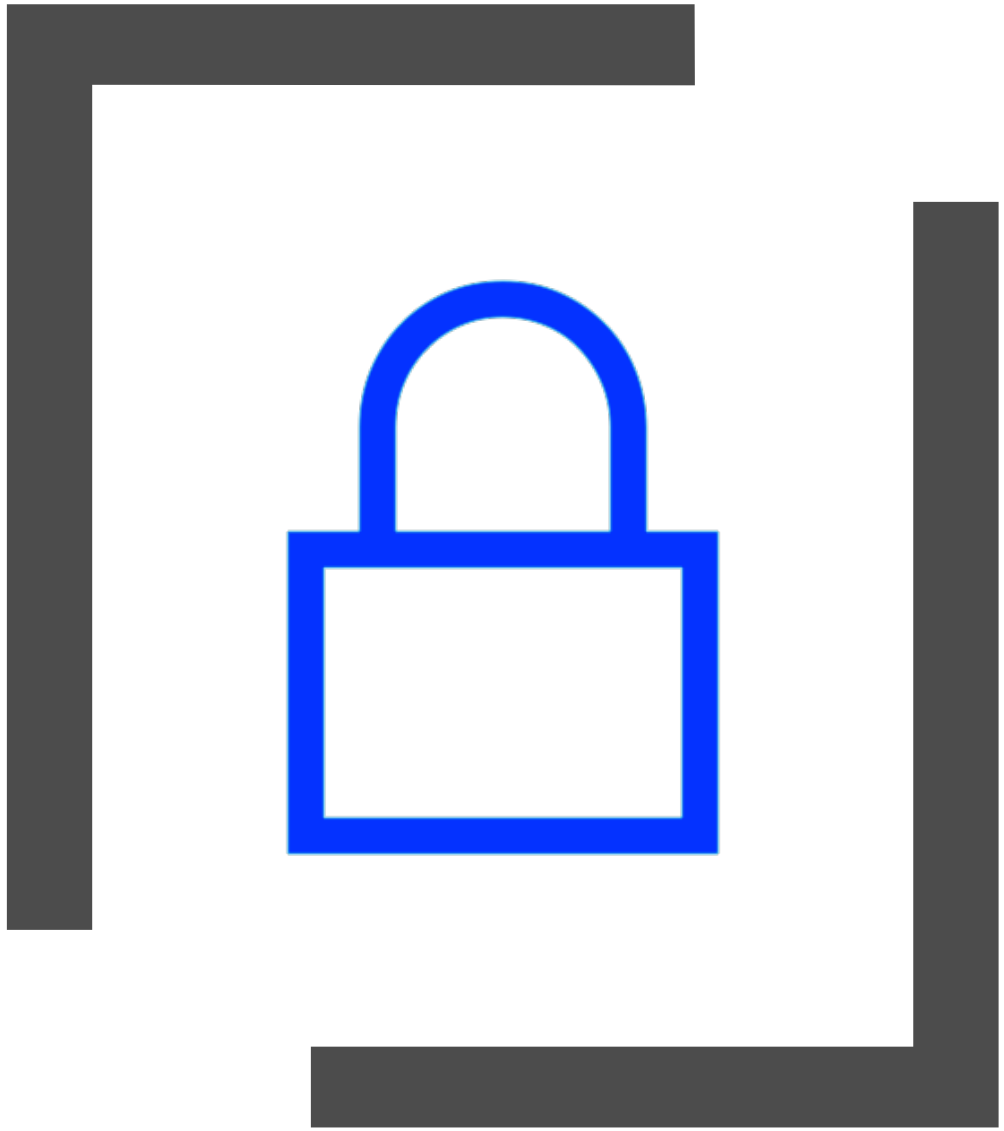
GDPR – General Data Protection Regulation

- Companies that collect data in EU countries
- European Parliament in 2016
- Protect the personal data and privacy of EU citizens
- Regulates the exportation of personal data outside the EU.
- What types of privacy data does the GDPR protect?
- Which companies does the GDPR affect?



How IoT Device Manufacturers can protect data and privacy?

- Invest in a common operating platform built with security in mind.
- Unnecessary services should be disabled.
- Do not run your management GUI from a web server that runs in root context.
- Use up-to-date versions of OS kernel and services such as Telnet/SSHD, web server, php or any other GUI supporting framework.
- Do not keep hidden backdoors.
- avoid the use of UPNP-IGD (Internet Gateway Device protocol).
- Enforce strong passwords -Do not store the passwords in reversible format.
- Create a vulnerability disclosure and handling program.
- Try to limit the personal data that needs to be stored on the devices.



BETTER SAFE THAN SORRY!

Security Guidelines – What we can do to protect our data?

- Say NO to default passwords.
- Control over your Data.
- Avoid a hostile environment.
- Set Limits.
- Regularly Install Updates.
- Wireless Networks.
- Be aware about potential vulnerabilities.
- Look to experts who will help you navigate the

THANK YOU !

Email: sandhya3895@gmail.com
LinkedIn:https://www.linkedin.com/in/sandhya3895/