# SIDON Intensive binary vulnerability analysing

Aishwarya RAMESH, Behan Remoshan BENET RUBAN, Lafi KAMEL, Bharani MOORTHY, Kumar SAURABH

## PROJECT DESCRIPTION

**SIDON** is an advancement to the existing **IoT security** through the power of machine learning. It helps the security experts to identify the presence of vulnerabilities in the core software of any interconnected IoT system. SIDON allows the manufactures to get the software tested for vulnerabilities while keeping their source code confidential. IoT devices don't go through software updates as other devices do, so the importance of delivering the finest software is significant. A complex model, trained with various binary files and vulnerability knowledge bases, evaluates the given binary files for any flaws.

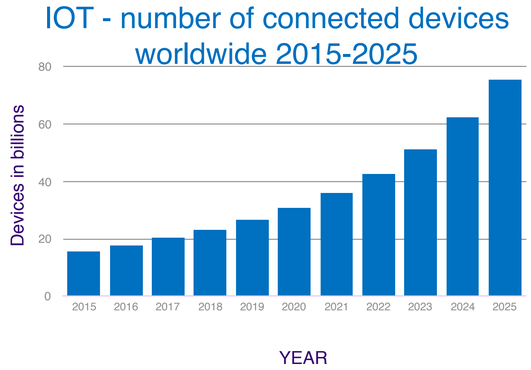
### HOW SIDON MAKES THINGS BETTER

> Reduces time consumed in repetitive assessments, which ensures faster deployment into the market.

> Goes beyond the boundaries of manual testing.

> Every analysis is also a learning, gets better and better as its being used.

> Get certified even without exposing the source code.




## RESEARCH CONCLUSIONS

The core model designing is a challenge for Data scientists and developers. This requires a lot of pre-thinking and planning before starting the development.

> Compiled binary will produce different assembly code respective to platforms, so pre-processing and classification are necessary before doing any machine learning on data.

> Analysing the code flow is essential to detect the vulnerabilities, hence, the model has to be robust to handle complex programming path ways.

> Increasing numbers of IOT devices their market value will strongly depend on its security, SIDON will assist the experts to make things better.

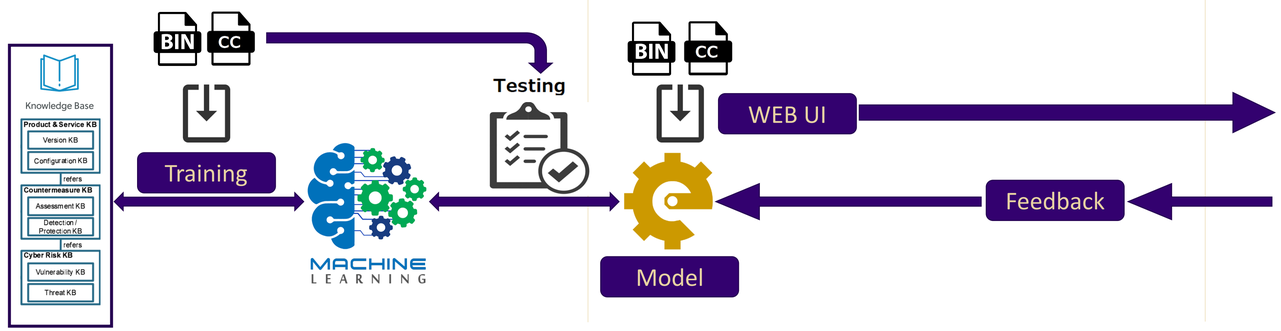
## TOOLS AND METHODOLOGY

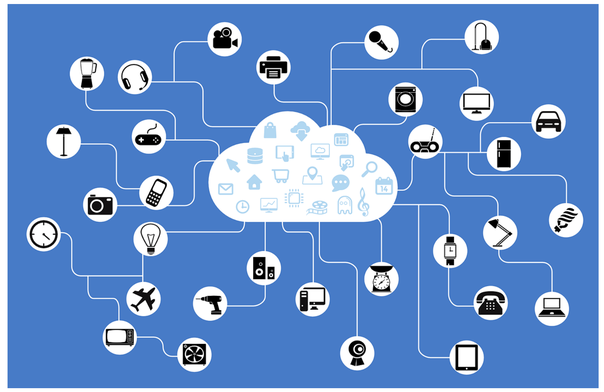
> **TensorFlow -** Deep learning models of the application are designed and trained using this open-source powerful library.
> **Google DataLab -** Large computing power Cloud service used to develop, train and test the model.
> **Docker -** Cross-device compatibility and easy deployment will be achieved using Docker, for development, test and delivery.
> **NGINX -** Open source server to run the application.
> **Flask -** Web framework that provides UI of the engine.
> **PostgreSQL -** Database engine to manage the application.
> **objdump, gdb & IDA -** Binary decoding is performed using basic Unix tools and IDA may be used for exceptional binaries.

## DEVELOPMENT PLANS

Machine learning is the core part of the project and it has a higher priority.

> Pre-processing module that decodes binary files and classifies the assembly code.
> **Development of the core model.**
> Train the model with the existing data.
> Web application and database design.
> Integration of the machine and the web application.
> Test the model continuously with known binary files to benchmark its efficiency after each training phase.



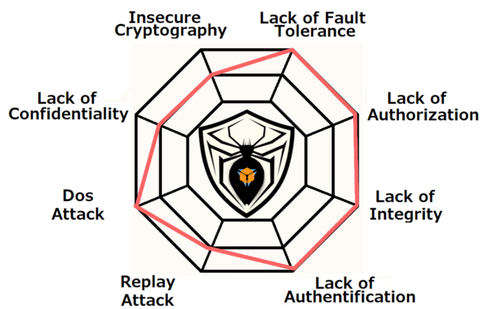
## SUMMARY / COMMENTS

When the machines started to learn, the world has changed. Imagination is now a reality.

> SIDON will change the way the security analysts are working, its automation saves times and effort, also delivering optimal outputs.

> Product manufactures will be excited to get certified faster and also feel secure as their source code is safe.

> Security standards for an IoT device will be soon redefined as applications like SIDON emerge up.




Spring Semester, July 2019