|  |  |
| --- | --- |
|  | **MINISTRY OF EDUCATION AND TRAINING** |

|  |
| --- |
| **FPT UNIVERSITY** |
| **Introduction** |
| Internet-connected Devices Checking System |
|  |
| |  |  |  | | --- | --- | --- | | **IDCS TEAM** | | | | **Group Members** | Nguyễn Quý Đôn | SE04468 | | Nguyễn Quý Tuấn | SE04330 | | Phạm Công Minh | SE04098 | | **Supervisor** | Lectuer : Phan Duy Hùng | | |
|  |

|  |
| --- |
| - Hanoi, 10/2019 - |

**TABLE OF CONTENT**

**Phan Duy**

**Introduction**

* 1. ***Purpose***

This chapter is created as the introduction to Internet-connected Devices Checking System project, it is also a capstone project of team at FPT University. This document describes the overview of some existing systems, the initial idea, brief description about expected system and provides an overview of the project, including background information, review of existing systems, their problem and proposal for ideas of improvement.

* 1. ***Project Information***
* Project name : Internet-connected Devices Checking System
* Project code : IDCS
* Project group name : IDCS Team
* Project Type : Web Application
* Business domain : Security Checking System
  1. ***Project Team***
     1. ***Supervisor***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Full Name | Phone | Email | Title |
| Supervisor | Phan Duy Hùng |  | HungPD2@fe.edu.vn | Lecture |

Table 1-1 : Supervisor's Information

* + 1. ***Team member***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| STT | Full Name | Student ID | Phone | Email | Role |
| 1 | Phạm Công Minh | SE04098 | 0969307911 | [Minhpcse04098@fpt.edu.vn](mailto:Minhpcse04098@fpt.edu.vn) | Leader |
| 2 | Nguyễn Quý Đôn | SE04468 | 0358008828 | [Donnqse04468@fpt.edu.vn](mailto:Donnqse04468@fpt.edu.vn) | Member |
| 3 | Nguyễn Quý Tuấn | SE04330 | 0972654951 | [Tuannqse04330@fpt.edu.vn](mailto:Tuannqse04330@fpt.edu.vn) | Member |

Table 1-2: Team member's information

* 1. ***Background***

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT is powering transformation for enterprises, consumers and government. Emerging tools and technologies like smart speakers, machine learning, and 5G are enabling huge gains to efficiency and more control at home and in the workplace.

The continued growth of the IoT industry is going to be a transformative force across all organizations. By integrating all of our modern day devices with internet connectivity, the IoT market is on pace to grow to over $3 trillion annually by 2026. This rise in popularity of IoT-connected devices leading to rise in IoT app development dose come with its fair share of concern and security challenges.

IoT is in no way immune to hacking. Hackers can launch DDoS attacks by infiltrating and leveraging thousands or millions of unsecured devices. They can cripple infrastructure, down networks, and as IoT advances into our everyday lives, those attacks may very well put real human lives in jeopardy. And even if hackers don’t outright threaten lives, they can compromise gateways and deeper levels of IoT networks in order to reveal and exploit sensitive personal and corporate information.

In fact, one of the main problems with tech companies building these devices is that they are too careless when it comes to handling of device-related security risks.

Most of these devices and IoT products don’t get enough updates while, some don’t get updates at all.

Spending on IoT Endpoint Security solutions will increase to $631M in 2021. Worldwide IoT security spending will increase from $912 million in 2016, soaring to $3.1 billion in 2021, attaining a 27.87% CAGR in the forecast period.

All of the above, we will have tried to create a system to checking security IoT system with temporary features such as check sever open port, running servies in server, check MQTT security. Botnet, Shell attack, Firmware bug will be opening soon.

* 1. ***Literature Review of Existing System***
  2. ***The Proposed System***

After reviewing all properties of the current systems, we have come to a decision to choose which features and functions we will provide in our system.

* + 1. ***System functions***
* Allow user to login by account have created at website
* Allow user to check open port, services running in server when user enter ip/domain
* Allow user to check security
* Give specific solutions for each case
* Allow user to export result as exel, xml or file text
* Allow user to contact with support team
* Allow user to manage their account at account management board
  + 1. ***Out of scope functions***

Because of the time limitation and the effort limitation, we will not implement these following functions, however we believe they could be implement in the feature:

* Fast scan : Check if user internet-connected devices at home are public without ip/domain
* Live support : Instead of contact with support team with email, etc . We need live chat to support user 24/7.
* Connect user with security specialist to given clear and specific solutions, overcome if user is needed.
  + 1. ***Technical Approach***

Architecture:

For back-end system:

For front-end system:

Project management :

* Using the github with GIT to stores code version control.
* Using Trello to manage the task and bug.
* Using some social networking like Messenger, Skype to communicate online