# Proposing Encryption Selection Model for IoT Devices Based on IoT Device Design

1st Matasem Saleh
*School of Computer Science and Engineering, SCE,*
*Taylor's University, Malaysia*
matasemsaleh@gmail.com

2nd NZ Jhanjhi
*School of Computer Science and Engineering, SCE,*
*Taylor's University, Malaysia*
noorzaman.jhanjhi@taylors.edu.my

3rd Azween Abdullah
*School of Computer Science and Engineering, SCE,*
*Taylor's University, Malaysia*
azween.abdullah@taylors.edu.my

4th Raazia Saher
*College of Computer Science and Information Technology (CCSIT)*
*King Faisal University, Saudi Arabia*
raaziasaher@gmail.com

**Abstract— The shortage of resources and services coincides with the expansion of urbanization. Modern technology utilization has become necessary to compensate for this shortage and to provide services which give urban residents a good life. The Internet of Things is one of the most reliable technologies for solving such problems because its devices are capable of collecting data via connected sensors. The problem of securing this data from cyberattacks increases because it contains important information about people. In addition, studies have also shown that most of the collected data is going to be stored in third-party databases in coming few years. For several reasons, designers are not able to adopt encrypt everything approach within IoT device which provides significant protection of collected data. In this research we are going to discuss the challenges which designers faces during the implementation of data encryption within their device as well as have a look on the present support. A model is proposed at the end of the paper to address designer discussed issues and challenges.**

***Keywords***—IoT, System Security, IoT Device Security, Cryptography, Machine Learning, System Design.

## I. INTRODUCTION

The Internet of things (IoT) is one of the most groundbreaking innovations in human life. Due to the useful services it delivers to users, IoT has evolved and spread quickly[1]. IoT device incorporates unlimited number of components in order to allow technological advancement and facilitate people's everyday life and function. Societal ideals such as equity, confidence, anonymity, discrete option and its behavior can be emphasized by the adoption of IoT technology. IoT applies to billions of internet-connected devices all over the world, that store and exchange data. There is a further growth in the amount of IoT devices in the world, predicted by Statista that by 2025 more than 75,440 billion of devices will be functioning [2]. This exponential rise is attributed to low cost manufacture of computer chips and the spread of communication technologies [3, 4].

In IoT devices, sensors are used for detecting and collecting real data from the world. The data obtained is redirected to remote services for further process and analysis, review thanks to the advanced internet access mechanism integrated in IoT devices. IoT devices are belonging to a broad collection of heterogeneous, because of the difference in its environment and its objectives. In comparison, the environment in which IoT devices may be installed restricts the size and resources sch as processing power, memory, and energy. Although IoT devices are of wide-ranging and diverse, they are identical in certain features, such as IoT devices are designed to collect and exchange data alongside limited resources [5-7]. The nature of IoT devices, constraint resources requires the involvement of compacted version of functional software in such devices. Therefore, the operational software in such devices has to be a lightweight to comply with resource constraints.

Since IoT devices are primarily configured to collect and transfer data through the internet without being administered by people, they can be at risk that any machine linked to the internet might confront. In addition, it is challenging to protect IoT devices in contrast to other online connected devices because of its restricted resources. IoT device's collected data hold numerous personal details of the consumer that places high emphasis on confidentiality in the user perspective. For these reasons attackers deem IoT device's collected data as their primary targets[8]. In fact, growing demand of IoT technologies has intrigued hackers to focus their efforts to manipulate and monitor these devices and data they generate. To mitigate this adverse situation, IoT devices should be safe from any possible attacks[9, 10]. The encryption of messages produced by IoT devices is important, taking into account data value, which eventually rises tremendously [11].

IoT device designers are responsible for delivering a sound and secure device without sacrificing their performance. Therefore, several studies are released to guide designers and developers in choosing appropriate encryption according to their device specifications, bearing in mind design efficiency. Besides available research, numerous organizations frequently issue recommendations for the same reason.

The encryption of the data collected and exchanged via IoT devices is essential and highly recommended. It improves consumers' trust and confidence in IoT products by ensuring that they do not disclose the collected data to any unwanted party, that will ultimately contribute to an acceleration of social adoption. For many factors, IoT device designers face difficulty in choosing a suitable encryption for their device which can do the aimed task at device basis without negotiating the device efficiency. These factors are being discussed in this paper. This paper covers the numerous forms of technical assistance offered by researchers