

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 such 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

and organizations to designers. Finally, we will introduce our proposed model concept, which would provide designers with significant assistance in attempt to remedy the complexities they are confronted with, when selecting a suitable encryption that can be consistent with their IoT device.

A. Research Contribution

IoT devices collect an important data about the user and their surroundings. Therefore, it is very important to transmit IoT data in secured manner. It enhances consumer trust in IoT applications and would inevitably lead to accelerating this technology's social acceptance. Software-level data protection inside an IoT device poses challenge for IoT device designers for several reasons which are discussed in this paper. Hence,

II. IOT SECURITY ISSUES

IoT smart utilities, including smart homes, smart cars, and smart drugs, have extended to everyday life, pushing the automation of the new virtual system into the corporeal realm [12]. Cyberthreats does not last in the virtual world only, but it may even roll into a physical life, such as a home, medical devices and smart cars that can affect human life in a significant fashion. As a result, the safeguarding of everyday life should not only be solved by cybersecurity – security problems declined when it was deemed at the time of IoT device design and development [13]. Cybersecurity numerous intrusion tactics tend to attack distinctive layers of an IoT network. As an IoT develops, cyber-attacks complement the physical threats.

In comparison to traditional users of embedded computers, most IoT devices are tracked via smartphone applications. To exploit a control panel of an IoT device, an IoT application intentionally transmits rich device's data, Connecting mainly to the firmware [14]. Data protection becomes a big concern for device architecture for each IoT network.

A number of IoT device producers did not establish security standard benchmarks for their devices, while others use their own security standards which are not consistent with other IoT devices produced by different manufacturer. Although there are no security measures in the old versions of IoT devices. Based on the White Scope study, seven pacemakers' model were found to have about 8000 susceptibilities. In the beginning, not utilizing cryptographic mechanisms were the key reasons for this large amount of vulnerabilities [15]. These concerns called for implementing security by design creative approaches in IoT devices to solve those problems.

III. SECURITY BY DESIGN METHOD GAIN

Security by design is a creative approach suggested by several corporations to integrate required security measures into the software and hardware development life cycle, not after detecting a violation. Security by design importance is increasing as by following this method billions of vulnerable IoT devices are expected to be secured from the majority of popular and widespread security breaches. Since these devices are connected to the Internet, they are a vulnerable point where any security attacker can collect sensitive information or disrupt service. In addition, most of these devices have been developed without any security considerations, making them

some sort of assistance provided by several organization and researchers to guide the IoT device designers are discussed as well. In addition, a model is proposed that might provide a significant assistance for the addressed challenges.

B. Paper Organization

This paper is organized in a way that will start with discussing IoT devices data security issues and the importance of including the security within the design of IoT device. Then it went through the challenges which the designers of IoT devices face when they want to secure the data of their device. Lastly, the insufficient support available resources led to the proposed model which discussed at the end of this paper.

easier targets for security attackers [16]. Many vulnerabilities and threats have proved to have an impact on the lives of individuals when the design of an IoT device is built relying on user knowledge, comprehension, and security awareness. Implementing device security during the design process, will help the user to identify IoT security importance and motivates them to make the correct decision that ensures their safety [17]. The government of UK is calling for the technical consideration of this idea to fulfil the criteria of IoT security [18].

In the next section we will discuss the reasons behind the need of designers to be guided and encouraged to involve the security in their design and what prevents them from doing that.

IV. DESIGNER CHALLENGES

A. IoT Environments

Internet of things (IoT) is an internet of (physical) devices [19] interconnected with electronics, software with the ability of exchanging data [20]. In short, IoT transforms connected nodes into intelligent devices for recording, monitoring and processing data which are collected from their surroundings in real time [21]. The goal of IoT is to simplify many facets of our lives and to increase process efficiency [21]. The use of IoT devices is currently increasing quickly [22] and found in quite diverse domains. For a number of purposes, separate domains implement IoT in their fields. For example, deploying IoT in the retail sector, is to enhance consumer engagement and to introduce useful resources[23]. Though IoT is more commonly used in medicine and for even more valuable reasons, such as remote patient observation, provide reliable analysis, care details and increased treatment quality [24, 25]. In the fields of curriculum, preparation, and management development, IoT has already started to be applied in education [26]. IoT is found in many other domains such as smart cities for purpose like electricity and transportation management [13, 27-29], smart homes for purposes like home automation and monitoring, Natural disasters, agriculture[30], social domain[31] etc. IoT implementation in different domains created heterogeneous measures for usage of IoT devices, rendering standardization an unlikely mission. The lack of standardization is one of the limiting factors in selecting an encryption technique and prohibits the labelling of the right encryption technique for IoT devices [32, 33].

B. Applications of IoT

Because IoT's ecosystem generated heterogeneity, the massive applications used led to system limitations that

eventually restricted their capacity and led to their resource constraints [34]. IoT devices are compact in scale and may be incorporated with other systems. [35] or may found as individual devices as CCTV camera. The sensor or actuator type can vary depending on the application for which IoT device is used. When IoT devices have been incorporated in other systems, designers must confine themselves to the main system necessity, including IoT device size and power supply, which ultimately limit IoT devices' performance. In recent years, the field of nanotechnology has significantly improved, enabling IoT device designers the opportunity of reducing the device specs to make it suitable for to be used in any application. In addition to the number of sensors and actuators that can be used increased the feasibility of implementing IoT device in different application [36]. The purpose and nature of the IoT device determines the sensor type used. Different types of sensor dependent on deployment applications may be used in IoT device. In terms of embedding these devices, the broad variety of used parts and resources are considered to be a positive feature which makes them applicable in a wide range of applications and environments, nevertheless the drawback is that each IoT device requires a customized encryption technique as the architecture and the used parts are vary from one device to another [37, 38].

The hardware issue with power and storage constraint often needed designer management [45]. IoT systems tend to have limited processing power in order to minimize costs and use of electricity. Computing constraints often hinder access to IoT-enabled resources. The hardware limitations mentioned affect the type of encryption technique used to protect IoT devices [37, 38].

C. Cost of IoT Devices

Besides the large rise in amount of IoT devices and their launch in different fields, which are supposed to accomplish certain IoT projections, they have had an overwhelming positive effect on the global economy. However, there is a more reality in price declines in the increased amount of IoT. To get an understanding of the downturn in the price for the IoT business, take the single sensor pixel price as an illustration, we can see that over 10^6 of price decline, as the cost dropped from EUR 100 000 in 1960, down to 0.02 in 2010 [39]. This fall in prices will deter developers of IoT devices from investing in IoT security research.

D. Embedded Systems to IoT Transformation

Usually, the embedded device can be described as a device that contains hardware and software that is intimately linked to a particular function, part of a broader framework, not independently programmable by the user, and can work with or without minimal human interference [40, 41]. In 1974, the first integrated computer machine was introduced utilizing a single-board computer and microcontrollers and built into a wider package [48]. IoT's fundamental basis is embedded systems, although the only difference is that they do not provide overt internet connectivity, while the internet was launched earlier in 1969. The IoT was first used in 1984, long before the name was recognized, as the coke press remained allied to the internet to document the availability and time of

the drink [49]. Mark Weiser invented omnipresent computing in 1990. Ubiquitous computation utilized advanced embedded machines to partake with anything but not seen [50]. Later, the basic idea of IoT was adopted when sensor nodes were designed to identify and exchange data of particular embedded devices seamlessly [1, 12, 51]. In 1999, Bill Joy first pioneered Device to Device Correspondence in his Internet taxonomy, and Ashton first used the term 'Internet of Things' [52, 53].

As background reveals, IoT devices are the product of the development of embedded systems. The background of several designers is from embedded systems who consider security not to be a problem since embedded systems are essentially used without any internet connectivity in closed and disconnected systems. [42].

V. IOT ENCRYPTION TYPES

Encryption is a structure that keeps knowledge from those who are not permitted to access it or change it [43]. The encryption strategies began with the popular 'Caesar Cipher' and after that period have progressed into more sophisticated algorithms that are quite reliable and not likely to be outbreaks much. Various encryption methods can be used in IoT devices, each has various hardware specifications, has a different effect on their resources and offers a different degree of protection, which makes it challenging to choose encryption.

A. Conventional Encryption Techniques

The two basic types of conventional encryption, symmetrical (public key) and asymmetrical (private key) encryption. Conventional encryption was planned mostly to attain higher degree of protection level and ignored device performance parameters such as AES for 128 192, 256 main sizes of hardware and software. [44]. IoT products scale is their signature, designers are compelled to reduce the resources of devices i.e., memory, storage, and processing capacity, to achieve the appropriate size. IoT systems are classified as resource-constrained devices, which essentially minimize their capacity to handle standard code size. Therefore, in many situations IoT devices cannot use conventional encryption [45, 46]. Two separate kinds of digital encryption are essential and are reviewed below.

1) **Symmetric Encryption:** Both a recipient and a sender grant a shared key through secure communication. Symmetric encryption is known for its easy operations[47], XOR and permutations are mainly faster and do not consume much resources, along with processing speed. [46, 48] this is why it is ideally suited for IoT applications [49]. Symmetric encryption provide reliable approaches and cost-effective data safety without negotiating security [48]. However, assigning a hidden key is susceptible to threat. In differentiating between different encryption methods through symmetrical encryption, the distinction between block cipher and stream cypher plays a significant role. In this category, there are several encryption techniques including AES, RC2 and blowfish. Moreover, most of these encryption techniques use significant power during operation. [50].

2) **Asymmetric Encryption:** Asymmetric encryption method requires the encryption and decryption of a couple of public and private keys. Under this method, there are many encryption techniques, such as RSA, DSA and ECC. In cryptography, asymmetric method addresses the key issue, but uses more power [51].

B. Encryption Approaches for IoT

In heterogeneous IoT environments and applications, there are various challenges and problems including energy usage, restricted batteries, performance costs, memory capacity and ICT security [52]. Furthermore, resources-limited devices with low computational power, less memory, short battery life and small bandwidth need a well-organized security solution without collapsing IoT resources [53, 54]. IoT devices are also not structured and the manufacturer has all the ability to choose things that will fulfill the product intent. Encryption technique is one of the attributes that designer must select carefully based on his device specs. Thus, the range of IoT encryption techniques must be comparable with the of IoT devices architecture variety without conceding security. Researchers are widening the spectrum of encryption methods in research. Growing Encryption techniques in research are of two forms, lightweight encryption, and combined encryption technique, discussed below.

1) **Light-weight Encryption:** Since conventional encryption techniques are incompetence with most IoT devices and applications, many researchers appeared to discover an effective encryption technique by lowering the coding scale of the conventional encryption techniques as in [55, 56] where the researcher created a compact version of AES encryption and optimized power and size efficiency. Although no extreme requirements and specifications are defined for lightweight cryptography algorithms, usually include one or more of limited hardware execution scale, the low computing capacity of microcontrollers (microprocessor); Low deployment costs and decent protection [57, 58].

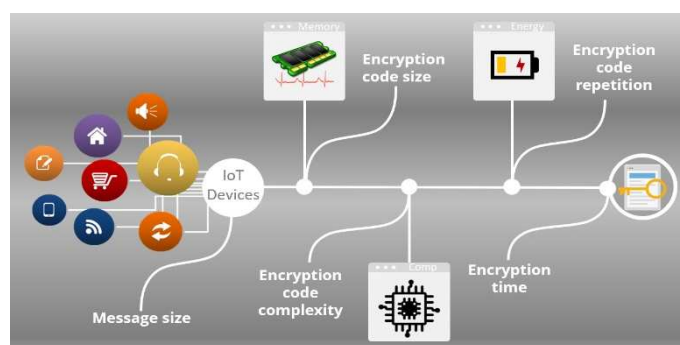


Figure 1. Encryption Code Impact on IoT Device Parameters.

The consideration of IoT devices requirement of minimizing the effect on hardware resources, security has been compromised and weakened. NIST notes that lightweight cryptography is a subset of encryption intended to offer solutions for applications typically involving smart low-powered devices [59, 60].

2) **Combined Encryption Technique:** The combined encryption technique was found to resolve the simplicity of lightweight encryption and bring some flexibility to IoT data encryption by combining two or more data encryption approaches [61, 62]. As each encryption strategy has its power and disadvantages, the unified technique aims to tackle each drawback [63]. Under the combined encryption strategy, there are two key types, i.e. hybrid encryption and cascaded encryption. The main distinction between the two groups is that: hybrid encryption splits the data into parts and uses separate encryption technique on each component. While cascaded encryption refers to a method which encrypts the entire data twice by same or different encryption techniques. The combined encryption technique has been successfully used in the research work and mostly with the watermarking techniques [62]. Hybrid cryptography attracts the interest of many researchers, as there were few stable hybrid cryptosystems offered to secure IoT devices, especially in smart cities [3].

VI. AVAILABLE SUPPORT

A. Security Guidelines

All the concerned organizations are not only responsible for providing significant resources to IoT device designers and developers but also to encourage and enable them in creating secured IoT devices capable of protecting the IoT user data [64]. Several organisations provide manuals to guide designers and developers with best practices to secure their device by design. IoT Security Foundation [65] is a non-profit organisation committed to IoT protection excellence. In their publication of Best Practice Recommendations, there is a full discussion devoted to encryption and what protocols to follow when implementing encryption for an IoT device [66]. For this purpose, they plan a conference in December 2020 for IoT designers and developers [67].

Infocom Media Development Authority IMDA [68] has an annual guideline released yearly for IoT device designers\developers and IoT users as well [69]. A discussion on cryptography and how to select a secured encryption technology was addressed in their 2019 guideline published in January 2019. In March 2020, their new guide was released. There are several other organisations of the same viewpoint as the above instances, such as European Union Agency for Cybersecurity (Anisa).

B. Researchers contribution

Many literature works have performed numerous experiments, analysis, and comparisons among various styles of encryption, and have given their conclusions in their literature to enhance the awareness of designers and developers and simplify their decisions on encryption selection. In one of the literature used raspberry pi and Arduino to test a number of symmetric encryption techniques and their effect of on energy of these devices [70]. Other paper concluded that algorithms such as RSA, 3DES, AES, blowfish and RC6 are unacceptable to be used with IoT devices because their energy consumption was higher than anticipated [50]. But the heterogeneity of the IoT environment has been neglected, and such encryption techniques could be used in certain IoT devices that have access to the power supply, as most found in smart home applications.

While other research compared the efficiency and implementation of four distinct methods of symmetric encryption and three forms of asymmetric techniques [5]. Other analysis has obtained data from the symmetrical and asymmetric encryption literature and then related the block and stream to various key sizes and numbers [46]. This study finds that block chips are additional multipurposed than stream ciphers. In other research, Raspberry Pi and Beagle Bone Black were used to test several symmetric encryption-decryption techniques and equate execution times by checking multiple blocks and stream cipher [71]. This research concluded that the encryption execution time ran faster on Raspberry pi. In [72], AES and XTEA were conducted with comparative analysis. This study was carried out to determine the possibility of using XTEA on embedded low-resource platforms.

VII. PROBLEM STATEMENT

IoT devices utilized in very wide range of environments such as healthcare, smart homes, smart city, education etc as well as its being used for different application within each environment caused the heterogeneous and constraint resources nature in IoT devices. In addition, the designers of IoT device knowledge basically comes from embedded systems, usually used in isolated systems and cybersecurity violations are not of major importance for them. Moreover, IoT devices belongs to a low-cost market that limited financial research investments. Besides all the above aspects of the challenges IoT designers face, the wide range of encryption available for IoT device with distinct impact on the IoT device parameter, selecting a suitable encryption for a particular IoT device has become a complicated task.

Taking into consideration the significance of securing the data of IoT device users in the social adoption and further development and growth of this technology, the available support to overcome this dilemma and provide designers with substantial assistance to simplify their job is not enough, Further work and commitment must be expended in this area, taking into consideration the new tools available. In this respect, we propose our model using machine learning in order to provide designers with additional assistance.

VIII. PROPOSED MODEL

The implementation of IoTES proposed model is a web-based service where the designer will access and provide his device parameters as shown in the figure 5. The model backend will run on matching the most appropriate encryption based on the IoT device information designer provides.

A. Dataset preparation.

IoTES will rely on a primary dataset which we are going to collect through several experiments. Several encryptions belonging to the four cryptography methods discussed above are going to be used. Three different message sizes will be encrypted by each encryption which will be operated on three different off shelf single board computers SBC such as raspberry pi to increase datapoints number and enhance the behaviour understanding of each encryption. The impact reading of tested encryption on SBC parameters will be

recorded, including processing power, execution time and memory usage.

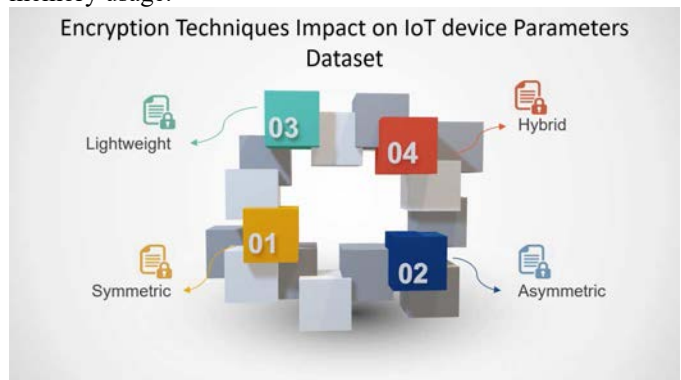


Figure 2. Data set building structure

B. Model development

Model development is the next step to dataset creation. It starts with Exploratory Data Analysis EDA where data is analysed, use different techniques to interpret the collected data to make analysis easier, more reliable and more effective. Feature Engineering plays an important role in machine learning success or failure. Features are important for predictive models. Those attributes which are useful to the model could qualify to be feature. Features should be carefully selected to reduce the curse of dimensionality and that occurs when feature space “Mathematical Space” has many dimensions and data points are spread far away from each other. Therefore depth versus breadth analysis will be conducted. The purpose of a feature, other than being an attribute, would be much easier to understand in the context of a problem. A feature is a characteristic that might help when solving the problem. Next, Dataset will be splatted into 2 segments. One is for training and the other for testing and portions will be distributed 80% and 20% respectively.

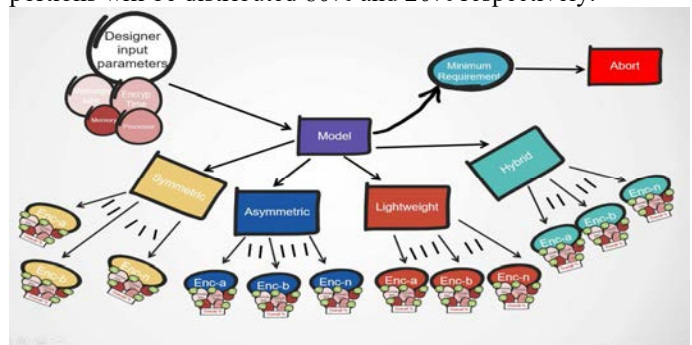


Figure 3. IoTES working mechanism.

We will be using several Multiclass classification techniques and choose the best performance outcome. Data will be validated using several techniques and tuned to help us in the selection of best fit technique for our model. Once the best performed classification technique has been selected then we will start to test the model and keep on tuning it until we reach to highest possible performance. Typically, as designers develop protection for IoT, have their own concerns and criteria.

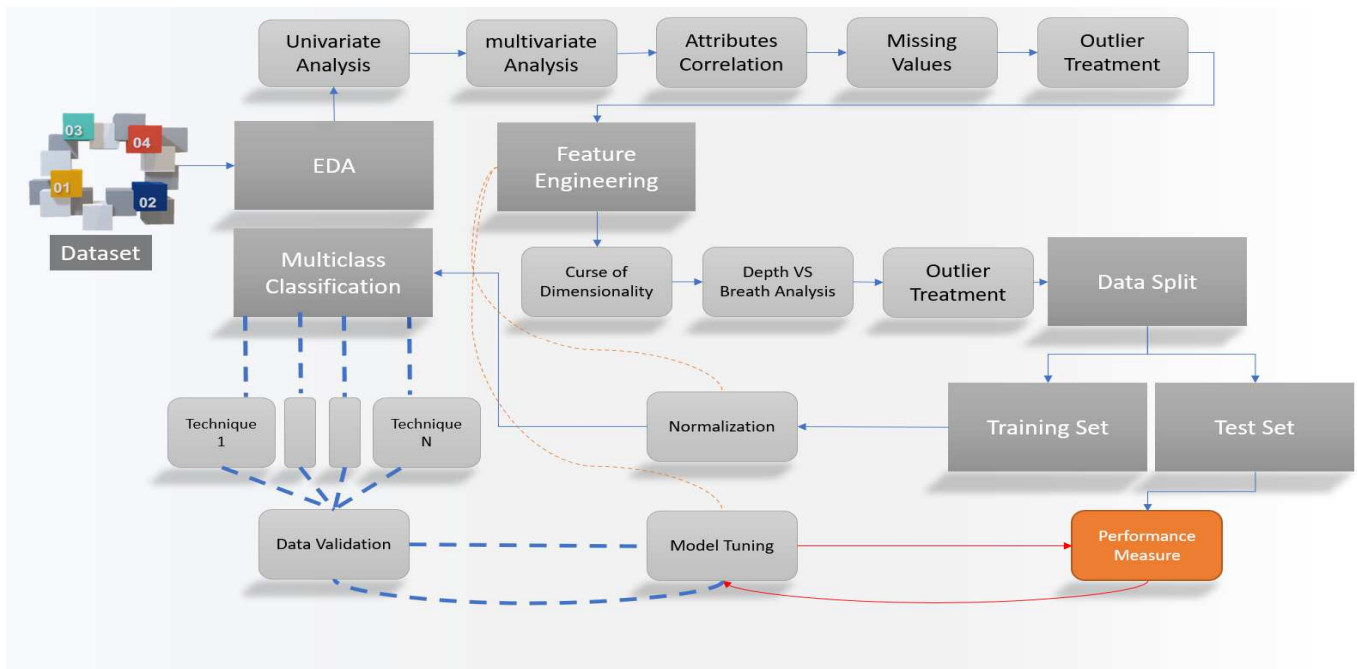


Figure 4. IoTES Model methodology

In our model, we combine the points concerning the designer and the technical aspects of selecting an acceptable encryption technique. Message size and encryption time are essential for selecting the necessary encryption, but designers may have other parameters for their IoT device, such as memory size and microprocessor/microcontroller model. In the first stage, the data generated by the IoTES user will be contrasted with the minimum data set criteria accessible, the model will abort execution if the inputs are less. This move is necessary to preserve the model output at the real level and ensure that the model performance is not adversely affected during the assessment period.

While the input fulfils the minimum requirement, the model transfer the data to all divisions and nodes until the input meet the minimum specifications. The output shall contain the total efficiency and effect on each of the input parameters of all matching encryption techniques. This offers designers the chance to determine, not just the final outcome, but on their priority criteria.

The model representation is given as in the first step, the designer enters the design parameters for a specific IoT device through a provided interface. Once the parameters are received, they are sent to the IoTES model. The model is consisting of our already designed dataset where the information and different parameters of all the IoT devices are present already. Based on the machine learning algorithm, the model decides and selects the suitable encryption mechanism for the particular IoT device. The model sends the feedback of matching encryption to the interface where designer can view and interact with the matching encryption provided options. Model representation is given in figure 5.

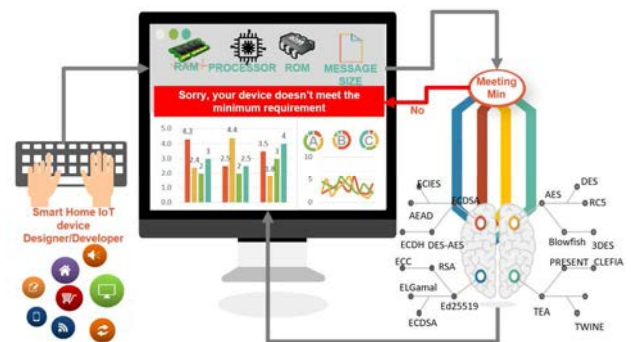


Figure 5. Model representation

IX. CONCLUSION

The lack of standardization and the flexibility of IoT device design are factors for the IoT industry to flourish and be employed in several environments and applications beside the great facilities IoT products offer at very low cost. In the other hand, most of low-price IoT devices and simpler design are being manufactured and shipped to the market and finally reached the end-user without any built-in data security. The reasoning behind this is that most IoT device designers are coming from embedded system background where these devices work in isolated, with cost-effective sensors and actuators for which security breaches are illuminated. Moreover, the broad variety of usable encryptions in IoT and dissimilar effects on device parameters complicate the selection of an appropriate encryption for a particular IoT device. These considerations go beyond IoT devices installed in smart homes or smart cities, they also address sensitive devices capable of accessing critical patient data and tracking the heart like a pacemaker implanted in the human body. Although designers face many obstacles, the task of securing IoT data is challenging. Many organisations and scholars have provided some sort of assistance. Due to the significance of securing IoT device data, further work is required

to provide more useful assistance. In this regard we have proposed IoTES model which is designed by using machine learning algorithm.

X. FUTURE WORK

Further analysis on the proposed model will be carried out. Aimed at implementing and testing IoTES model.

XI. REFERENCES

- [1] A. Rghioui, and A. Oumnad, "Internet of Things: Visions, technologies, and areas of application," *technology*, vol. 6, no. 7, 2017.
- [2] S. H. Mahmud, L. Assan, and R. Islam, "Potentials of internet of things (IoT) in malaysian construction industry," *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN, pp. 2516-0281, 2018.
- [3] A. Ragab, G. Selim, A. Wahdan, and A. Madani, "Robust Hybrid Lightweight Cryptosystem for Protecting IoT Smart Devices," *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, Lecture Notes in Computer Science, pp. 5-19, 2019.
- [4] S. J. Hussain, M. Irfan, N. Jhanjhi, K. Hussain, and M. Humayun, "Performance Enhancement in Wireless Body Area Networks with Secure Communication," *Wireless Personal Communications*, pp. 1-22, 2020.
- [5] M. N. B. Anwar, M. Hasan, M. M. Hasan, J. Z. Loren, and S. T. Hossain, "Comparative Study of Cryptography Algorithms and Its' Applications," *International Journal of Computer Networks and Communications Security*, vol. 7, no. 5, pp. 96-103, 2019.
- [6] T. Poongodi, R. Krishnamurthi, R. Indrakumari, P. Suresh, and B. Balusamy, "Wearable Devices and IoT," *A Handbook of Internet of Things in Biomedical and Cyber Physical System*, pp. 245-273: Springer, 2020.
- [7] N. Maryanti, R. Rohana, and M. Kristiawan, "The Principal's Strategy In Preparing Students Ready To Face the Industrial Revolution 4.0," *International Journal of Educational Review*, vol. 2, no. 1, pp. 54-69, 2020.
- [8] M. Humayun, N. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egyptian Informatics Journal*, 2020.
- [9] N. Jhanjhi, and A. Alhumam, "Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP," *Sensors (Basel, Switzerland)*, vol. 20, no. 21, 2020.
- [10] Z. A. Almusaylim, A. Alhumam, and N. Jhanjhi, "Proposing a Secure RPL based Internet of Things Routing Protocol: A Review," *Ad Hoc Networks*, vol. 101, pp. 102096, 2020.
- [11] M. S. Mahdavejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for Internet of Things data analysis: A survey," *Digital Communications and Networks*, vol. 4, no. 3, pp. 161-175, 2018.
- [12] S. M. Muzammal, R. K. Murugesan, and N. Jhanjhi, "A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-based Approaches," *IEEE Internet of Things Journal*, 2020.
- [13] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arabian Journal for Science and Engineering*, pp. 1-19, 2020.
- [14] J. Chen, W. Diao, Q. Zhao, C. Zuo, Z. Lin, X. Wang, W. C. Lau, M. Sun, R. Yang, and K. Zhang, "IoTfuzzer: Discovering Memory Corruptions in IoT Through App-based Fuzzing."
- [15] H. Chizari, and E. C. Lupu, "Extracting randomness from the trend of IPI for cryptographic operators in implantable medical devices," *IEEE Transactions on Dependable and Secure Computing*, 2019.
- [16] H. Atlam, R. Walters, and G. Wills, "Internet of Things: state-of-the-art, challenges, applications, and open issues," *International Journal of Intelligent Computing Research (IJICR)*, vol. 9, no. 3, pp. 928-938, 2018.
- [17] H. F. Atlam, and G. B. Wills, "IoT security, privacy, safety and ethics," *Digital Twin Technologies and Smart Cities*, pp. 123-149: Springer, 2020.
- [18] M. James, "Secure by Design: Improving the cyber security of consumer Internet of Things Report," *Department for Digital, Culture Media & Sport: London, UK*, 2017.
- [19] N. Gershenfeld, R. Krikorian, and D. Cohen, "The internet of things," *Scientific American*, vol. 291, no. 4, pp. 76-81, 2004.
- [20] S. K. Biswas, D. Devi, and M. Chakraborty, "A hybrid case based reasoning model for classification in internet of things (iot) environment," *Journal of Organizational and End User Computing (JOEUC)*, vol. 30, no. 4, pp. 104-

- 122, 2018.
- [21] S. Madakam, V. Lake, V. Lake, and V. Lake, "Internet of Things (IoT): A literature review," *Journal of Computer and Communications*, vol. 3, no. 05, pp. 164, 2015.
- [22] M. Nardelli, S. Nastic, S. Dustdar, M. Villari, and R. Ranjan, "Osmotic flow: Osmotic computing+iot workflow," *IEEE Cloud Computing*, vol. 4, no. 2, pp. 68-75, 2017.
- [23] J. I. R. Molano, J. M. C. Lovelle, C. E. Montenegro, J. J. R. Granados, and R. G. Crespo, "Metamodel for integration of internet of things, social networks, the cloud and industry 4.0," *Journal of ambient intelligence and humanized computing*, vol. 9, no. 3, pp. 709-723, 2018.
- [24] A. Haleem, M. Javaid, and I. H. Khan, "Internet of things (IoT) applications in orthopaedics," *Journal of Clinical Orthopaedics & Trauma*, vol. 11, pp. S105-S106, 2020.
- [25] S. Jacob, M. Alagirisamy, V. G. Menon, M. Kumar, N. Jhanjhi, V. Ponnusamy, P. Shynu, and V. Balasubramanian, "An Adaptive and Flexible Brain Energized Full Body Exoskeleton with IoT Edge for Assisting the Paralyzed Patients," *IEEE Access*, 2020.
- [26] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, "A Survey of Internet of Things (IoT) in Education: Opportunities and Challenges," *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*, pp. 197-209: Springer, 2020.
- [27] N. Cvar, J. Trilar, A. Kos, M. Volk, and E. Stojmenova Duh, "The Use of IoT Technology in Smart Cities and Smart Villages: Similarities, Differences, and Future Prospects," *Sensors*, vol. 20, no. 14, pp. 3897, 2020.
- [28] V. Singhal, S. Jain, D. Anand, A. Singh, S. Verma, J. J. Rodrigues, N. Z. Jhanjhi, U. Ghosh, O. Jo, and C. Iwendi, "Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned Railway Level Crossings," *IEEE Access*, vol. 8, pp. 113790-113806, 2020.
- [29] Z. A. Almusaylim, and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT)," *Wireless networks*, vol. 25, no. 6, pp. 3193-3204, 2019.
- [30] M. Saleh, N. Jhanjhi, and A. Abdullah, "Proposing a privacy protection model in case of civilian drone." pp. 596-602.
- [31] Q. Du, H. Song, and X. Zhu, "Social-feature enabled communications among devices toward the smart IoT community," *IEEE Communications Magazine*, vol. 57, no. 1, pp. 130-137, 2018.
- [32] J. Saleem, M. Hammoudeh, U. Raza, B. Adebisi, and R. Ande, "IoT standardisation: Challenges, perspectives and solution." pp. 1-9.
- [33] S. S. A. Simnani, S. Shah, and M. T. Banday, "Architectural standards for internet of things: standardising IoT architecture," *International Journal of Forensic Engineering*, vol. 4, no. 3, pp. 196-213, 2019.
- [34] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 14-21, 2015.
- [35] F. Samie, L. Bauer, and J. Henkel, "IoT technologies for embedded computing: A survey." pp. 1-10.
- [36] K. Pardini, J. J. Rodrigues, S. A. Kozlov, N. Kumar, and V. Furtado, "IoT-based solid waste management solutions: a survey," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, pp. 5, 2019.
- [37] S. Zeadally, and M. Tsikerdekis, "Securing Internet of Things (IoT) with machine learning," *International Journal of Communication Systems*, vol. 33, no. 1, 2020.
- [38] S. Zeadally, and M. Tsikerdekis, "Securing Internet of Things (IoT) with machine learning," *International Journal of Communication Systems*, vol. 33, no. 1, pp. e4169, 2020.
- [39] C. Corsi, "History highlights and future trends of infrared sensors," *Journal of modern optics*, vol. 57, no. 18, pp. 1663-1686, 2010.
- [40] M. Jiménez, R. Palomera, and I. Couvertier, *Introduction to embedded systems*: Springer, 2013.
- [41] S. Kok, A. Azween, and N. Jhanjhi, "Evaluation metric for crypto-ransomware detection using machine learning," *Journal of Information Security and Applications*, vol. 55, pp. 102646, 2020.
- [42] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? a survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182-8201, 2019.
- [43] Y. Wang, S.-F. Sun, J. Wang, J. K. Liu, and X. Chen, "Achieving Searchable Encryption Scheme with

- Search Pattern Hidden," *IEEE Transactions on Services Computing*, 2020.
- [44] M. James, and D. S. Kumar, "An implementation of modified lightweight advanced encryption standard in FPGA," *Procedia Technology*, vol. 25, pp. 582-589, 2016.
- [45] S. Roy, U. Rawat, H. A. Sareen, and S. K. Nayak, "IECA: an efficient IoT friendly image encryption technique using programmable cellular automata," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-20, 2020.
- [46] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey." pp. 0475-0481.
- [47] E. Setyaningsih, R. Wardoyo, and A. K. Sari, "Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution," *Digital Communications and Networks*, 2020.
- [48] A. Patil, and R. Goudar, "A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices," *International journal of scientific & technology research*, vol. 2, no. 8, 2013.
- [49] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," *Wireless Personal Communications*, 2020.
- [50] A. Hameed, and A. Alomary, "Security Issues in IoT: A Survey." pp. 1-5.
- [51] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, "Cryptography: A Comparative Analysis for Modern Techniques," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, 2017.
- [52] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-18, 2017.
- [53] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375-1384, 2016.
- [54] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26-33, 2017.
- [55] J. J. Tay, M. M. Wong, and I. Hijazin, "Compact and low power aes block cipher using lightweight key expansion mechanism and optimal number of s-boxes." pp. 108-114.
- [56] T. Sharma, "Lightweight Encryption Algorithms, Technologies, and Architectures in Internet of Things: A Survey," *Innovations in Computer Science and Engineering*, pp. 341-351: Springer, 2020.
- [57] S. Surendran, A. Nassef, and B. D. Beheshti, "A survey of cryptographic algorithms for IoT devices." pp. 1-8.
- [58] M. Humayun, N. Jhanjhi, M. Alruwaili, S. S. Amalathas, V. Balasubramanian, and B. Selvaraj, "Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things," *IEEE Access*, vol. 8, pp. 183665-183677, 2020.
- [59] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Nistir 8114: Draft report on lightweight cryptography," *Available on the NIST website: http://csrc.nist.gov/publications/drafts/nistir-8114/nistir_8114_draft.pdf*, 2016.
- [60] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman, and Y. Nam, "Lightweight authenticated-encryption scheme for Internet of Things based on publish-subscribe communication," *IEEE Access*, vol. 8, pp. 60539-60551, 2020.
- [61] S. Mocanu, A. Duluta, D. Merezanu, and R. Pietraru, "Improved Security Based on Combined Encryption and Steganography Techniques," *Studies in Informatics and Control*, vol. 26, no. 1, pp. 116, 2017.
- [62] C. Pradhan, B. J. Saha, K. K. Kabi, and A. K. Bisoi, "Robust watermarking technique using 2d logistic map and elliptic curve cryptosystem in wavelets," *International Journal on Recent Trends in Engineering & Technology*, vol. 10, no. 2, pp. 70, 2014.
- [63] T. N. Phu, and Y.-C. Lee, "Encryption Algorithm Selection to Protect IoT Devices from Local Network Attacking using Analytic Network Process and BCR Model," *Journal of Engineering and Applied Sciences*, vol. 12, no. 24, pp. 7453-7457, 2017.
- [64] M. R. Warner, C. Gardner, R. Wyden, and S. Daines, "Internet of Things Cybersecurity Improvement Act of 2017." p. 1691.
- [65] I. S. Foundation, "IoT Security Foundation," *IoT Security Foundation 2015 - 2020 website: <https://www.iotsecurityfoundation.org/about-us/>*.
- [66] I. S. Foundation, "IOTSF Best Practice Guide," *IoT*

Security Foundation 2015 - 2020.

- [67] I. S. Foundation, "IoT Security Foundation Conference," *IoTSF Conference*, <https://iotsfconference.com/>.
- [68] "Infocom Media Development Authority IMDA" 2020, *Infocomm Media Development Authority*. Last updated 22 May 2020m website: <https://www.imda.gov.sg/Who-We-Are>.
- [69] "Infocomm Media Development Authority IMDA Guidelines," 2020, *Infocomm Media Development Authority*. Last updated 13 Mar 2020.
- [70] M. El-Haii, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of cryptographic algorithms on iot hardware platforms." pp. 1-5.
- [71] N. Kumar, and N. Reddy, "ESTIMATION OF CRYPTOGRAPHIC APPROACH ON IoT DEVICES," 2019.
- [72] S. Maitra, D. Richards, A. Abdelgawad, and K. Yelamarthi, "Performance Evaluation of IoT Encryption Algorithms: Memory, Timing, and Energy." pp. 1-6.



Matasem Saleh is a Ph.D. scholar at Taylor's University, Malaysia. There, he is working as a researcher in the area of Drone Detection System, Privacy Protection and IoT security. He has worked in industry for a decade as Telecom Project Manager in EmaarAltelal, Saudi Arabia. Obtained his MSc in Computer Engineering from the University of Engineering and Technology, Pakistan in 2008, where he developed FlocARe, an open source network management software.



Dr Noor Zaman received his Ph.D. degree in IT from UTP, Malaysia. He has great international exposure in academia, research, administration, and academic quality accreditation. He was with ILMA University, King Faisal University (KFU) for a decade. He is currently with Taylors University, Malaysia. He has 19 years of teaching and administrative experience. He has an intensive background of academic quality accreditation in higher education besides scientific research activities. He had worked a decade for academic accreditation. He received ABET accreditation twice for three programs from CCSIT, King Faisal University, Saudi Arabia. He also worked for National Commission for Academic Accreditation and Assessment (NCAAA), Education Evaluation Commission Higher Education Sector (EECHES) formerly NCAAA Saudi Arabia, for institutional level accreditation. He also worked for National Computing Education Accreditation Council (NCEAC). Dr. Noor Zaman has been awarded the top Reviewer 1% globally by WoS/ISI (Publons) recently. He has edited/authored more than 11 research books with international reputed publishers, received several research grants, and a great number of indexed research articles on his credit. He has supervised several postgraduate students, including master's and Ph.D. He is an Associate Editor of IEEE ACCESS, Keynote speaker for several IEEE international conferences globally, External examiner/evaluator for Ph.D. and master's for several universities, Guest editor of several reputed journals, a member of the editorial board of several research journals, and an active TPC member of reputed conferences around the globe.



Developer and a IT/MIS consultancy and training.

Dr Azween Abdullah is currently working with Taylor's University. He is currently a Professional Development Alumni of Stanford University and MIT. His work experience includes 30 years as an academic in institutions of higher learning and as the Director of research and academic affairs at two institutions of higher learning, the Vice-President for educational consultancy services, 15 years in commercial companies as a Software Engineer, a Systems Analyst, and as a Computer Software



Raazia Saher is a lecturer at King Faisal University in the Department of Computer Science and Information Technology. She has over 10 years of academic experience in this prestigious institution. She has a master's degree in electrical engineering and is a registered professional engineer in Pakistan Engineering Council. She acquired specialized skills in Next Generations Networks & Soft Switches while working as an operational engineer in Pakistan Telecommunications Company Limited.