International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 12 (2020), pp. 5149-5165
© International Research Publication House. http://www.irphouse.com

Design Challenges of Securing IoT Devices: A survey

Matasem Saleh[1], NZ Jhanjhi[2], Azween Abdullah[3], Raazia Saher[4]

[1]Research Scholar, School of Computer Science and Engineering, SCE, Taylor's University, Subang Jaya, Malaysia.

[2,3]Associate Professor, School of Computer Science and Engineering, SCE, Taylor's University, Subang Jaya, Malaysia.

[4]Lecturer, College of Computer Science and Information Technology (CCSIT), King Faisal University, Saudi Arabia.

ORCIDs: [1]0000-0003-4987-2013, [2]0000-0001-8116-4733, [3]0000-0003-4425-8604, [4]0000-0001-7095-5628

Abstract

Conferring to United Nations (UN) projections, by 2050, 68% of global population would be living in cities. Present resources and facilities for appropriate urban living conditions are becoming extremely daunting for the metropolitan population's needs. Fortunately, IoT, along with communication technology and some innovations, paved the way for smart cities to develop and grow. The data collection ability of IoT devices using sensors has made multiple data sources accessible. Furthermore, 90 percent of all IoT data will be saved in third-party databases in the next five years. This is one example of why organizations have to follow an "encrypt-everything" approach to protect the data of their IoT devices. IoT devices are diverse in their hardware design, lack proper standardization and have a resource constraint nature which makes them less efficient at processing complex algorithms. The IoT carries a new traditions of security anxieties. Contrasting VPN encryption, which protects networks with an anonymous tunnel and encryption, the IoT devices essentially need to be inbuilt with their specific robust security and encryption standards. Many encryption methods are already existing for IoT devices. However, each encryption approach has its advantage and disadvantages. The best-fit encryption method will depend on IoT device design which differs from one design to another. Hence, choosing encryption that complies with specific hardware among various encryption techniques is challenging for hardware designers. IoT device designers and developers shoulder the highest responsibility to secure their devices from malicious activities; therefore, they need guides to ensure that they can do their job correctly. This paper highlights the difficulties encountered in choosing a device dependant suitable encryption method for IoT devices.

This paper is meant to point out why selecting suitable encryption for a specific device is difficult.

Keywords: IoT, System Security, IoT Device Security, Cryptography, System Design.

I. INTRODUCTION

Internet of things (IoT) is a leading technology which innovates human lives. The revolution in IoT integrating the use of robots in numerous ordinary life applications makes embedded IoT have a tremendous impact on the forthcoming social growth. The IoT intents to refine the eminence of subsequent social things comparable to urban life by gathering private data, pursuing human activities, plotting them with numerous sources of information. IoT aims to link billions of objects like actuators, sensors, RFID, etc., to make this technology a significant facet in our daily work and life. The IoT might accentuate societal values of equality, trust, privacy, discrete choice and their operations. Internet of things (IoT) technology has won the ground quickly[3]. The secret behind IoT's fame is that it changes people's lives through innovative applications and launches the modern application of this technology. Certainly, IoT is a perception that not only inspires our lives but also has a tremendous impact on how we work. This technology can prominently expand user protection, electricity utilization, edification, health, and various areas of daily life [4, 5]. It can also improve trade, supply chain management, engineering, agriculture, and supplementary sectors' decision-making and affordability by refining solutions [6]. IoT refers to billions of physical devices around the globe with Internet connectivity, all of which gather and share data. IoT devices are increasing rapidly, where Statista expected more than 75.440 billion of devices, "Things," would be linked to internet till year 2025 [7]. This explosive growth is due to low-cost computer chip production and the proliferation of communication technology [8, 9]. IoT devices contain sensors, capture and analyse information from their environment and send it for further analysis to remote locations. IoT is an extensive variety group of heterogeneous devices, owing to the disparity of the environment where it is deployed and the purpose of deployment. Moreover, the environment where IoT devices can be mounted limits their scale and resource capabilities. Therefore, we may find an IoT device under the soil to sense moisture, or we may carry an IoT tracker to monitor our activities. While IoT devices are of wide variance and diversity, they are still similar in many characteristics; for example, all IoT devices are intended to capture and share data along with constrained resource capabilities (computational power, memory size, and energy) [10-12].

Resource limitation ultimately will limit the software installed on them. Therefore, the software which is supposed to facilitate the IoT devices has to be a lightweight to meet resource restrictions. Since IoT devices are mainly designed to handle and transmit data over internet without human supervision, they are susceptible to the risk which any device connected to the internet might face. The data collected via these devices in smart cities mostly related to health monitoring such as blood pressure, heartbeat or tracking body activity, and home automation such as temperature and moisture details, power consumption trends. Due to the information type, they store, they are primary targets for attackers. More ever, increasing demand for IoT technology has fascinated hackers to concentrate their efforts to exploit and gain control of these devices and data emanating from them. To prevent this adverse circumstance, IoT devices should be secured from internal and external threats. Encrypting the messages generated by IoT devices is essential, taking into account data importance that eventually increases every day [13, 14].

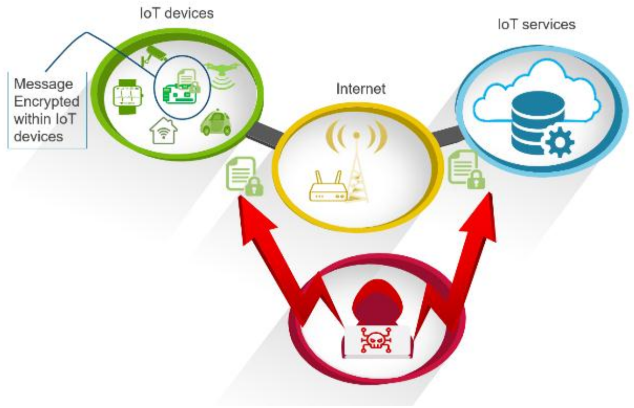


Fig. 1. Built in device data encryption advantage

IoT device designers and developers bear a great deal of responsibility in order to provide a secured and safe device without compromising their efficiency. Therefore, many researches guide the designers and developers in selecting suitable encryption as per their design requirement keeping in mind the device efficiency. Besides the published researches, there are periodically released guidelines by different organizations for the same purpose. These kinds of guidelines are being released frequently not only to help the designer and developers in choosing but also encourages them to test their device security as well. HP security research analyzed and observed that 70 percent of the devices are susceptible to system attack because IoT devices are generally not adequately checked and do not practice conventional encryption methods [15].

I.I Research Contribution

Encrypting the data transmitted by the IoT devices is crucial. It increases the level of confidence and trust of IoT device user, by ensuring that the collected data is guarded from being exposed to any unauthorized entity which will eventually contribute to an acceleration in the social adoption of this technology. Data encryption within an IoT device at software level poses a challenge for IoT device designers for several reasons. This research thoroughly discusses those details. Numerous organizations and researchers have contributed in providing different forms of support to guide the IoT device designers which has also been conversed in this paper.

I.II Paper Organization

This paper has been organized into three main sections:

II. Literature review

This section provides a detailed insight into the challenges faced by the IoT device designers while choosing suitable encryption method for their devices.

III. A Critical review of Encryption

Several types of encryptions are available for IoT devices. In this section four main classes of encryptions have been discussed.

IV. Available support

In an attempt to choose the finest device compatible encryption method for the IoT devices, the designers have confronted countless obstacles. Some organizations and researchers came to the rescue and provided certain guidelines for these designers which can be considered by them to achieve their goals. These attempts have been discussed in this section.

II. LITERATURE REVIEW

II.I IoT Security Concerns

The IoT smart services, including smart houses, smart vehicles and smart medics have protracted to daily life, moving the intimidations of the present virtual environment to the corporeal world [16]. Stress-free hacking not just endures in the virtual environment, but it can be rolled into a way of life, such as a house, medical equipment, and smart vehicle, which can meaningfully influence human life from daily life. Consequently, not just cybersecurity however also the protection of daily life should be deliberated—the security issues declined at the pace of the design and development of an IoT. Attackers might be using numerous techniques in distinctive layers to the attack on an IoT network. As an IoT advances, the cyber-attacks are fitting into the physical threats. The security of data is becoming a major priority deliberation for the system designing of each IoT network. Several manufactures did not set security standards for their products; some devices use their own standards of security that are not compatible with other manufactures' products. The old versions of devices don't have security measures at all [17]. Computer-controlled devices in automobiles such as breakers, engines, locks, and dashboards have been shown to the vulnerable to attackers who have access to the network. Because the IoT is a rich source of data, it will always be vulnerable to sophisticated attacks.

Unlike conventional embedded devices, users monitor most IoT devices through mobile apps. An IoT app is deliberate to exploit the control panel of device, and thus transmits rich info of the concerning device, predominantly the approach to communicate to its firmware. Exemplars of such evidence comprise authority (seed) communications and URLs [18]. Grounded on the report available by White Scope, approximately 8000 susceptibilities have been discovered in observing only seven models of pacemakers. The foremost explanations for this great number of vulnerabilities were, initially, not exercising encryption methods at all [17]. Several vendors use non-standard functions for encryption to encrypt the messages [18]. Storing in IoT device is not generally considered with security apprehensions, and most companies may supervise these. Data might be conveyed over a protected commercial network. However, the data at both ends (destination and source) might be in cleartext (unencrypted). The end-to-end encryption is crucial when collaborating amongst devices [19]. Discretion for the data storage data and diffusion is at a high level [20].

II.II Significance of design for security operations on IoT devices.

Social adoption of IoT technology and its services greatly relies on information security and privacy[21]. Meanwhile the IoT is a dynamic, heterogeneous device, it has many privacy and security challenges. Presently, developing an efficient and secure IoT device is the top priorities [7]. Furthermore, IoT protection is considered the most essential to avoid the IoT (and its components) from emitting physical harm or unwanted danger and to guard the atmosphere from huge damage. Construction of an IoT devices having embedded protection and consistency features must be cogitated to build novel design architectures that ensure a secure and trustworthy system. Moreover, ethical system development is required to guarantee that the IoT is utilized for the benefit of mankind. A clear ethical framework would empower enterprises to develop better, socially inclusive devices to prevent algorithmic challenges and maintain global connectivity health.

Security by design is an innovative method proposed by many organizations to incorporate necessary security controls in the life cycle of software and hardware creation, not after discovering a breach. The need for security by design befits necessary to protect billions of devices which are not protected against popular security attacks. As these machines are linked to internet, they are a weak point that any security intruder may leverage to capture confidential information or interrupt service. Also, most of these devices were designed without protection, rendering them simple targets for security attackers [22]. Relying a lot on consumer understanding, knowledge, and awareness of security has proven to produce multiple bugs and risks which can impact people's lives. The security implemented for the system designing phase can aid the user to recognize IoT security necessities and inspires them to make the correct verdict that guarantees their safety [23]. Security based on the design of the IoT device assists in constructing the device security. The UK government request this concept in novel products to tackle IoT security needs. The command claimed that companies must assimilate adequate security hooked on their IoT devices to guard them against any possible threats [24].

Government is also considering offering encouragements for the IoT industries; this will endorse the described idea for traders and deliver additional information about the built-in security (on devices) for users at acquisition. Their approach involves inspiring corporations and developers to construct protection narratives into their products from start, to guarantee that the linked devices are protected equally in the design phase and during the cycle of diverse products. Nevertheless, the utmost didn’t use thorough security info to minimalize the security risk[25]. Selecting an encryption technique suitable for IoT devices is Included in security by design. But this is not a simple task for IoT device designers and developers. In the below section, we will discuss the reasons behind making the task of selecting a suitable encryption technique a difficult task.

II.III IoT Heterogeneous Environment

Internet of things (IoT) is an internetworking of (physical) devices[26, 27] integrated with electronics, software, and data sharing [28] (also known as smart devices). In short, IoT turns physical objects into intelligent tools to capture, track, and interpret information in real-time from their environments[29]. IoT links devices over the internet with a unique IP address for each device that allows remote monitoring and controlling via cloud-based control systems [30, 31]. IoT's mission is to simplify several aspects of our lives while increasing process efficiency[29]. Currently, the usage of IoT devices is growing rapidly[32] and being used in very various domains. Different domains are deploying IoT in their fields is for a different reason. For example in case of deploying IoT in the retail industry is to improve customer experience and add more valuable services [33], as a recently conducted study[34] concluded that IoT services substantially influence consumer loyalty and experience. Although this study finds that IoT technologies are already being utilized in the payment market in retail, followed by consumer applications and indicating that the customer's purchasing experience can be improved by introducing new IoT services. While IoT uses in medicine, medical treatments and purposes [35] are vast more and used for much more lucrative benefits such as remote patient monitoring, provide accurate information for analysis and treatment, and treatment efficiency enhancement[36].

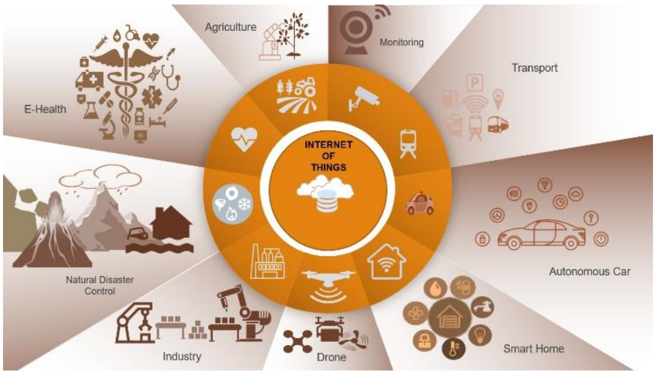


Fig. 2. Versatile IoT environment

IoT has also begun to be implemented in the areas of education for learning, training, and management advancement. Several higher training institutions all around the globe, embraced IoT to carry substantial efficiency improvements [37, 38]. In smart cities and smart villages, IoT is being used in Electricity, transportation, and mobility, smart construction, everyday life, government, economy, and society[39]. While in smart homes, IoT is used for home automation, monitoring, energy-saving, controlling appliances remotely, and entertainment. IoT is found in many other domains such as Natural disasters, agriculture[40], social domain[41] etc. The IoT inventions would improve as a consequence of the steady progress in ; communications, cloud-computing, sensors, nano electronics, smart objects and big data [37]. IoT deployment in various domains generated a heterogeneous behaviour for IoT devices being used and made standardization an impossible task. The absence of standardization is one of the restricting factors for choosing an encryption technique and prevents from labelling the best encryption technique for IoT devices is the absence of standardization in their design [42, 43].

II.IV IoT Application

As the environment where IoT has been deployed created the heterogeneity feature, the vast applications being used caused device limitations, which ultimately limited their capabilities and caused its constrained resources nature[44]. IoT devices are small in size and can be embedded in other systems[45] as well as standalone devices as CCTV camera. Based on the application IoT used for, the type of sensor or actuator is going to be used will differ. When IoT devices are embedded in other systems, designers have to be restricted to the main system requirement as in device size and power supply, which will reflect on the processor efficiency and memory size, which caused constrained nature for IoT devices. The area of nanotechnology has advanced considerably in recent years, which allowed the IoT devices designers to minimize to adjust its attributes to make it useable for the specific application. Besides the variety of sensors and actuators, which can be utilized[46]. The emergence of smart transducers has improved the electronics specifications[47]. The usage of sensors in an IoT devices certainly escalate the operations of the devices[48]. IoT device functionality and design determine the type of sensor used. Various sorts of sensors could be introduced in IoT applications, and several can be installed in a system based on the application area. These include body sensors, weather sensors, and car sensors, for example [49, 50]. Sensors implementation in IoT devices suffers from a lack of standardization [51]. The wide range of used parts and resources is considered as a positive characteristic in term of embedding these devices which make them applicable to be used in a wide variety of systems and several environments [52]. Setups of this kind require a customized encryption technique for each IoT device [50, 53].

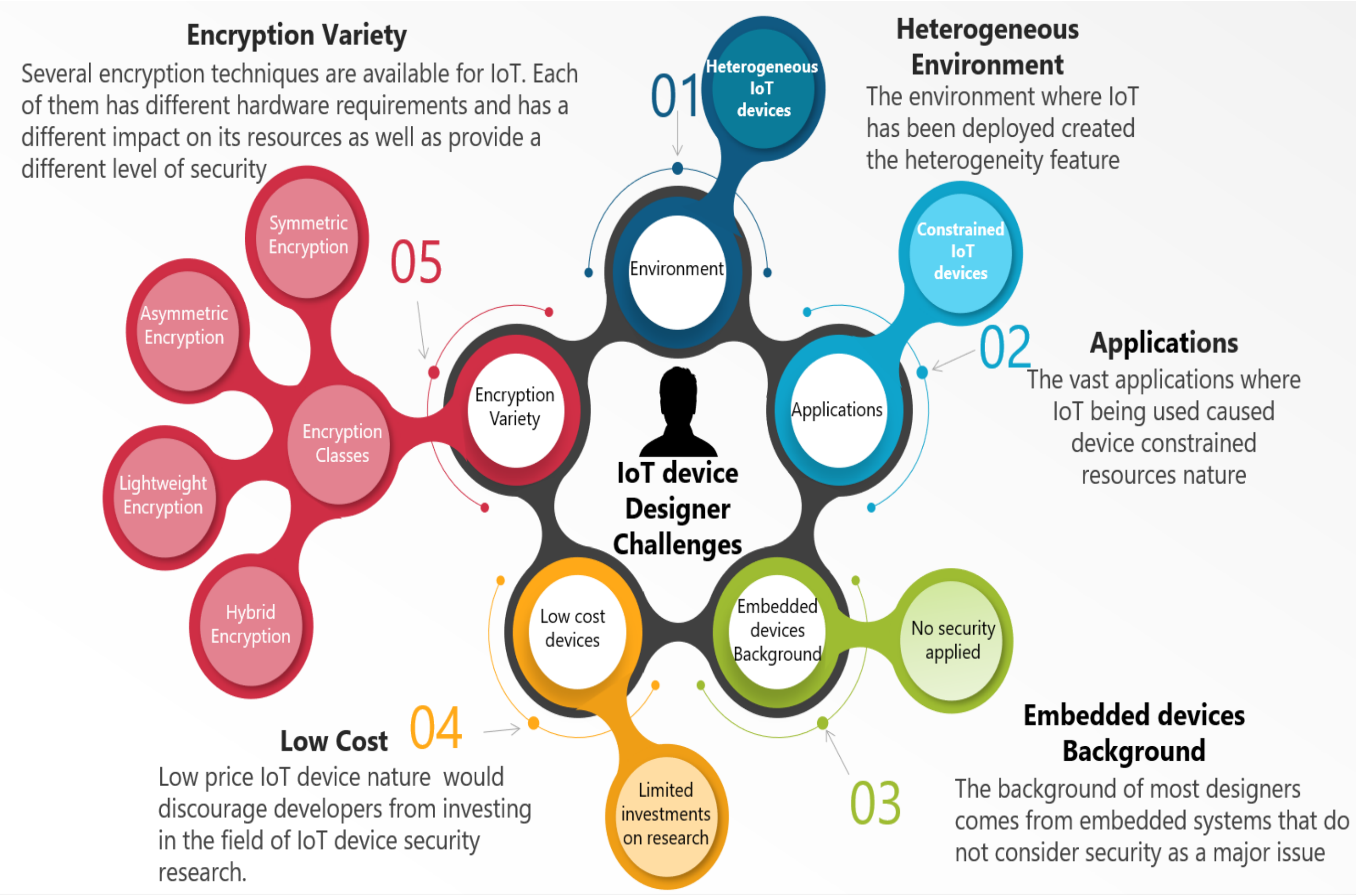

Encryption Variety
Several encryption techniques are available for IoT. Each of them has different hardware requirements and has a different impact on its resources as well as provide a different level of security
01
Heterogeneous IoT devices
Heterogeneous Environment
The environment where IoT has been deployed created the heterogeneity feature
Environment
Constrained IoT devices
05
Symmetric Encryption
Asymmetric Encryption
Encryption Classes
Lightweight Encryption
Hybrid Encryption
Encryption Variety
02
Applications
The vast applications where IoT being used caused device constrained resources nature
Applications
IoT device Designer Challenges
Low cost devices
Embedded devices Background
No security applied
Limited investments on research
04
Low Cost
Low price IoT device nature would discourage developers from investing in the field of IoT device security research.
03
Embedded devices Background
The background of most designers comes from embedded systems that do not consider security as a major issue

Fig. 3. IoT device designer challenges.

The hardware problem with power and storage limitation also demanded management from the designer [54]. But some software is still very heavy and hard to be used or handled within IoT devices. IoT devices appear to have minimal computing resources to reduce their costs and energy consumption. Computational limitations often limit access to services that can run on IoT devices. Storage in some IoT devices is the least available resource. The discussed hardware limitations affect the form of encryption technique that could be utilized to defend IoT devices [50, 53].

II.V Transformation form Embedded systems to IoT

Typically, the embedded system can be defined as a computer that comprises hardware and software that are intimately allied for a specific purpose, part of a larger system, not designed to be individually programmable by the consumer, and can operate with or without minimal human intervention [55]. The first embedded computer system was implemented in 1974 by using a single-board computer and microcontrollers and incorporated into a bigger device [48]. The basic foundation of IoT is embedded systems, and the main exception is that they do not have direct access to the internet, even though the internet was released earlier in 1969, the IoT was firstly used in 1984 even before the name was known when the coke press remained allied to the internet to record the supply and temp of drink [49]. In 1990 Mark Weiser introduced the idea of ubiquitous computation. The ubiquitous computing used sophisticated embedded computers to be involved in everything, but unseen [50]. Later the fundamental concept of IoT was introduced when sensor nodes were built to detect the data of specific embedded devices and share them seamlessly [1, 12, 51]. Bill Joy has introduced Device to Device communication for the first time in 1999 in his taxonomy of the internet, and Ashton used for the first time the word 'Internet of Things' [52, 53].

As history shows that IoT devices are the result of embedded systems development [6]. Therefore the background of most designers comes from embedded systems that do not consider security as a major issue because embedded systems basically were used in closed and isolated systems without any internet connection[56].

II.VI IoT Devices Costs

In addition to the substantial increment in IoT devices' numbers and their deployment in several domains, which are projected to reach some IoT predictions, they have had a huge positive influence on the global economy. However, the prediction statistics are very different. Gartner forecasts it to be 2 trillion USD by 2025 [36], while McKinsey believed that internet of things (IoT) will escalate from US$ 4 trillion in 2025 to US$ 11 trillion in 2025. [35], and IDC sees a reward of 1.7 trillion in 2020 [37]. The amplified number of IoT devices has an additional fact in the price drops. In [57] shown the drop in Single sensor pixel cost from 1960 (the worth was 100,000 euro, to 2010 (the price was 0.02 euro) with a reduction of more than 10^6. This price drop would discourage IoT device developers from investing in the field of IoT security research.

III. A CRITICAL REVIEW OF ENCRYPTION

Encryption is a mechanism in which information is kept hidden from people not allowed to see or modify it [58]. The encryption techniques started with the famous "Caesar Cipher" and have since then evolved to more advanced algorithms that are very secure and not prone to frequent attacks. There are several techniques available for IoT. Each of them has different hardware requirements and has a different impact on its resources as well as provide a different level of security, which make the selection of encryption is very hard.

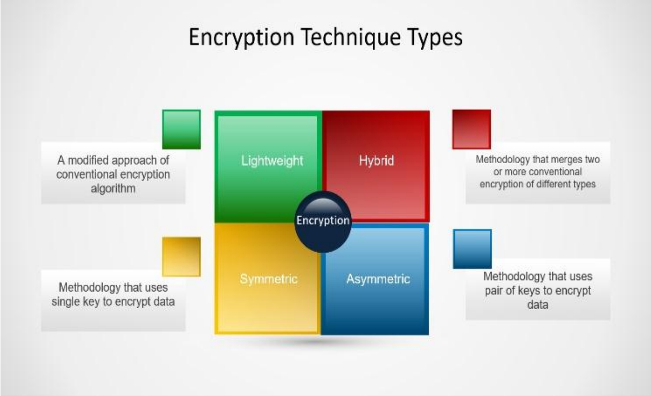

Encryption Technique Types
A modified approach of conventional encryption algorithm
Lightweight
Hybrid
Methodology that merges two or more conventional encryption of different types
Encryption
Methodology that uses single key to encrypt data
Symmetric
Asymmetric
Methodology that uses pair of keys to encrypt data

Fig 4: Encryption Types

III.I Conventional Encryption Techniques

The two standard forms of conventional encryption techniques, symmetric (public key) and asymmetric (private key) encryption methods are primarily designed to achieve a higher level of security and neglected system capability parameters such as AES is suitable for hardware and software delivery of 128,192,256 main sizes [59]. IoT devices size is their trademark; designers are forced to minimize devices' resources, i.e., memory, energy, and computational power, to reach the required size. Therefore, IoT devices are known as resource-constrained devices, which ultimately minimize their capability of processing normal code size [60]. Hence, IoT devices cannot use conventional encryption in many cases [61, 62]. Furthermore, most of these encryption techniques consume a considerable amount of power while running [63]. There are two diverse types of conventional encryption, and they are discussed below.

III.I.I Symmetric Encryption

A receiver and sender, both assign a conjoint key over stealthy communication. Symmetric encryption is known for its easy operations[64], primarily XOR and permutations, as well as processing speed is quicker and not use much energy [62, 65] that's why it is considered to be better suited for IoT applications [66]. Block ciphers and stream ciphers can play a significant part in the distinction between the different encryption techniques lay under symmetric encryption. There are several encryption techniques under this category, such as AES, while RC2 is the most power-consuming encryption, though the lowest is blowfish.

III.I.II Asymmetric Encryption

This method requires a pair of public and private key for encryption and decryption respectively. Recently, lightweight cryptography moved to asymmetric-key cryptography, nevertheless tests are not as stable and successful as symmetric key cryptography. An asymmetric algorithm are operationally complicated and time consuming. The scale of operands & the constant progress of the attack models render such algorithms susceptible. There are several encryption techniques under this category, such as RSA, DSA, and ECC.

Symmetric encryption solutions deliver efficient methods and cost effective for data protection deprived of negotiating security[65]. Allocating a secret key, though is a risk. Asymmetric systems address the key distribution question in cryptography, however they are reluctant to symmetric encryption and use more resources. [67]. So, symmetric and asymmetrical encryption methods in conjunction are one of the best possible encryption solutions. In [66] provided a table of evaluation between asymmetric and symmetric encryptions, as shown in table 1.

In addition, there are multi types of the Block Ciphers including Data Encryption Standard (DES), Advanced Encryption Standard (AES), 3DES, Twofish and Blowfish. Researchers followed various techniques to make them lightweight and to make them suitable for IoT devices. Table 2 shows a simple evaluation amongst different block ciphers and some of the other trivial block ciphers like Curupira, RECTANGLE, SIMON, PRESENT, KATON, TEA, Humming Bird.

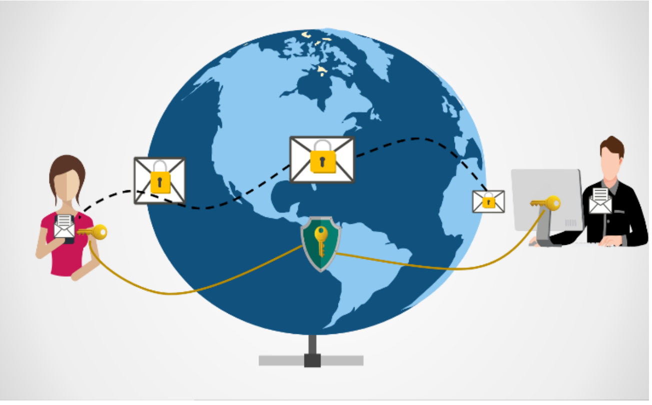


Fig. 5. Symmetric Encryption

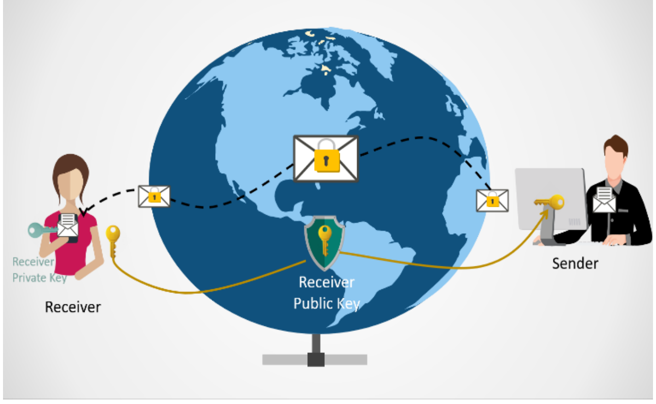


Fig. 6. Asymmetric Encryption

Table 1. Comparative analysis between symmetric and asymmetric encryption

	Cryptography Method		
	Asymmetric Key	**Symmetric-Key**	
Keys	An exclusive couple of public and private key	One shared private key.	
Number of keys	Linearly proportionate to number of users	Exponentially proportionate to number of users	
Speed and Complexity	For the diverse keys used, it needs additional time in doing transmission.	Quicker than asymmetric	
Hardware Complexity	Extra multifaceted hardware operation as it gears heavy computational algorithms which demand extra powerful hardware	Simple hardware operation as it implements algorithms with modest operations which require comparatively low-cost hardware	
Use	Distributing keys and encryption keys provide confidentiality.	Data encryption in bulk and communication paths, provides Privacy and Verification.	
Examples	ESA, DSA, ECC	Stream cipher	Trivium, Chacha, G-8, Espresso, Grain 128
		Block Ciphers	AES, DES, 3DES, Blowfish, Two fish, Curupira, PRESENT, KATAN. TEA, Hummingbird, RECTANGLE, SIMON

Table 2. Properties of different block ciphers

Block Cipher	Key size (bit)	Block Size (bit)	No. of Rounds	Characteristic
AES	128, 192, 256	128	10, 12, 14	Excellent security, flexible
DES	64	64	16	Not very secure but flexible
3DES	112,118	64	48	Good security, flexible
Blowfish	32-448	64	16	Excellent security, flexible
Twofish	128,192, 256	128	16	Can't be broken remotely
Curupira	96, 144, 192	96	96, 144, 192	Fewer space needed to stock S-boxes
PRESENT	80, 128	128	32	Fewer gate count, fewer memory for encrypting lesser amount of data
KATAN	80	32, 48, 64	256	Hardware oriented block cipher, incompetent software execution, spends high energy, little throughput.
TEA	128	64	32	Security can be boosted just by mounting the iterations.
Humming Bird	256	16	4	Appropriate for RFID tags or wireless sensor network, little power use, Excessive speed
SIMON	64-256	32-128	32-2	Easy to implement, flexible, excellent performance,
TWINE	80, 128	64	36	Ultra-light-weight, enough speed
LED	64, 128	64, 128	-	Efficient hardware implementation, used for transmission of RFID tags
RECTANGLE	80	64	25	Faster, gives high throughput, Hardware friendly,

III.II Encryption Approaches for IoT

IoT devises design is relying mostly on two main factors, IoT device's functionality and the environment where the device is going to be installed. Based on these factors, the Designer will be having a better image of how limited resources his device will be (i.e., size, energy, computation, and memory). There are numerous challenges and problems in the heterogeneous IoT environments, including energy consumption, limited batteries, performance cost, memory space and safety in ICT network [68, 69]. IoT also uses the cloud computing framework that raises various security issues and challenges. In addition, resource-restricted devices with reduced calculating power, a lesser memory, battery life, and short bandwidth need a well-organized security solution that does not crush IoT resources [70, 71]. Therefore, IoT devices don't fall under any standardization, and the designer has all the flexibility to select the items which can serve the purpose of the design. One of the items in which the designers has to choose for hid device is the type of encryption technique he is going to use. Therefore, the variety of IoT encryption techniques has to be comparable with the variety of IoT device's nature without compromising security. This means that the conventional primitive cryptography may not be appropriate for smart, low-resource devices. For instance, an RSA algorithm of 1204 bits cannot be used for RFID tags [72]. Many researchers have work on the security issues of IoT, but due to their dynamic nature, there is variation. A recent survey categorizes issues relating to security, including application, design, communication, and data. The proposed IoT security taxonomy differs from conventional architecture layers. IoT threats for hardware, networks, and application components discussed [73]. In the same way, another survey [74] discusses and analyzes security issues for IoT protocols. Security analyzes are presented in the discussion and comparison of key management systems and cryptographic algorithms. Another survey examines the contributions for privacy, security, IoT access control, and privacy as well as middleware security [75]. In addition, the tight constraints are inherent in the mass elaborations of intelligent devices that hinder the development of latest cryptographic algorithms that have a strong safety mechanism, encryption and decryption and other features for the computer industry. This growing concept of research is known as lightweight encryption [76]. In the other hand, merging two encryption technique to get the maximum pros of both is commonly used method by many researchers and test it on IoT device. Both these methods are going to be discussed in this section.

III.II.I Light-weight Encryption

Due to the inadequacy of conventional encryption techniques with IoT implementations, many researchers tended to find an effective encryption method by reducing the size of the conventional encryption techniques as in [77, 78] where the researcher produced a compacted version of AES encryption and optimized the performance in term of power and size. Lightweight encryption is a modified approach of conventional cryptographic algorithm field applicable to resource-restricted devices in IoT [78, 79]. Although no severe criteria are specified for lightweight cryptography algorithms, the features typically include one or more of limited size required for hardware execution, the low computing capacity of microcontrollers (microprocessor); low cost of implementation; and good security [80]. Despite lightweight encryption, considering the limited resources of IoT tools, it has undermined and weakened security. NIST states that lightweight cryptography is a subset of encryption, which is designed to deliver solutions for applications that engage intelligent low-powered devices in general [81]. The lightweight cryptography algorithm is supported in applications such as Wireless Sensor Network (WSN)RFID, Wireless Body Area Network (WBAN), smart cards, etc. [82]. Nearly all the presented lightweight cryptography is based on symmetric-key (cryptography), necessitating users to allocate number of symmetric keys to each of smart home IoT devices [83]. The key agreement on data encryption is an important preceding process; the more the security is improved, the more resources are used. To overcome this problem, lightweight encryption algorithm technology became important. It contains lightweight encryption algorithm and lightweight encryption protocol [79, 84].

III.II.II Combined Encryption Technique

The combined encryption approach was found to overcome the simplicity of lightweight encryption and add some complexity to IoT data encryption by integrating two encryption approaches on the same data [85, 86]. As each encryption techniques have its strength and weaknesses, the combined technique tries to deal with each of the disadvantage [87]. There are two main categories under the combined encryption technique, i.e., Hybrid encryption and cascaded encryption. The main difference between the two categories is that: hybrid encryption divides the data into parts ad apply different encryption technique into each part. While cascaded encryption applies the first encryption technique on the whole data, and then, the second encryption is applied to the cipher data resulted from the first encryption technique. The combined encryption technique has been successfully used in the research work and mostly with the watermarking techniques [86].

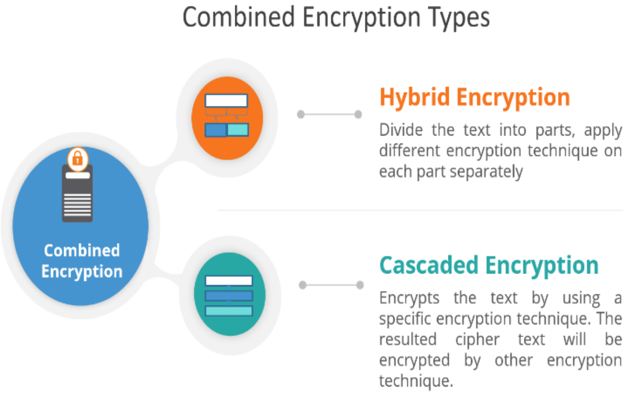

Combined Encryption Types
Combined Encryption
Hybrid Encryption
Divide the text into parts, apply different encryption technique on each part separately
Cascaded Encryption
Encrypts the text by using a specific encryption technique. The resulted cipher text will be encrypted by other encryption technique.

Fig. 7. Combined Encryption Types

The hybrid encryption fascinate the attention of many researchers, as there were few reliable hybrid cryptosystems available to safeguard the IoT devices, particularly in the smart cities [8]. Nevertheless, more related work has to be done[88]. In publications, many hybrid encryption algorithms are mentioned based on different techniques.

Hybrid encryption is a protocol that better blends several conventional encryptions of dissimilar kinds to its finest advantage. The common approach is to generate an arbitrary secret key for symmetric cipher and afterward encrypt it with the help of public key of receiver [89]. The passed message itself only authenticated with the assistance of cipher and hidden key. The encrypted secret key and authenticated message are then directed to the receiver. The user then decrypts the secret by their private key and uses it to decrypt the message [90]. In [91], a Hybrid cryptographic scheme combining a simple symmetric key algorithm (which was proposed by [92] and focused on integer and modular 37, choosing number and computing the inverted amount of the chosen integer by means of modular 37) with that RSA algorithm was suggested. Symmetric key algorithms focused on the integers and RSA algorithm is used extensively in all data security applications. The benefit of this method is that the hybrid's encryption/decryption period is less than the other algorithms. This is easier than other work when combining two different algorithms. In comparison, the disadvantage of this system is that, it only reaches authenticity and confidentiality.

Researcher in [93] has used the Advance Encryption Standard (AES) and the asymmetric-key ECC to provide a high level of protection and computational sophistication via a combination of the different encryption algorithm. The data transfer for IoT to database server is private, integrity, and non-repudiated. This approach has improved the security level as well as it is easy to comprehend and implement, but on the other hand, its downside is that AES in ROM and RAM is high during the processing time.

Hybrid encryption was proposed [94]to reduce security vulnerability, improve the encryption speed, and reduce the computational process requirements. The object of this hybrid algorithm is data integrity and confidentiality. It has used symmetric AES encryption to produce the key and asymmetric encryption NTRU to enhance security. This uses new grid reduction strategies to encrypt NTRU to find the initial key to get the original text.

In [95], The mixture of the asymmetric algorithm (RSA) and symmetric cryptographic algorithm (AES) and hate function (MD5) was conducted using a hybrid method. The three algorithms are used to uphold basic cryptography, rudimentary privacy, authentication, and reliability of data. Experiments have been conducted to appraise the projected algorithm. The result shows that the proposed algorithm has better security when it is compared to the use of AES encryption alone. Furthermore, encryption execution time was not up to a satisfactory level; therefor different encryption combination was suggested for future work. However, AES mostly has a large size impact on ROM and RAM processing, and MD5 is vulnerable to discrepancy attacks and also has a broad buffer for the retrieval of the RSA file.

A health protection model to protect the transmission of medical data in IoT environments was proposed by [96]. The model safeguards patient data by using the AES and RSA hybrid encryption algorithm. The recommended model starts by encrypting the stealthy data; then, it coats the result in a cover image with the help of 2D-DWT-1L or 2D-DWT-2L. Mutually, the gray-scale and coloured images are used as cover images to hide unlike text sizes. The proposed model demonstrated the ability to hide sensitive patient data in a strong imperceptibility, capability, and limited degradation of the obtained stego-image cover image.

In [97], A hybrid model was designed to ensure data security and privacy during transmission. The model is an application of two encryption algorithms for encrypting and decrypting messages, including the SHA1, hash algorithm, and AES. The research also addressed numerous other cryptographic algorithms and discussed why AES and SHA1 are favoured in the RFID system. The downside is that SHA1 is vulnerable to collision attacks [98].

In [99] implemented a hybrid encryption methodology utilizing symmetric algorithms AES and Blowfish. This work also profited from introducing key hashing in their model by using the MD5 hashing feature in the encryption process and make the same at the time of decryption. This will improve key protections[8]. This feature induces CPU exhaustion and memory use in double plaintext encryption.

To improve the reliability of hybrid encryption, a model was introduced [100] using the XTEA lightweight algorithm for data encryption and ECC for key encryption. PBKDF2 was used to generate the IoT key. The model is introduced for the purpose of securing the IoT wireless sensor network (WSN). The model implementation was done with the help of an Arduino kit. The downside of this method is that XTEA is got damaged, and inside PBKDF2 function, the security is reduced and increased its vulnerability to brute force attack [88].

In [101] has proposed a hyper encryption closed scheme. The scheme is featured with information security level selection as required to maintain power and improve processing speed, which is the essential requirement for IoT devices and wireless applications. The security standard of the scheme is analysed and discussed based on the combined strength of symmetric and asymmetric algorithms such as RSA and AES algorithms. A closed system utilizing tunnelling technologies for internet-sensitive application and file storage. The disadvantages of this method are that AES uses more space of the memory, and RSA requires more energy to generate RSA key [102]. It also revealed that the lightweight block cipher XXTEA outperforms AES output [88].

In [3] worked on a hybrid encryption model of enhanced XXTEA and ECC. XXTEA was enhanced to overcome its vulnerability to the related key attack by employing S-Box along with chaos system key generation.

Table 3. Comparison of different Encryption algorithm in the existing literature

Ref	Year	Encrypt-1	Encrypt- 2	Encrypt-3 or Hash	Pros	Cons
[103]	2017	AES	RSA		Stable	Low algorithm complexity, Low power efficiency
[104]	2015	AES	ECC		Less encryption decryption time, robust, low consumption of energy, low time complexity, lesser packets drop rate.	Large cipher-text
[105]	2011	Dual RSA	ECDSA and ECDH	MD5	Low computation cost • Low memory storage needs • Robust Short response time • Lightweight	ECDSA and ECDH are a bit complex to use
[106]	2015	symmetric key	Asymmetric Key	Hash Function	Efficiency rises as number of intermediary nodes rises • Great security at both levels • Quicker processing rapidity • Extra secure	More computation time
[107]	2016	AES+ECC	Dual-RSA	Hash Function	Extra robust • Hard attacked • Fewer encryption-decryption time• Small cipher-text	Not discussed
[101]	2017	RSA	AES		The scheme is featured with information security level selection as required to maintain power and improve processing speed, which is the essential requirement for IoT devices and wireless applications.	The disadvantages of this method are that AES uses more space of the memory, and RSA requires more energy to generate the RSA key. It also revealed that the lightweight block cipher XXTEA outperforms AES output
[91]	2014	the symmetric key algorithm based on integer numbers. Introduced by [80]	RSA		Encryption/decryption time of hybrid is lower as compared to the others. It is an extra secure than others by means of the combination of two diverse algorithm	The drawback of this system is that it only achieves confidentiality and authenticity.
[95]	2017	AES	RSA	MD5	Reserve authentication, privacy, and reliability of information.	AES mostly has a large size impact in ROM and RAM processing, and MD5 is vulnerable to differential attacks and also has a broad buffer for the retrieval of the RSA file.

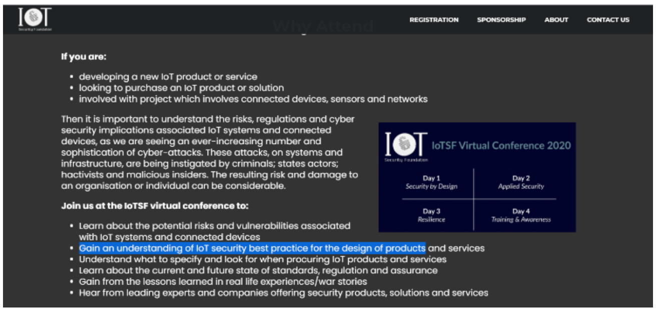
Ref	Year	Encrypt-1	Encrypt- 2	Encrypt-3 or Hash	Pros	Cons
[108]	2018	AES	ECDH		Appropriate enough for use on IoT a device without having to overload the memory usage of the device	vulnerable to MITM attacks when network layer security is poor
[109]	2017	DES	RC4		It uses one-time encryption technique, and it is appropriate for the business encryption of network terminal equipment which has only partial resources.	Low performance
[110]	2019	AES	ECC	MD5	better performance in terms of encryption and decryption time	
[94]	2017	AES	NTRU		Uses new grid reduction strategies to encrypt NTRU in order to find the initial key to get the original text.	
[93]	2015	AES	ECC		This approach has improved the security level as well as it is easy to comprehend and implement, but on the other hand, its downside is that.	AES in ROM and RAM is high during the processing time.
[99]	2018	AES	Blowfish	MD5	improve key protections	This feature induces CPU exhaustion and memory use in double plaintext encryption.
[100]	2017	ECC	XTEA		for sending a small size data such as blood pressure	XTEA is got damaged, and inside PBKDF2 function the security is reduced and increased its vulnerability to brute force attack

IV. AVAILABLE SUPPORT

IV.I Security Guidelines

The absence of standardization and simplicity of IoT device architecture are reasons for the IoT market to be flourished. Many IoT devices are giving very wonderful services and at a very low price. Indeed. On the other hand, IoT devices with low prices and simple device architecture are being produced and supplied to the market and ultimately reached the end-user without including any built-in security. The reason behind this is the fact that several IoT device producers uses low-cost sensors and actuators, which originally were built to operate in an isolated system, for which security risks are far more restricted. These reasons don't comply with IoT devices being installed in smart homes or smart cities only, but it goes beyond that as well, and it reached to very critical devices which can access critical information about patience and control their hearts as such pacemaker which are installed within the human body. There is a study saying that there were more than 8000 pacemakers available in the market and were susceptible to cyberthreats. The main reason is that these devices have been produced without having any encryption within them[17].

Indeed, there is a call of responsibility to all the concerned organizations to encourage IoT device designers and developers to produce products with built-in security during the design stage [111]. Several organizations publish guides publications to guide designers and developers with best practice to secure their design. IoT Security Foundation[112] is a non-profit organization dedicated to driving security excellence. In their Best Practice Guidelines publication, there is a complete topic dedicated to encryption and what are the procedures to be followed when adopting encryption in their design[113]. They are organizing a conference in December 2020 for the IoT designers and developers for the same purpose [1].



If you are:

- developing a new IoT product or service
- looking to purchase an IoT product or solution
- involved with project which involves connected devices, sensors and networks

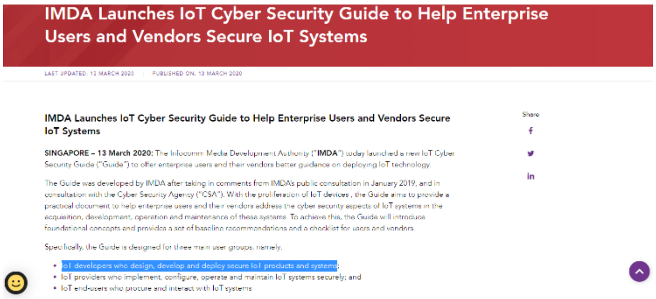
Then it is important to understand the risks, regulations and cyber security implications associated IoT systems and connected devices, as we are seeing an ever-increasing number and sophistication of cyber-attacks. These attacks, on systems and infrastructure, are being instigated by criminals; states actors; hactivists and malicious insiders. The resulting risk and damage to an organisation or individual can be considerable.

Join us at the IoTSF virtual conference to:

- Learn about the potential risks and vulnerabilities associated with IoT systems and connected devices
- Gain an understanding of IoT security best practice for the design of products and services
- Understand what to specify and look for when procuring IoT products and services
- Learn about the current and future state of standards, regulation and assurance
- Gain from the lessons learned in real life experiences/war stories
- Hear from leading experts and companies offering security products, solutions and services

Fig. 8. IoT Security Foundation 2020 conference [1]

Infocom Media Development Authority IMDA[114] has a periodical guideline published every year and meant for IoT device designers and developers and the user[2]. In their 2019 guidelines published in January 2019, they have mentioned a topic on cryptography and how to choose the secured encryption technique. Their latest guide was published in March 2020. There is much more organization have the same perspective as the examples mentioned above such as European Union Agency for Cybersecurity (Anisa) and their guidelines publication decent exercises for Security of Internet of Things in the context of Smart Engineering.



IMDA Launches IoT Cyber Security Guide to Help Enterprise Users and Vendors Secure IoT Systems

LAST UPDATED: 13 MARCH 2020 | PUBLISHED ON: 13 MARCH 2020

IMDA Launches IoT Cyber Security Guide to Help Enterprise Users and Vendors Secure IoT Systems

SINGAPORE – 13 March 2020: The Infocomm Media Development Authority ("**IMDA**") today launched a new IoT Cyber Security Guide ("Guide") to offer enterprise users and their vendors better guidance on deploying IoT technology.

The Guide was developed by IMDA after taking in comments from IMDA's public consultation in January 2019, and in consultation with the Cyber Security Agency ("CSA"). With the proliferation of IoT devices , the Guide aims to provide a practical document to help enterprise users and their vendors address the cyber security aspects of IoT systems in the acquisition, development, operation and maintenance of these systems. To achieve this, the Guide will introduce foundational concepts and provides a set of baseline recommendations and a checklist for users and vendors.

Specifically, the Guide is designed for three main user groups, namely.

- IoT developers who design, develop and deploy secure IoT products and systems;
- IoT providers who implement, configure, operate and maintain IoT systems securely; and
- IoT end-users who procure and interact with IoT systems

Fig 9. Infocom Media Development Authority IMDA launching 2020 guideline [2]

However, IoT's broad heterogeneity obstructs the creation of well-established security-by-design for IoT [115, 116]. The task is complex and challenging by the extreme limitations. Many IoT devices' power, connectivity, processing, and storage capacities. Such restrictions preclude the implementation of common protection protocols in more conventional Internet-connected devices [56]

IV.II Researchers contribution:

Many works of literature have conducted several kinds of testing, analysis, and comparison between different encryption types, and they provided their finding in their literature to increase the knowledge of designers and developers and simplify their decision on which encryption could be used. In [117] used raspberry pi and an Arduino to determine the impact of a limited number of symmetric encryption techniques on the energy of these devices. While in [63] has concluded that, the present security algorithms like RSA, 3DES, AES, blowfish, and RC6 are unsuitable to work with IoT because their energy consumption was above the expected range but ignored the heterogeneity fact of IoT field and these encryption techniques could be used in some IoT devices which have access to the power supply as most of the ones used in smart homes. In [10] has compared the performance of four different symmetric encryption techniques and three types of asymmetric techniques and suggested the application of each. In [62] has collected some data from literature about Symmetric and Asymmetric Key Cryptographic solution and then compared block cipher and stream ciphers, the two different types of symmetric encryption with several key sizes and round numbers. This study has concluded that block ciphers are extra multipurpose than stream ciphers. In [118] has tested several blocks and stream cipher of symmetric encryption-decryption techniques on Raspberry Pi and Beagle Bone Black and compared their execution times. This research concluded that the encryption execution time was faster when they were running on Raspberry pi. In [119], Comparative analysis was performed with AES and XTEA. This research was conducted to evaluate algorithm output in control, and execution time, the probability of using XTEA in low-resource embedded platforms. In [66], a systematic analysis was undertaken to include an in-depth investigation of usable trivial cryptographic primitives till 2019. This paper addressed 19 lightweight stream ciphers, 21 lightweight block ciphers, 9 lightweight hash functions, and five variations of elliptic curve cryptography (ECC). Fifty-four lightweight encryptions were contrasted in their respective groups. The comparisons between encryptions were supported out in terms of chip area, energy, power, hardware, software efficiency, throughput, latency, and figure of merit (FoM). Based on their results, AES and ECC are the most appropriate for lightweight cryptographic primitives used.

V. CONCLUSION

IoT devices are suffering from cyber threats; many devices have been outsourced to market and then to end-user without including any type of encryption. Several incidents show that the absence of encryption is quite harmful to IoT devices, user's data, and ultimately it may extend to user safety. IoT device designers are shouldering the responsibility of providing safe and secured devices. Unfortunately, he/she are working in multidimensional problems where he has to consider the device limitations and its constrained nature and consider the environment as well as the performance of his device and above all, he/she has to choose the most suitable encryption for his device among hundreds of available encryption techniques with minimal effect on the performance of his device. Keeping in mind, IoT device designers are coming from embedded system background, which is a closed system, and cybersecurity is not an issue. Therefore, they don't have the required experience to make a decision. On the other hand, IoT comes from low-price markers, which discourage the developers from investing in the field of research for their device security. There are some kinds of help offered by some organizations and researchers, but this is not sufficient to solve such an important issue. Therefore, more work has to be done in this regard with the help of available technology such as Machine Learning, which is going to be our future research scope.

VI. FUTURE WORK

With the marvellous growth in IoT, the cyber risks and attacks associated with these devices have also increased intensely. Designers are on a continuous urge of securing the IoT device data. Our future work aims to propose a machine learning based model which will assist the designers in their tedious task of choosing a suitable encryption technique.

REFERENCES

[1] I. S. Foundation, "IoT Security Foundation Conference," *IoTSF Conference, https://iotsfconference.com/.*

[2] "Infocomm Media Development Authority IMDA Guidlines," *2020, Infocomm Media Development Authority. Last updated 13 Mar 2020*.

[3] A. Rghioui, and A. Oumnad, "Internet of Things: Visions, technologies, and areas of application," *technology,* vol. 6, no. 7, 2017.

[4] A. Pal, A. Mukherjee, and S. Dey, "Future of Healthcare—Sensor Data-Driven Prognosis," *Wireless World in 2050 and Beyond: A Window into the Future!*, pp. 93-109: Springer, 2016.

[5] J. Green, "The internet of things reference model." pp. 1-12.

[6] N. Sharma, M. Shamkuwar, and I. Singh, "The history, present and future with IoT," *Internet of Things and Big Data Analytics for Smart Generation*, pp. 27-51: Springer, 2019.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] M. S. Mahdavinejad, 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.

[14] 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.

[15] A. C. Chhoton, "Executing an Effective IoT Security Testing Methodology: A Complete Guideline for Device Developers," 2018.

[16] 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.

[17] 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.

[18] 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."

[19] M. A. Nematollahi, C. Vorakulpipat, and H. G. Rosales, *Digital watermarking*: Springer, 2017.

[20] C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew, and H. D. Hai, "Recent challenges, trends, and concerns related to IoT security: An evolutionary study." pp. 405-410.

[21] 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.

[22] 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.

[23] H. F. Atlam, and G. B. Wills, "IoT security, privacy, safety and ethics," *Digital Twin Technologies and Smart Cities*, pp. 123-149: Springer, 2020.

[24] M. James, "Secure by Design: Improving the cyber security of consumer Internet of Things Report," *Department for Digital, Culture Media & Sport: London, UK*, 2017.

[25] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into IoT device purchase behavior." pp. 1-12.

[26] N. Gershenfeld, R. Krikorian, and D. Cohen, "The internet of things," *Scientific American,* vol. 291, no. 4, pp. 76-81, 2004.

[27] 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.

[28] 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.

[29] 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.

[30] C. Srinivasan, B. Rajesh, P. Saikalyan, K. Premsagar, and E. S. Yadav, "A review on the different types of Internet of Things (IoT)," *Journal of Advanced Research in Dynamical and Control Systems,* vol. 11, no. 1, pp. 154-158, 2019.

[31] 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.

[32] 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.

[33] 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.

[34] V. V. Ratna, "CONCEPTUALIZING INTERNET OF THINGS (IOT) MODEL FOR IMPROVING CUSTOMER EXPERIENCE IN THE RETAIL INDUSTRY," *International Journal of Management (IJM),* vol. 11, no. 5, 2020.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] M. Saleh, N. Jhanjhi, and A. Abdullah, "Proposing a privacy protection model in case of civilian drone." pp. 596-602.

[41] 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.

[42] J. Saleem, M. Hammoudeh, U. Raza, B. Adebisi, and R. Ande, "IoT standardisation: Challenges, perspectives and solution." pp. 1-9.

[43] 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.

[44] 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.

[45] F. Samie, L. Bauer, and J. Henkel, "IoT technologies for embedded computing: A survey." pp. 1-10.

[46] 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.

[47] J. Bryzek, and A. Rastegar, "Advances in state-of-the-art in smart sensor signal conditioning," *Analog Circuit Design*, pp. 123-149: Springer, 1997.

[48] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats to internet-of-things (iot) devices and applications," *arXiv preprint arXiv:1802.02041*, 2018.

[49] K. K. Patel, and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," *International journal of engineering science and computing,* vol. 6, no. 5, 2016.

[50] 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.

[51] A. Haroon, M. A. Shah, Y. Asim, W. Naeem, M. Kamran, and Q. Javaid, "Constraints in the IoT: the world in 2020 and beyond," *Constraints,* vol. 7, no. 11, pp. 252-271, 2016.

[52] 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.

[53] S. Zeadally, and M. Tsikerdekis, "Securing Internet of Things (IoT) with machine learning," *International Journal of Communication Systems,* vol. 33, no. 1, 2020.

[54] A. Musaddiq, Y. B. Zikria, O. Hahm, H. Yu, A. K. Bashir, and S. W. Kim, "A survey on resource management in IoT operating systems," *IEEE Access,* vol. 6, pp. 8459-8482, 2018.

[55] M. Jiménez, R. Palomera, and I. Couvertier, *Introduction to embedded systems*: Springer, 2013.

[56] 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.

[57] C. Corsi, “History highlights and future trends of infrared sensors,” *Journal of modern optics*, vol. 57, no. 18, pp. 1663-1686, 2010.

[58] 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.

[59] M. James, and D. S. Kumar, “An implementation of modified lightweight advanced encryption standard in FPGA,” *Procedia Technology*, vol. 25, pp. 582-589, 2016.

[60] M. Humayun, N. Jhanjhi, A. Alsayat, and V. Ponnusamy, “Internet of things and ransomware: Evolution, mitigation and prevention,” *Egyptian Informatics Journal*, 2020.

[61] 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.

[62] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey." pp. 0475-0481.

[63] A. Hameed, and A. Alomary, "Security Issues in IoT: A Survey." pp. 1-5.

[64] 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.

[65] 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.

[66] S. S. Dhanda, B. Singh, and P. Jindal, “Lightweight Cryptography: A Solution to Secure IoT,” *Wireless Personal Communications*, 2020.

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] B. Padmavathi, and S. R. Kumari, “A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution,” *IJSR, India*, 2013.

[73] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of Things security: A survey,” *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017.

[74] S. Görmüş, H. Aydın, and G. Ulutaş, “Security for the internet of things: a survey of existing mechanisms, protocols and open research issues,” *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 33, no. 4, pp. 1247-1272, 2018.

[75] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Computer networks*, vol. 76, pp. 146-164, 2015.

[76] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in IoT." pp. 887-890.

[77] 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.

[78] 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.

[79] 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.

[80] S. Surendran, A. Nassef, and B. D. Beheshti, "A survey of cryptographic algorithms for IoT devices." pp. 1-8.

[81] 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.

[82] S. Qamar, N. Khan, N. Ahmad, M. R. Hussain, A. Naim, N. N. Quadri, M. Israil, M. S. Arafath, and A. A. El Rahman, "Fault Analysis for Lightweight Block Cipher and Security Analysis in Wireless Sensor Network for Internet of Things," *Innovations in Electronics and Communication Engineering*, pp. 3-11: Springer, 2020.

[83] S. Al Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home." pp. 382-388.

[84] A. A. Diro, N. Chilamkurti, and Y. Nam, “Analysis of lightweight encryption scheme for fog-to-things communication,” *IEEE Access*, vol. 6, pp. 26820-26830, 2018.

[85] S. Mocanu, A. Duluta, D. Merezeanu, and R. Pietraru, “Improved Security Based on Combined Encryption and Steganography Techniques,” *Studies in Informatics and*

Control, vol. 26, no. 1, pp. 116, 2017.

[86] 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.

[87] 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.

[88] A. Ragab, G. Selim, A. Wahdan, and A. Madani, "Robust Hybrid Lightweight Cryptosystem for Protecting IoT Smart Devices." pp. 5-19.

[89] P. Rasmi, and V. Paul, "A Hybrid Crypto System based on a new CircleSymmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications." pp. 14-18.

[90] V. Janakiraman, R. Ganesan, and M. Gobi, "Hybrid Cryptographic Algorithm for Robust Network Security." p. 33.

[91] P. Kuppuswamy, and S. Q. Al-Khalidi, "Securing E-Commerce Business Using Hybrid Combination Based on New Symmetric Key and RSA Algorithm," *MIS REVIEW: An International Journal*, vol. 20, no. 1, pp. 59-71, 2014.

[92] P. Kuppuswamy, and S. Q. Al-Khalidi, "Implementation of security through simple symmetric key algorithm based on modulo 37," *International Journal of Computers & Technology*, vol. 3, no. 2c, pp. 335-338, 2012.

[93] M. Xin, "A mixed encryption algorithm used in internet of things security transmission system." pp. 62-65.

[94] A. Safi, "Improving the security of Internet of things using encryption algorithms," *World Acad Sci Eng Technol Int J Comput Electr Autom Control Inf Eng*, vol. 11, no. 5, pp. 546-549, 2017.

[95] M. Harini, K. P. Gowri, C. Pavithra, and M. P. Selvarani, "A novel security mechanism using hybrid cryptography algorithms." pp. 1-4.

[96] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *Ieee Access*, vol. 6, pp. 20596-20608, 2018.

[97] S. Njuki, J. Zhang, E. C. Too, and R. Richard, "An evaluation on securing cloud systems based on cryptographic key algorithms." pp. 14-20.

[98] V. Shoup, *Advances in Cryptology-CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*: Springer Science & Business Media, 2005.

[99] D. S. AbdElminaam, "Improving the security of cloud computing by building new hybrid cryptography algorithms," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 40-48, 2018.

[100] O. Khomlyak, "An investigation of lightweight cryptography and using the key derivation function for a hybrid scheme for security in IoT," 2017.

[101] A. Darwish, M. M. El-Gendy, and A. E. Hassanien, "A new hybrid cryptosystem for Internet of Things applications," *Multimedia Forensics and Security*, pp. 365-380: Springer, 2017.

[102] D. Mahto, D. A. Khan, and D. K. Yadav, "Security analysis of elliptic curve cryptography and RSA." pp. 419-422.

[103] Y. Chandu, K. R. Kumar, N. V. Prabhukhanolkar, A. Anish, and S. Rawal, "Design and implementation of hybrid encryption for security of IOT data." pp. 1228-1231.

[104] R. Rizk, and Y. Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks," *Journal of Electrical Systems and Information Technology*, vol. 2, no. 3, pp. 296-313, 2015.

[105] M. J. Dubai, T. Mahesh, and P. A. Ghosh, "Design of new security algorithm: Using hybrid Cryptography architecture." pp. 99-101.

[106] P. A. Jatoi, A. A. Memon, B. S. Chowdhry, M. G. Ullah, and S. Latif, "An Efficient Hybrid Cryptographic Algorithm, Consuming Less Time for Exchanging Information in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 85, no. 2, pp. 449-462, 2015.

[107] D. Bhole, A. Mote, and R. Patil, "A new security protocol using hybrid cryptography algorithms," *International Journal of Computer Sciences and Engineering*, vol. 4, no. 2, pp. 18-22, 2016.

[108] M. S. Asang, D. Manongga, and I. Sembiring, "Data Security on Internet of Things Device Using Hybrid Encryption Models," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 16, no. 8, 2018.

[109] Z.-Y. Hong, Z.-P. Qiu, S.-L. Zeng, S.-D. Wang, and M. Sandrine, "Research on fusion encryption algorithm for Internet of Things monitoring equipment." pp. 425-429.

[110] P. M. Chanal, and M. S. Kakkasageri, "Hybrid Algorithm for Data Confidentiality in Internet of Things." pp. 1-5.

[111] M. R. Warner, C. Gardner, R. Wyden, and S. Daines, "Internet of Things Cybersecurity Improvement Act of 2017."." p. 1691.

[112] I. S. Foundation, "IoT Security Foundation," *IoT Security Foundation 2015 - 2020 website: https://www.iotsecurityfoundation.org/about-us/*.

[113] I. S. Foundation, "IOTSF Best Practice Guide," *IoT Security Foundation 2015 - 2020*.

[114] "Infocom Media Development Authority IMDA " *2020, Infocomm Media Development Authority. Last updated 22 May 2020m website: https://www.imda.gov.sg/Who-We-Are*.

[115] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294-1312, 2015.

[116] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an

analysis of security issues, challenges, and open problems in the internet of things." pp. 21-28.

[117] M. El-Haii, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of cryptographic algorithms on iot hardware platforms." pp. 1-5.

[118] N. Kumar, and N. Reddy, “ESTIMATION OF CRYPTOGRAPHIC APPROACH ON IoT DEVICES,” 2019.

[119] S. Maitra, D. Richards, A. Abdelgawad, and K. Yelamarthi, "Performance Evaluation of IoT Encryption Algorithms: Memory, Timing, and Energy." pp. 1-6.