Efficient Security Algorithm for Power Constrained IoT Devices

Joseph N. Mamvong, Gokop L. Goteng, Bo Zhou, Yue Gao, Senior member, IEEE

***Abstract*—Internet of Things (IoT) devices characterized by low power and low processing capabilities do not exactly fit into the provision of existing security techniques, due to their constrained nature. Classical security algorithms which are built on complex cryptographic functions often require a level of processing that low power IoT devices are incapable to effectively achieve due to limited power and processing resources. Consequently, the option for constrained IoT devices lies in either developing new security schemes or modifying existing ones to be more suitable for constrained IoT devices. In this work, an Efficient security Algorithm for Constrained IoT devices; based on the Advanced Encryption Standard is proposed. We present a cryptanalytic overview of the consequence of complexity reduction together with a supporting mathematical justification, and provisioned a secure element (ATECC608A) as a trade-off. The ATECC608A doubles for authentication and guarding against implementation attacks on the associated IoT device (ARM Cortex M4 microprocessor) in line with our analysis. The software implementation of the efficient algorithm for constrained IoT devices shows up to 35% reduction in the time it takes to complete the encryption of a single block (16bytes) of plain text, in comparison to the currently used standard AES-128 algorithm, and in comparison to current results in literature at 26.6%**

***Index terms*—** Encryption, Complexity, Security Algorithms, Internet of Things (IoT) Security, Constrained IoT Devices.

I. Introduction

In the recent past, there has been a gradual shift of the IoT technology discuss from being highly theoretical to a realistic actualization. IoT devices have been estimated in several scholarly articles to be in the range of twenty to fifty billion devices by the year 2025 [1], [2]. The projection of the Internet of Things (IoT) technology is to give every real object a virtual reality, bringing about an unprecedented connectivity of things more than ever before. In the years ahead, the Internet of Things will have major impact on business models [3]–[7], agriculture [8], [9], transportation [10]–[12], automated industrial processes [13]–[15], homes [16], [17], infrastructure, security, trade standards, and much more. However, as interesting and promising as the projection of the complete actualization of the IoT technology sounds, this advancement is going to be closely accompanied by myriads of challenges -including security. Such extreme interconnection will bring unprecedented convenience and economy, but it will also require novel approaches to ensure its safe and ethical use [18]. In [19], while acknowledging the emergence of the IoT in redefining convenience in the lives and education of children through emerging applications on mobile phones, it was identified that these apps also make illegal and inappropriate contents such as pornography, violence and drugs -to mention a few, become more accessible to children and thus, negatively impacting the growth of minors. They proposed a novel automatic content detection framework for detecting inappropriate content in effort to solve this problem. In [20], an attack tolerance scheme to cooperate with existing defence mechanism is proffered for enabling self-recovery ability for the vehicular edge networks sub-domain, of the Industrial Internet of Things (IIoT). In [21], an analysis of the security challenges for Internet of Things (IoT) according to the various layers of the IoT architecture was presented. Some of these challenges include node reputation, information interception, access control, terminal security, privacy, heterogeneous technology and network security to mention but a few.

A. Motivation

Securing the Internet of Things (IoT) is a necessary milestone towards expediting the deployment of its applications and services [22]. According to [23], As smart home systems get more and more popular recently, the security protection of smart home systems has become an important problem. Architecting IoT focused security solutions must however, take into considerations the unique circumstance of power constrained IoT devices as according to [24], reaping the benefits of the Internet of Things (IoT) is contingent upon developing IoT-specific security and privacy solutions. According to [25], Since IoT communication protocols and technologies differ from traditional IT realms, their security solutions ought to take this difference into account. Security of conventional IT infrastructure is achieved using classical cryptographic protocols and algorithms whereas, applying classical cryptographic methods for IoT security is not efficient as those methods were not ideally designed for these kind of systems [21]. Consequently, the option for IoT in terms of security lies either in the development of new schemes or the modification of existing ones.

B. Contributions

Motivated by the aforementioned works which summarize the unsuitability of the usage of conventional cryptographic algorithms for security in the IoT landscape, We propose an

J.N Mamvong, G.L. Goteng, are with the Department of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, UK (email:{j.n.Mamvong, g.l.goteng}@qmul.ac.uk)

Bo Zhou is with the School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool L3 3AF, UK. (email: b.zhou@ljmu.ac.uk).

Y. Gao is with the Department of Electrical and Electronic Engineering, University of Surrey, Surrey GU2 7XH, UK (email:yue.gao@ieee.org).

efficient security algorithm for power constrained IoT devices which aimed to reduce complexity of the currently used security algorithm: The Advanced Encryption Standard, in the IoT landscape. The major contributions of this paper are thus summarized as follows:

- We present a cryptanalytic overview and analysis of the consequences of reducing the complexity of the AES, which is the currently used encryption algorithm in the IoT landscape.
- We present a mathematical justification of reducing the complexity of the standard AES-128 algorithm, using the core algebraic properties of the standard algorithm. This is followed by provisioning a secure element: the ATECC608A to aid authentication and guard against implementation attacks in line with our analysis of the consequence of round reduction of the AES-128.
- We implemented a safely reduced round versions (four rounds and two rounds) of the AES-128 algorithm, based on the the structure of the AES in order to reduce complexity (measured by the time it takes to complete the encryption of 16bytes of plain text).
- We compared the reduced round algorithm and the standard AES-algorithm. Our results show that up to 35% of the time it takes to complete the encryption of a single byte of plain-text is saved.

With respect to the categories of security challenges in the IoT and cyber-physical systems landscape as outlined in [21], our work aims to address the bit of privacy and access control, through message encryption and secure authentication respectively, and also to guard against implementation attacks on the associated IoT device. The remaining of this paper is organized as follows: Section II contains the background information and mechanism that was used in complexity reduction aimed at constrained IoT devices. In section III, we present a cryptanalytic analysis of the consequence of complexity reduction together with a detailed mathematical justification for doing such, and then the efficient algorithm for constrained IoT devices. In section IV, we present an implementation evaluation wherein we discussed the experimental setup, computation complexity, results and summary of our implementation. Section V covers related work on the notion of complexity in terms of key sources and cipher in line with the IoT narrative. A discussion section highlighting some IoT applications, the plausibility of the developed solution and future works is presented in section VI and an appendix section showing the detailed proves of theorems used in the work is presented in VII

II. Background of Complexity Reduction aimed at Constrained IoT Devices

According to [26], IoT devices are known for their limited memory space and computational capabilities, and conventional solutions such as encryption methods are inadequate to solve many privacy concerns. According to [27], the running time of the algorithm imposes a constraint on its applicability in several domain. In favor of the narrative of constrained IoT devices, they proposed that an extension of DES into Galois fields of GF (16) with a 256-bits key might be a good alternative to the advanced encryption standard if the technology is sufficiently developed to run fast enough. In [28], A low power algorithm aimed at improving on the power consumption by classical algorithms for IoT was proposed. Observing that the power cost of transmission and reception of data typically outweighs the cost of the cryptographic algorithms themselves, they proposed a method called Authenticated Encryption with Replay protection (AERO), which shows to significantly reduce overheads even when used in higher-layer protocols above the link layer. This work suggests that the cost of transmission and reception of messages could be reduced by up to 30%, which translates into improving the limited resource of power in constrained IoT devices, although [29] observed that significant power can be saved by this method but the security of the method needs to be confirmed. The authors in [30] proposed a lightweight enhanced Distributed Low-rate Attack Mitigating (eDLAM) mechanism in tandem with the constrained resource narrative of IoT devices, which aims to mitigate DDoS attacks and obtain maximum utility in IoT deployments

In [29], an AES-128 based Secure Low Power Communication (SeLPC) algorithm for LoRaWAN IoT environment, which details in two phases namely: the key generation phase and data encryption phase was proposed. The algorithm aimed at significantly improving on AES to meet low powered devices security constrains, detailing that in the standard AES encryption process, the SubBytes stage typically looks up S-Box to encrypt and decrypt data stream but as the contents of the S-Box in AES are fixed, this greatly reduces its security level since the only nonlinear component of this block ciphering technique is the manipulation on S-Box. To enhance AES's cryptographic strength, an encryption key that generates the corresponding dynamic box (D-Box) to substitute for the primary substitution box(S-Box) was derived. Following this, the simplified standard AES-128 encryption process of 10 cycles down to 5 cycles with the aim to reduce computational complexity and save power consumed by end devices in a LoRaWAN IoT environment, although the reason or rationale for simplifying to specifically 5 rounds was not stated. However, the SelPC algorithms utilizes an Enhanced Dynamic Accumulated Shifting Substitution (EDASS) algorithm which leverages high input sensitivity and randomness to harden the security of the D-Box against attacks. According to [29], if a hacker would like to decrypt an application- layer message, the attacker needs to know the 128-bit AppSKey and D-Box. As n-bit security is defined by 2^n; where n = number of bits, the possibility of the AppSKey and D-Box combination multiplies to $2^{128} \times 256!$ and thus, enhancing the security of the standard AES-128 algorithm with the default n-bit security of 2^{128} bits. Results of their method shows that the SeLPC algorithm can save 26.2% of power consumption in comparison to the traditional security algorithm based on the standard AES algorithm in a LoRaWAN environment and thus, improving the security of constrained IoT devices.

III. The Proposed Security Algorithm for Power Constrained IoT Devices

The security algorithm for power constrained IoT devices aims to reduce the complexity of the AES which is currently the widely used security algorithm for LPWA networks based on our investigation in section II A above. The AES-128 variant of the algorithm is considered for this exercise. The natural question that arises however is of what the consequence of this reduction might be. Our approach takes directly in providing a cryptanalytic overview of the consequence of complexity reduction and its corresponding mathematical justification, following which we provision a secure element, the ATECC608A for aiding authentication and hardening the security of the associated IoT device in the perspective of the consequence from our analysis.

A. Cryptanalytic Overview of the Consequence of AES Round Reduction

Here, we present an overview of the consequence of reducing the rounds of the AES algorithm from a cryptanalytic standpoint. We make the point that the major consequence of this exercise is with respect to implementation attacks; and this is precisely the perspective in which we have provisioned a compensation with the secure element as a trade-off in the efficient security algorithm for power constrained IoT devices.

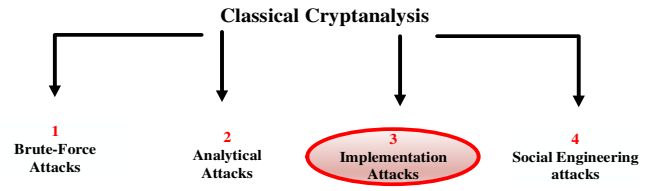

Fig. 1. Cryptanalytic overview of the consequence of AES round reduction.

While a formal analysis of security protocols is on its own, an whole area of fertile research [31], according to [32], the security of an encryption scheme is usually measured through the application of different types of cryptanalysis methods. The security of the AES algorithm with respect to key length is based on its resistance against breakability by brute-force/exhaustive key search. This is usually expressed in bits, where n-bits security means that the attacker would have to perform 2^n operations to break it. In the standard AES-128 algorithm, this is equals 2^{128} operations, for which there are no computing resources currently available. In this context of exhaustive key-search attack, the reduction of the number of rounds while retaining the key length of 128bits means that the security level is still preserved. The security structure of the algorithm against the analytical family of attacks is based on the Galois field properties which operations render the S-Boxes. We rationalized the preservation of this structure of the algorithm using the core algebraic properties of the algorithm. The details of this rationalization are in the section III-B. Implementation attacks however is a family of attacks that try to achieve what cannot be achieved through Brute-force attacks and analytical attacks, by attempting to manipulate the encryption algorithm at the point of hardware implementation. This is mainly characterized by measuring the electrical power consumption of a processor which operates on the key [33], [34], and the power trace can then be used to recover the key by applying signal processing techniques. In the efficient security algorithm for power constrained IoT devices, the trade-off for the round reduction is the introduction of a secure element: which doubles for authentication of the associated IoT device and to guard against implementation attacks, thereby sufficiently ensuring security covering: brute-force, analytical and implementation attacks and leaving social engineering attacks which can be managed by policies as shown in Fig. 2.

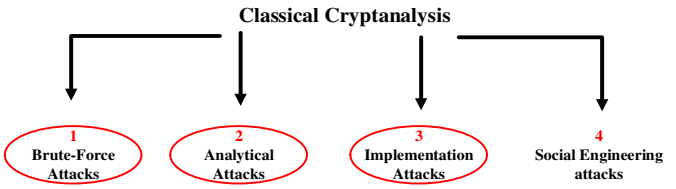

Fig. 2. Cryptanalytic overview of the efficient security algorithm for power constrained IoT devices.

B. Justifying Round Reduction and Security Trade-off

The following presents the mathematical details of the justification for reducing the rounds of the AES algorithm. We rationalized that the security structures with respect to brute-force and analytical attacks is preserved based on the underlying algebraic properties of the cipher.

Firstly, round reduction does not impact on the key length of the cipher and since n-bit security is defined by 2^n; where $n =$ number of bits then

$$\Rightarrow 2^{128} = 2^{128}$$

Thus, we have that the cipher's properties which guarantee defense against brute-force attacks is preserved. Next, we want show that the Galois Fields properties of the cipher that guards against analytical attacks are preserved. It suffices to show that the algebraic structure which renders elements of the S-box tables is undefiled by round reduction.

TABLE I
Table of Important Symbols

Notation	Meaning
Nbr	Number of rounds executed by the round function
F	Field (as an algebraic structure)
n	An arbitrary natural number
GF	Galois Field
Deg	degree of a polynomial elements in the Galois Field
P	An arbitrary prime number
Mod	Modulo: the operation or function that returns the remainder of one number divided by another
$\mathbb{Z}_p$	Ring of integers modulo p
$n(x)$, $m(x)$, $\alpha(x)$,$\beta(x)$	Arbitrary polynomial elements of the Galois Field $GF(P^n)$
$\mathcal{O}$	The "big oh" notation

Let n and m be some arbitrary bytes of an AES message block. As n and m are bytes of an AES message, it implies that n and m are elements of the Galois Field $F = GF(2^8) = GF(P^n)$. Since the elements of a Galois Field

F are non-numerical: precisely polynomials with the element representation:

$$A(x) = x^{m-1} + ... + a_1x + a_0$$

for any arbitrary $A(x) \in F = GF(p^n)$, $n = n(x) = a_{n-1}x^{n-1} + ... + a_1x + a_0$. For the additive operator, given two arbitrary polynomials n and m in F, the sum $n(x)$ + $m(x)$ is defined by

$$z(x) = n(x) + m(x) = \sum_{i=1}^{m-1} z_i x^i \text{ where } z_i = n_i + m_i \ mod 2$$

. Elements inversion with this operation naturally gives rise to subtraction defined by =

$$z(x) = n(x) - m(x) = \sum_{i=1}^{m-1} z_i x^i \text{ where } z_i = n_i - m_i \ mod 2$$

To show the field properties of element combination and inversion with respect to the multiplicative operator, we consider the following theorems:

Theorem 1: Let F be a field and let $n(x)$, $m(x)$ be polynomial elements in F, where $m(x) = 0$, then there exist unique polynomials (x) and $r(x)$ in F such that;

$$n(x) = m(x)(x) + r(x) \quad (1)$$

where either $r = 0$ or $deg(r(x)) < deg(m(x))$

Theorem 2: Let F be a field, and $n(x)$ and $m(x)$ be non-zero polynomials in F, then $n(x)$ and $m(x)$ have a unique monic greatest common divisor, say $d(x)$ in F such that:

$$d(x) = \alpha(x)n(x) + \beta(x)m(x) \quad (2)$$

Theorem 3: Let $F = GF(2^8) = GF(P^n)$ be a field, then there exists an irreducible polynomial of degree n over Z_p

As F is a field, we have that for the arbitrary elements $n(x)$,$m(x)$ and $z(x) \in F = GF(P^n)$, $n(x) + m(x) = (a_{n-1}x^{n-1} + ... + a_1x + a_0) + (a_{m-1}x^{m-1} + ... + a_1x + a_0)$, $z(x) = n(x) + m(x) = \sum_{i=1}^{m-1} z_i x^i$, where $_i = n_i + m_i mod 2 \in F = GF(2^8)$ =$GF(P^n)$.
Also, by the application of Theorem 1 and Theorem 3 above we have that $n(x) \times m(x) = [(a_{n-1}x^{n-1} + ... + a_1x + a_0) \times (a_{m-1}x^{m-1} + ... + a_1x + a_0)] \ mod x^8 + x^4 + x^3 + x + 1 = z(x) \in F = GF(2^8) = GF(P^n)$ and so, closure; with respect to the additive and multiplicative operators hold in F. Associativity also holds in F by a combination of the same theorems with the arbitrary elements on: $(a_{n-1}x^{n-1} + ... + a_1x + a_0) + [(a_{m-1}x^{m-1} + ... + a_1x + a_0) + (a_{z-1}x^{z-1} + ... + a_1x + a_0)] = [(a_{n-1}x^{n-1} + ... + a_1x + a_0) + (a_{m-1}x^{m-1} + ... + a_1x + a_0)] + (a_{z-1}x^{z-1} + ... + a_1x + a_0)$ and $(a_{n-1}x^{n-1} + ... + a_1x + a_0) \times [(a_{m-1}x^{m-1} + ... + a_1x + a_0) \times (a_{z-1}x^{z-1} + ... + a_1x + a_0)] = [(a_{n-1}x^{n-1} + ... + a_1x + a_0) \times (a_{m-1}x^{m-1} + ... + a_1x + a_0)] \times (a_{z-1}x^{z-1} + ... + a_1x + a_0)$ for the additive and multiplicative operators respectively. Similarly, $n(x) + (-(n(x)) = (a_{n-1}x^{n-1} + ... + a_1x + a_0) + (-(a_{n-1}x^{n-1} + ... + a_1x + a_0)) = 0$,
$n(x) \times (n(x)^{-1}) = [(a_{n-1}x^{n-1} + ... + a_1x + a_0) \times (n(x)^{-1})] \ mod x^8 + x^4 + x^3 + x + 1 = 1$ and the identity elements and inverses exist for the additive and multiplicative operators in F accordingly. Distributivity also holds in F accordingly and so, satisfying the properties of an additive group and a multiplicative group in F. By Theorem 2, the existence of a greatest common divisor between the arbitrary bytes of the AES message blocks: $n(x)$ and $m(x)$ is guaranteed. Division, which implies element inversion with respect to the multiplicative operator is also guaranteed in $GF(2^8)$ by Theorem 1 and by Theorem 3, the existence of an irreducible polynomial over the message field $GF(2^8)$ is guaranteed. Moreover, the irreducible polynomial: $x^8 + x^4 + x^3 + x + 1$ is a part of the AES specification and so, the operations of addition and multiplication, together with their corresponding inversions are guaranteed given the arbitrary AES message bytes n,m and $z \in F = GF(P^n)$. Therefore, the underlying structures of the cipher that renders the entries of the AES S-boxes hold and thus, the core security attributes of algorithm in the context of analytical attacks is preserved with respect to round reduction.

C. The efficient algorithm for power constrained IoT devices:

The efficient security algorithm executes a two-step process for an associated power constrained IoT device as follows:

1) Secure authentication using the ATECC608A
2) Message encryption using the reduced round cipher

Leveraging the tamper-proof secure element for secure authentication, the reduced round algorithm executes the round function in four iterations using a total of 80bytes scheduled key as against the 176bytes of the standard AES, for every block of the plaintext, following the process of key-whitening, initialization and the execution of the round function. The pseudo code of the process flow of the proposed algorithm is presented in Table II.

TABLE II
THE ALGORITHM FLOW

	The Efficient Security Algorithm for Constrained IoT Devices
Step1	
*	Initializing the IoT device and the ATECC608 secure element
*	Invoking authentication using ATECC608 and generating tamper-proof security keys
Step2	
1.	Input: message, key
2.	Nbr selection: 2 or 4 and initialization of the Nbr counter
3.	Expand key to length: (block size) *Nbr + block size
4.	STATE = message XORed with Key (Key whitening)
5.	Invoke the round function: While counter is less than the selected Nbr: i. STATE = SubByte(STATE) ii. STATE = ShiftRows(STATE) iii. If counter $<$ selected nbr: 1. STATE = MixColumn(STATE) iv. Invoke addRoundKey(STATE,NextRoundkey)
6.	Output STATE as resulting Ciphertext

The secure element (SE): ATECC608A-MAHTN-T is a microprocessor which can store sensitive data and run secure applications. Developed by the ARM in collaboration with LoRaWAN and the Things industry, it holds the potential to automatically offload all cryptographic operations, such that keys will never be visible nor accessible, even when the associated IoT device might be compromised [35]. The ARM Cortex M4 is a microprocessor designed for low energy efficient devices. With both processors Run by the Mbed operating system (OS),

they support IoT application development via the Mbed Integrated Development Platform and supports the IEEE 802.15.4 specification and lower power communications protocols including: Bluetooth Low Energy (BLE), Zigbee, Low Power Wide Area Network (LoRaWAN), Routing Protocol for Low power devices (RPL), Constrained application protocol (CoAP) and the Message Queueing Telemetry Transport (MQTT) messaging protocol for constrained IoT devices and support the LoRaWAN 1.x and 1.1. The ATECC608A functionality to wades against implementation attacks which aim to exploit the recovery of encryption keys through manipulating the efficient security algorithm for power constrained IoT device at the point of hardware implementation. This serves as compensation for the reduced round and consolidating the preserved security properties of the algorithm in the perspective of brute-force and analytical attacks as discussed in section III-A. Moreover, the ATECC608A-MAHTN-T microchip offers a secure authentication of the associated IoT device onto the network infrastructure; a requirement that precedes the functionality of secure message encryption and decryption hence, enabling the two-step process of the efficient security algorithm for power constrained IoT with functionality summarized against the IEEE 802.15.4 architecture as shown in Fig. 3.

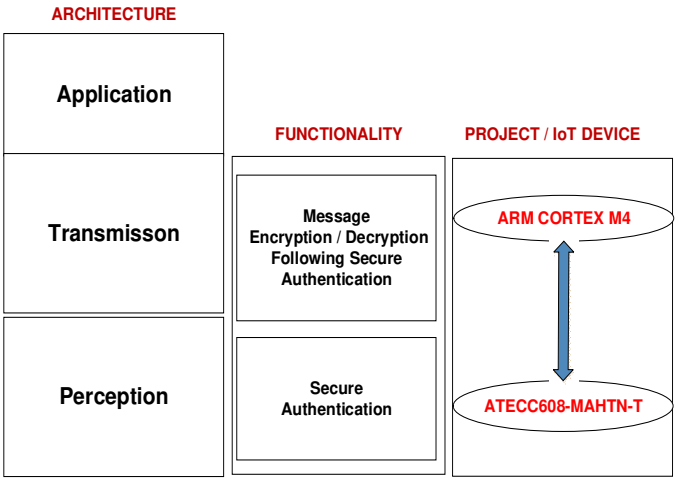

Fig. 3. Algorithm Functionality in the IEEE 802.15.4 architecture

IV. IMPLEMENTATION EVALUATION

In this section, we present a summary of our experimentation setup for implementation, computational complexity of the proposed algorithm and finally, the results of our experimentation and a comparative analysis of the proposed efficient algorithm for low power IoT devices with respect to the standard AES.

A. Experimental setup

Our experimentation tools include the Zerynth studio which runs python optimized with C, and Jupyter notebook for the software implementation, analysis and plots respectively. For each instance of encryption, the encryption is repeated for one thousand iterations and the average execution time of the one thousand iterations is logged as the execution time for that instance. The notion of average is here employed to obtain statistically relevant values and easily identify and handle outliers for the various encryption instances and this was done for the reduced round algorithm and all the key lengths of the standard AES algorithm as detailed in the Tables III and IV.

B. Results and Analysis of Computation Complexity of the Efficient Algorithm for Constrained IoT Devices

The measure of an algorithm's complexity is popularly using the big $\mathcal{O}$ notation, which essentially is a mathematical notation that describes the limiting behavior of a function when the argument tends to a value or infinity [36]. According to [37], this is frequently used in the analysis of algorithms to describe an algorithm's usage of computational resources: the worst case or average case running time or memory usage of an algorithm is often expressed as a function of the length of its input. The input sized of the proposed algorithm for constrained IoT devices is a fixed 16bytes block size of input, and thus of $\mathcal{O}(1)$ computational complexity in terms of the big $\mathcal{O}$ notation with respect to the input size and $\mathcal{O}(m)$, with a growing message size m, as there would be m blocks to encrypt. As reviewed in section V, the running time of an encryption algorithm ultimately impacts on the power and processing resources of the constrained IoT devices . In line with this reality, we present an analysis of the computation complexity of the proposed algorithm which we measured by the execution time-difference between the standard AES and variants of the proposed algorithm for constrained IoT devices. While the AES-128 is 10.5% and 16.1% cheaper than the AES-192 and AES-256 respectively in encrypting a single block (sixteen bytes) of plain text on a one thousand average; the proposed algorithm is 27.1% and 35% cheaper than the standard AES-128 for the rr2 and rr4 implementations respectively. This is further detailed in the results and analysis below:

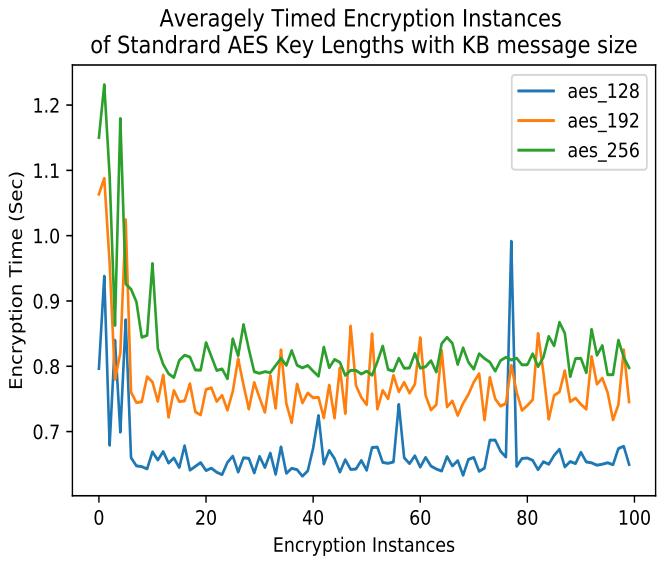

Fig. 4. 1000 average-timed encryption instances of standard AES variants

Our results show that the proposed efficient low power algorithm for constrained IoT devices in comparison is 27.1% cheaper than the standard AES128 (in the case of reducing to four rounds -rr4) and 35% cheaper than the AES-128 (in the case of reducing to two rounds -rr2) in favor of the narrative of the constrained IoT devices. This is shown in Fig. 5

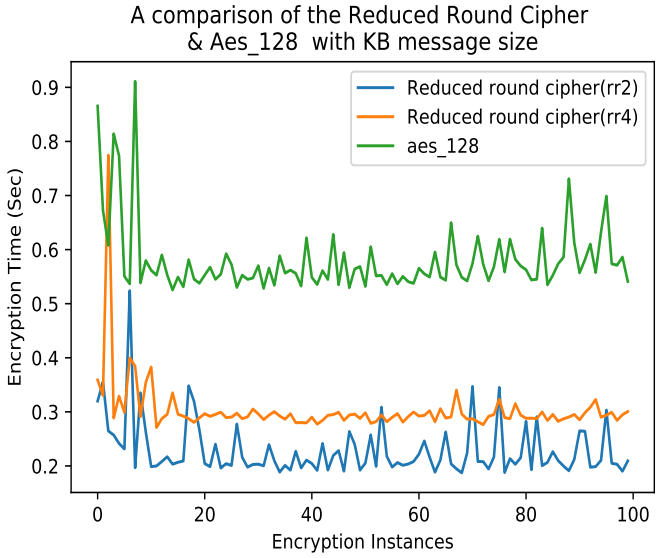

Fig. 5. A comparison of the Reduced Round Cipher (rr2, rr4) and standard AES-128

The degree of complexity reduction measured by the complexity difference between the AES-128 and proposed algorithm for low power constrained IoT devices is obtained to be higher than the complexity difference between the AES-256 and the AES-128 by 11.57%:

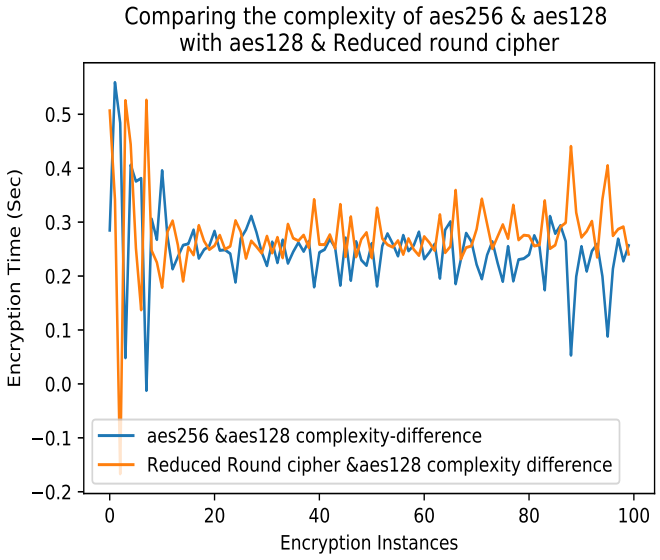

Fig. 6. A comparison of cost difference between AES-256 AES-128; AES-128 the reduced round algorithm.

Tables III and IV show the head and tail respectively, of the data generated from our experimentation of the measure of complexities of the standard AES key lengths and those of the reduced round algorithm, and from which figures 4, 5 and 6 were plotted.

TABLE III
HEAD (FIRST 5 ROWS) OF GENERATED DATA OF ENCRYPTION TIMES OF THE KEY LENGTHS CONSIDERED

Instances	AES-128 (Sec)	AES-192 (Sec)	AES-256 (Sec)	rr4(Sec)	rr2(Sec)
1	0.7964807	1.063512	1.150296	0.35891	0.31994
2	0.9380837	1.087956	1.231360	0.33022	0.35540
3	0.6789956	0.958238	1.091734	0.77476	0.26462
4	0.8400028	0.779829	0.862398	0.28851	0.25722
5	0.6990071	0.820398	1.179501	0.32904	0.24158

TABLE IV
TAIL (LAST 5 ROWS) OF GENERATED DATA OF ENCRYPTION TIMES OF THE KEY LENGTHS CONSIDERED

Instances	AES-128 (Sec)	AES-192 (Sec)	AES-256 (Sec)	rr4(Sec)	rr2(Sec)
96	0.652252	0.759551	0.787011	0.29394	0.30342
97	0.649166	0.717744	0.787098	0.29911	0.20491
98	0.673988	0.741114	0.840172	0.28418	0.20308
99	0.677502	0.825463	0.813646	0.29465	0.19018
100	0.649555	0.745380	0.797678	0.30057	0.20931

We carried out a covariances analysis of the various key lengths from the data generated from our experimentation. This was done through the computation of the covariance matrixes of pairs of key lengths to buttress the notion of growing complexities associated with the key lengths as discussed in section V. This is demonstrated by the result of positive covariance values as shown in table V and this is further consolidated by the reduced algorithm being 27.7% and 35% cheaper than the standard AES as shown in Fig. 5. A table of the comparisons of covariances is shown below:

TABLE V
COVARIANCES COMPARISON OF THE REDUCED ROUND ALGORITHM THE STANDARD AES KEY LENGTHS

Cov(AES-128, AES-192)	Cov(AES-192, AES256)	Cov(AES-128 AES256)	Cov(rr4-AES128, AES128)	Cov(rr2-AES128, rr4-AES128)
0.00202746	0.0033184	0.00202	0.00065489	0.00055592

V. Related Work

A. Constrained IoT Devices and Security Algorithms

Effectively implementing conventional security mechanisms in the IoT domain is challenging as most of state-of-the-art mechanisms are too heavy to suit for the tiny and resource constrained IoT devices [38]. Leading classical security algorithms which have been widely used for encrypting messages include; but not limited to the Data Encryption Standard (DES) [33], [39], [40], the Triple Data Encryption Standard (3DES) [27], [41], and the Advanced Encryption

Standard (AES) [33], [39], [42]–[44]. On the security standing of these classical algorithms and their viability in the rapidly developing IoT landscape, while DES has been widely accepted as insecure and although the security of the 3DES is being adjudged to be reasonably secure [40] in certain applications, the properties of 3DES when juxtaposed with the characteristics of constrained IoT devices shows no viability as according to [41], the triple encryption/decryption in comparison to standard DES triples the cost of required resources and latency as a corresponding consequence, resulting in the 3DES being slower than other cipher algorithms [45] [31]. These properties when juxtaposed with the constrained properties of IoT devices in addition to the inherent drawbacks of the standard DES algorithm makes the triple DES still a very expensive option for the IoT landscape. According to [27], the running time of the algorithm imposes a constraint on its applicability in several domain. They proposed that an extension of DES into Galois fields of GF (16) with a 256-bits key might be a good alternative to the AES if the technology is sufficiently developed to run fast enough. Encryption refers to the processes of transforming an original message called plaintext into a secret form called ciphertext, using a key called an encryption key, such that only authorized parties can access the message and those who are not authorized cannot. Decryption refers to the reverse process of inverting a ciphertext back to plaintext using a corresponding secret key.

In [46], a survey of the technical specifications of leading Low Power Wide Area (LPWA) technologies including the Long Range Wide Area Network (LoRaWAN) and INGENU (formally known as On-Ramp wireless) is presented. INGENU is a competing standard to the LoRaWAN in the rolling out of LPWA technologies. The survey shows that the AES is currently the adopted algorithm for authentication and encryption and thus, crowning the AES as the algorithm currently being widely used for communication security in constrained IoT devices.

However, According to [21], applying these classical cryptographic methods for IoT security is not efficient as those methods were not ideally designed for these kind of systems. They advocated for hybrid light weight models for improving security situation in IoT. Thus, the need for investigating what components of the existing algorithms make them expensive and explore how they can be improved. According to [47], It will be of particularly importance to explore new techniques of jointly defending against multiple types of wireless attacks, which may be termed as mixed wireless attacks. Traditionally, the protocol layers have been protected separately to meet their individual communications security requirements. However, these traditional layered security mechanisms are potentially inefficient, since each protocol layer introduces additional computational complexity and latency. As a result, the need of addressing security challenges in more than one layer of the IoT protocol architecture is also advocated. In [47], it was said the classic Diffie–Hellman key agreement protocol is traditionally used to achieve the key exchange between the source and destination and requires a trusted key management centre. The complexity of these security algorithms with respect to the constrained nature of the IoT devices can be broadly considered in two perspectives viz: the method through which encryption keys are obtained and the cypher itself. Fig. 1 shows a rather compressed summary of these various methods of obtaining the encryption keys by these algorithms, of which each of these methods hold its own inherent notion of complexity when juxtaposed with the constrained nature of IoT devices such as limited power resource and processing capabilities.

On a broad category, sources of encryption keys being used by these classical algorithms can be classified into three as summarized in Fig. 7 viz: Centralized key generation and management systems [21], [48], [49], Public Key Cryptography key generation methods [24], [33], [39], [44], [48] and most recently, the exploration of Channel State Information (CSI) key generation methods [47], [48], [50]–[53]. For each of the above-listed method of encryption key generation being used with these classical algorithms, there is the associated challenges with respect to complexity and the constrained nature of IoT devices. According to [21], key management which includes generating, distributing, storing and destroying the secret key is identified as a security challenge in wireless sensor networks, a category within the lager body of the Internet of things (IoT) [24], [49]. According to [49], due to resource constraints, key agreement in IoT is non-trivial. Many key agreement schemes used in general networks, such as Kerberos and RSA, may not be suitable for IoT because there is usually no trusted infrastructure in IoT. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. According to [48], this approach of encryption key generation have been long regarded as expensive in terms of computational complexity. According to [22], securing the IoT devices has become challenging due to the simplicity, resource-constrained nature and low storage capabilities of IoT devices at the perception layer. In [54], a True Random Number Generator using Random Telegraph Noise (RTN) was proposed to address speed, design area, power and cost as constrained resources in low power devices, thereby making a plausible candidate for cryptographically secure IoT applications. The notion of complexity on the part of the cipher however depends on factors such as the design and structure of the cipher. However, According to [24], complex security techniques such as classical cryptographic protocols cannot be easily implemented on IoT devices due to the memory and computational resources required in deploying such algorithms. Hence, the option for constrained IoT devices lies in either developing new security schemes or modifying existing security schemes towards reducing complexity of these classical algorithms aimed at constrained IoT devices.

B. The Advanced Encryption Standard (AES) and The Reduced Round Algorithm

The Advanced Encryption Standard (AES) is a block cipher cryptographic algorithm defined by the National Institute of

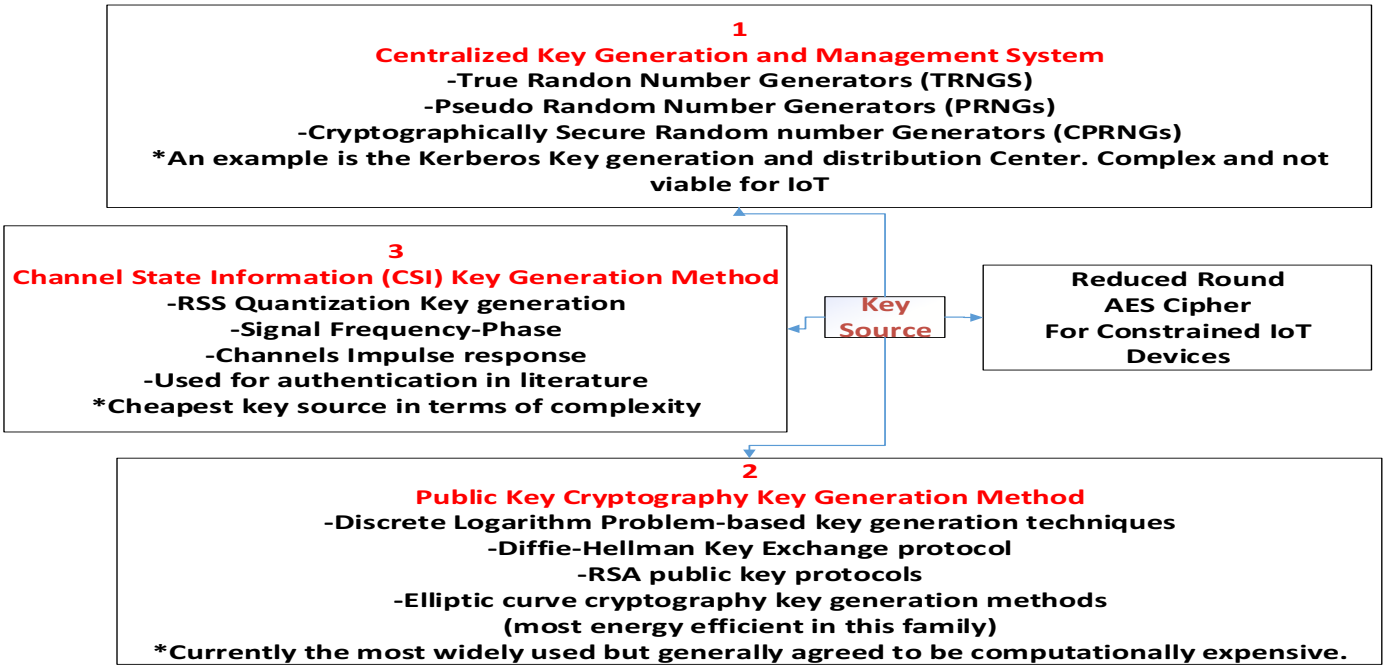

Fig. 7. Encryption Key generation sources

Standards and Technology (NIST) in 2001, following the concern of the insecurity that plagued the DES and 3DES algorithms and calls for new algorithms to be standardized [29], [33]. Based on Rijndael cipher, it encrypts messages in blocks of 128bits and supports three distinct key lengths of 128, 192 and 256bits with corresponding cipher rounds of ten, twelve and fourteen respectively. The process of AES encryption is described as follows:

1) State/Initialization (Key Whitening)

The result of the State/initial round which is also known as the key whitening stage is basically having the message bits XORed with the key bits: Message (16bytes) XORed Key(16bytes)

2) The Round Function

SubBytes: This stage involves a non-linear, invertible transformation whereby each of the bytes in the message block is replaced by another byte. These substitutions usually follow the presentation of the Rijndael S-box look up table.

The ShiftRows Stage: The ShiftRows operation is done on the result of the STATE produced after the SubBytes operation. Visualizing the result as a matrix, the ShiftRow is an element-wise rotational operation with elements of the first Row being shifted by zero to the left (or not being shifted at all), the second row being shifted by one element, the third element shifted by two elements and so on until the last Row is shifted.

The MixColumns Stage: The MixColumn operation is done on the STATE, having undergone the shiftRow operation. The operations involve multiplying each column of the data block with a modular polynomial in the Galois Field $GF(2^8)$.

Add Round Key Stage: During the key expansion, the original key is used to generate round keys that are used in the rounds. This means the key in each round is different, although all generated from the same key during key schedule. In the add round key stage, the STATE bytes from the MixColumn stage are XORed with the bytes of the sub-key for that round. Depending on the key length which determines the number of rounds, each round of the AES encryption process except for the last round; performs the process of the round function above. The last round ends with the MixColumns stage and outputs the ciphertext.

In comparison to the standard AES-128 algorithm which repeats the round function described above for 10 iterations and uses a total length of one hundred and seventy six bytes (176B) scheduled key, the proposed reduced round algorithm executes the round function in four iterations using a total of 80bytes scheduled key as against the 176bytes of the standard AES. In addition, a tamper-proof secure element (ATECC608A) which guarantees secure authentication for the associated IoT device is first p rovisioned p rior t o message encryption using the proposed reduced round algorithm.

VI. DISCUSSION AND CONCLUSION

A. Discussion

The proposed solution can be applied in IoT deployment scenarios with devices requiring low cost encryption solution due to constrained resources. Some of the challenges accompanied by the advent of cloud computing being a key enabler for the provisioning of IoT devices is the need for encrypting IoT device data before outsourcing it to the cloud, despite the inherent constraints of most IoT devices in terms of processing capabilities. According to [55], encryption-before-outsourcing is a widely recommended method to guarantee the confidentiality of user data in the IoT domain, whereas the

need of architecting these devices with client-side encryption capabilities in order to preserve the privacy of data generated and outsourced to cloud storage systems brings on another layer of burden on the devices, given the scarcity of resources. In order to protect the security of the outsourced data, an intuitive way is to encrypt the data before outsourcing it to the cloud [56] and according to [57], the integration of IoT devices and cloud servers is highly dependent on how security issues such as authentication and data privacy are handled. Thus, provisioning these IoT devices with low-cost encryption algorithms and without compromise to secure provisioning is advocated. The efficient security algorithm for constrained IoT devices would be useful in aiding such low cost client side encryption and secure provisioning of these devices to the cloud. On another front, resources sharing mechanism in the IoT domain where resource constrained IoT devices can offload computationally intensive resources to resource-rich ones in order to achieve high quality of experience is encouraged in [15]. Accordingly, more complex scenarios of the use case of the proposed power efficient algorithm can be explored to leverage these efforts, and use the algorithm for resource constrained devices while adapting to the standard algorithm for the resource rich scenarios. Hinging on the discussed challenges, the following plausible directions for future work is derived:

- Utilization of the efficient security algorithm for constrained IoT devices for a low cost client-side encryption and secure provisioning of constrained IoT devices onto the cloud.
- leveraging the efficient security algorithm for constrained IoT devices in dynamic resource sharing environments where computationally intensive tasks are off-loaded to the resource-rich ones for assisted processing, and compare the efficiency of the two methods.
- leveraging the method in [54] for a low power high speed True Random Number Generator (TRNG) using random telegraph noise to source for low power IoT-friendly encryption keys generation, in combination with the proposed solution to enhance client-side authentication, encryption and provisioning of an IoT device onto a cloud infrastructure.

B. Conclusion

We proposed an Efficient Security algorithm for Power Constrained IoT devices which aimed to reduce complexity of the currently used security algorithm: The Advanced Encryption Standard, in the IoT landscape. We showed a cryptanalytic overview and the associated consequence of such complexity reduction, together with a mathematical justification that the core algebraic properties of the algorithm are preserved, following which we provisioned a secure element: The ATECC608A for aiding authentication and guarding against implementation attacks in line with our analysis.

ACKNOWLEDGEMENT

This research work was supported by the Tertiary Education Trust Fund (TETFUND), Nigeria.

REFERENCES

[1] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, ser. HotNets-XIV. New York, NY, USA: Association for Computing Machinery, 2015. [Online]. Available: https://doi.org/10.1145/2834050.2834095

[2] I. E. Etim and J. Lota, "Power control in cognitive radios, internet-of things (iot) for factories and industrial automation," in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, 2016, pp. 4701–4705.

[3] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "Normachain: A blockchain-based normalized autonomous transaction settlement system for iot-based e-commerce," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4680–4693, 2019.

[4] O. Sohaib, H. Lu, and W. Hussain, "Internet of things (iot) in e-commerce: For people with disabilities," in *2017 12th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2017, pp. 419–423.

[5] H. Yu and X. Zhang, "Research on the application of iot in e-commerce," in *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 2, 2017, pp. 434–436.

[6] H. Desai, D. Guruvayurappan, M. Merchant, S. Somaiya, and H. Mundra, "Iot based grocery monitoring system," in *2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN)*, 2017, pp. 1–4.

[7] P. Gyeltshen and K. Osathanunkul, "Linking small-scale farmers to market using ict," in *2018 International Conference on Digital Arts, Media and Technology (ICDAMT)*, 2018, pp. 120–125.

[8] R. Dagar, S. Som, and S. K. Khatri, "Smart farming – iot in agriculture," in *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2018, pp. 1052–1056.

[9] K. T. E. Keerthana, S. Karpagavalli, and A. M. Posonia, "Smart system monitoring agricultural land using iot," in *2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR)*, 2018, pp. 1–7.

[10] K. Guan, D. He, B. Ai, D. W. Matolak, Q. Wang, Z. Zhong, and T. Kürner, "5-ghz obstructed vehicle-to-vehicle channel characterization for internet of intelligent vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 100–110, 2019.

[11] X. Luo, H. Zhang, Z. Zhang, Y. Yu, and K. Li, "A new framework of intelligent public transportation system based on the internet of things," *IEEE Access*, vol. 7, pp. 55 290–55 304, 2019.

[12] R. Silva and R. Iqbal, "Ethical implications of social internet of vehicles systems," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 517–531, 2019.

[13] K. Al-Gumaei, K. Schuba, A. Friesen, S. Heymann, C. Pieper, F. Pethig, and S. Schriegel, "A survey of internet of things and big data integrated solutions for industrie 4.0," in *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, 2018, pp. 1417–1424.

[14] D. C. Trancă, D. Rosner, R. Curatu, A. Surpăteanu, M. Mocanu, Pardău, and A. V. Pălăcean, "Industrial wsn node extension and measurement systems for air, water and environmental monitoring: Iot enabled environment monitoring using ni wsn nodes," in *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 2017, pp. 1–6.

[15] W. Sun, J. Liu, Y. Yue, and Y. Jiang, "Social-aware incentive mechanisms for d2d resource sharing in iiot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5517–5526, 2020.

[16] L. C. Souza, J. J. P. C. Rodrigues, G. D. Scarpioni, D. A. A. Santos, V. H. C. de Albuquerque, and S. K. Dhurandher, "An iot automated curtain system for smart homes," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 249–253.

[17] K. Hayashi and H. Suzuki, "Cooperation between heterogeneous iot devices using ihac hub," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1–2.

[18] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[19] Q. Luo, J. Liu, J. Wang, Y. Tan, Y. Cao, and N. Kato, "Automatic content inspection and forensics for children android apps," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[20] J. Wang, Y. Tan, J. Liu, and Y. Zhang, "Topology poisoning attack in sdn-enabled vehicular edge network," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[21] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Comput. Secur.*, vol. 68, pp. 81–97, 2017.

[22] A. Ferdowsi and W. Saad, "Deep learning for signal authentication and security in massive internet-of-things systems," *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1371–1387, 2019.

[23] E. Ruiz, R. Avelar, and X. Wang, "Poster: Protecting remote controlling apps of smart-home-oriented iot devices," in *2018 IEEE/ACM 40th International Conference on Software Engineering: Companion (ICSE-Companion)*, 2018, pp. 212–213.

[24] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the internet of things," in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2016, pp. 1–3.

[25] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[26] A. Riahi Sfar, Y. Challal, P. Moyal, and E. Natalizio, "A game theoretic approach for privacy preserving model in iot-based transportation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4405–4414, 2019.

[27] L. Scripcariu, P. Mătăsaru, and F. Diaconu, "Extended des algorithm to galois fields," in *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*, 2017, pp. 1–4.

[28] D. McGrew, "Low power wireless scenarios and techniques for saving bandwidth without sacrificing security," 2015.

[29] K. Tsai, Y. Huang, F. Leu, I. You, Y. Huang, and C. Tsai, "Aes-128 based secure low power communication for lorawan iot environments," *IEEE Access*, vol. 6, pp. 45 325–45 334, 2018.

[30] G. Liu, W. Quan, N. Cheng, H. Zhang, and S. Yu, "Efficient ddos attacks mitigation for stateful forwarding in internet of things," *Journal of Network and Computer Applications*, vol. 130, pp. 1–13, 03 2019.

[31] D. Gollmann, "Analysing security protocols," *Formal Aspects of Security*, pp. 71–80, 2002.

[32] K. B. Jithendra and T. K. Shahana, "New results in related key impossible differential cryptanalysis on reduced round aes-192," in *2018 International Conference On Advances in Communication and Computing Technology (ICACCT)*, 2018, pp. 1–5.

[33] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, 01 2010.

[34] A. Bar-On, O. Dunkelman, N. Keller, E. Ronen, and A. Shamir, "Improved key recovery attacks on reduced-round aes with practical data and memory complexities," *Journal of Cryptology*, pp. 1–41, 2019.

[35] h. y. microchip.com, title=Network and Accessories secure authentication.

[36] h. y. wikipedia.org, title=Big O notation.

[37] S. Gayathri Devi, K. Selvam, and S. P. Rajagopalan, "An abstract to calculate big o factors of time and space complexity of machine code," in *International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2011)*, 2011, pp. 844–847.

[38] G. Liu, W. Quan, N. Cheng, B. Feng, H. Zhang, and X. S. Shen, "Blam: Lightweight bloom-filter based ddos mitigation for information-centric iot," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–7.

[39] S. Yan, "Computational number theory and modern cryptography," *Computational Number Theory and Modern Cryptography*, 12 2012.

[40] S. Mitra, B. Jana, and J. Poray, "Implementation of a novel security technique using triple des in cashless transaction," in *2017 International Conference on Computer, Electrical Communication Engineering (ICCECE)*, 2017, pp. 1–6.

[41] M. Noura, H. N. Noura, A. Chehab, M. M. Mansour, and R. Couturier, "S-des: An efficient secure des variant," in *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*, 2018, pp. 1–6.

[42] D. Kumar, A. Reddy, and J. S A K, "Implementation of 128-bit aes algorithm in matlab," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 33, p. 126, 03 2016.

[43] C.-W. Hung and W.-T. Hsu, "Power consumption and calculation requirement analysis of aes for wsn iot," *Sensors*, vol. 18, p. 1675, 05 2018.

[44] N. Reilly, *Introduction to Applied Algebraic Systems*. Oxford University Press, 2009. [Online]. Available: https://books.google.co.uk/books?id=q33he4hOlKcC

[45] Y. He and S. Li, "A 3des implementation especially for cbc feedback loop mode," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2017, pp. 1–4.

[46] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[47] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[48] T. Wang, Y. Liu, and A. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, 08 2015.

[49] P. P. Jayaraman, X. Yang, and Ali, "Privacy preserving internet of things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Generation Computer Systems*, vol. 76, pp. 540 – 549, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17303308

[50] J. M. Hamamreh, H. M. Furqan, Z. Ali, and G. A. S. Sidhu, "An efficient security method based on exploiting channel state information (csi)," in *2017 International Conference on Frontiers of Information Technology (FIT)*, 2017, pp. 288–293.

[51] M. Bottarelli, G. Epiphaniou, D. K. B. Ismail, P. Karadimas, and H. Al-Khateeb, "Physical characteristics of wireless communication channels for secret key establishment: A survey of the research," *Computers Security*, vol. 78, pp. 454 – 476, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818300841

[52] A. Ghosal, S. Halder, and S. Chessa, "Secure key design approaches using entropy harvesting in wireless sensor network: A survey," *Journal of Network and Computer Applications*, vol. 78, pp. 216 – 230, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804516302880

[53] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with svd for reciprocal mimo channels," in *2016 International Symposium on Wireless Communication Systems (ISWCS)*, 2016, pp. 597–602.

[54] J. Brown, R. Gao, Z. Ji, J. Chen, J. Wu, J. Zhang, B. Zhou, Q. Shi, J. Crowford, and W. Zhang, "A low-power and high-speed true random number generator using generated rtn," in *2018 IEEE Symposium on VLSI Technology*, 2018, pp. 95–96.

[55] H. Deng, Z. Qin, L. Sha, and H. Yin, "A flexible privacy-preserving data sharing scheme in cloud-assisted iot," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[56] L. Liu, H. Wang, and Y. Zhang, "Secure iot data outsourcing with aggregate statistics and fine-grained access control," *IEEE Access*, vol. 8, pp. 95 057–95 067, 2020.

[57] A. Sahoo, S. S. Sahoo, S. Sahoo, B. Sahoo, and A. K. Turuk, "2020 international conference on communication systems networks (comsnets)," 2020, pp. 419–426.

VII. Appendix

This section holds more detailed proves of the theorems used in this paper.

Theorem 1: Let F be a field and let $n(x)$, $m(x)$ be polynomial elements in F, where $m(x = 0)$, then there exist unique polynomials (x) and $r(x)$ in F such that;

$$n(x) = m(x)(x) + r(x) \tag{3}$$

where either $r = 0$ or $deg(r(x)) < deg(m(x))$

proof: Firstly, we show the existence of the polynomials $(x$ and $r(x)$ satisfying 3 above, together with the requirement that either $r = 0$ or $deg(r(x)) < deg(m(x))$ and then we establish the uniqueness of these polynomials.If $deg(m(x)) = 0$, then (x)=c is a non-zero constant in F and by the inverse property of F, we have that:

$$n(x) = cc^{-1}n(x) \qquad \textit{by the identity in F}$$

.

$$c(c^{-1}n(x)) + 0 \qquad \textit{by associativity in F}$$

such that $m(x) = c^{-1}n(x))$ and $r(x) = 0$, satisfying (1). If on the other hand the degree of $m(x) \geq 1$, let Z denotes the set of all polynomials of the form $n(x) - m(x)(x)$, where $m(x)F$, then the degrees of all polynomials in Zform a set of non-negative integers and by the principle of the well ordering of natural numbers, there exists a smallest element of Z, say s. Let

$$r(x) = n(x) - m(x)\alpha(x) \tag{4}$$

Be such a polynomial of degree s in Z, then:

$$deg(r(x)) < deg(m(x)) \tag{5}$$

for if we suppose for contradiction that $deg(r(x)) > def(m(x))$, let $deg(m(x)) = m$ and let

$$m(x) = a_m x^m + ... + a_0, \qquad a_m \neq 0$$
$$r(x) = b_s x^s + ... + b_0, \qquad b_s \neq 0$$

As F is a field, we have that a$_m hasaninverseinF$ and so, let
$r_1(x) = r(x) - b_s a^{-1} x^{s-m} m(x) \in Z$
=$b_s x^s + ... + b_0 - ([b_s a^{-1} x^{s-m} m(x)]$
=$b_s x^s + ... + b_0 - b_s a^{-1} x^{s-m}(a_m x^m + ... + a_0)$
=$b_s x^s + ... + b_0 - [b_s a^{-1} x^{s-m} \times amx^m + ... + b_s a^{-1} x^{s-m} \times ama^0]$
=$b_s x^s$+...+b_0−[$b_s x^s$+$b_s a^{-1} x^{s-m} a_0$. by the inverse property of F. As
$b_s x^s - b_s x^s = 0$, $deg(r_1(x) = r(x) - b_s a^{-1} x^{s-m} m(x) < deg(r(x))$. This contradicts 4 which requires that $r(x)$ is of the least degree in Z and thus, validating 5 which validates 3 accordingly. To show that (x) and $r(x)$ are unique in the field F, let $\alpha_1(x) and r_1(x)$ be another pair of polynomials in F satisfying 3, then we have that:

$$n(x) = m(x)\alpha_1(x) + r_1(x) \tag{6}$$

where either $r = 0$ or $deg(r_1(x)) < deg(m(x))$. By the inverse and identity property of the additive operator in F, we have that:
$0 = n(x) - n(x)$
$\Rightarrow 3 - 6$
$= m(x)\alpha(x) + r(x) - (m(x)\alpha_1(x) + r_1(x))$

$$\Rightarrow (m(x)[\alpha(x) - \alpha_1(x)] = r_1 x \tag{7}$$

If $\alpha(x) - \alpha_1(x) \neq 0$, then $deg(m(x)[\alpha(x)\alpha_1(x)]) < deg(m(x))$ and thus making 7 a contradiction of the requirements of (4), which require that $deg(r_1(x)) < deg(m(x))$. Hence,

$$\alpha(x) - \alpha_1(x) = 0 \tag{8}$$

Substituting 8 into 7 shows accordingly that

$$r_1 x - r(x) = 0 \tag{9}$$

From 8 and 9, we have that $\alpha(x) = \alpha_1(x)$, $r_1 x = r(x)$ and thus, showing the uniqueness of $\alpha(x)$ and $r(x)$ in F and hence, 3.

Theorem 2: Let F be a field, and $n(x)$ and $m(x)$ be non-zero polynomials in F, then $n(x)$ and $m(x)$ have a unique monic greatest common divisor, say $d(x)$ in F such that:

$$d(x) = \alpha(x)n(x) + \beta(x)m(x) \tag{10}$$

proof: Let $d(x) = d_0 + d_1 x + + d_n x^n$, $d_n \neq 0$ be a polynomial greatest common divisor of $n(x)$ and $m(x)$ in F. As a greatest common divisor is not unique, if $d_n \neq 1$, by the inverse property of F, there exists $d_n^{-1} \in F$ such that $d_n^{-1} d(x)$ is also a greatest common divisor. Let $d_1(x)$ be another monic greatest common divisor of $n(x)$ and $m(x)$ in F, then $d(x)|d_1(x)$ and $d_1(x)|d(x)$.
$\Rightarrow \exists y(x), z(x) \in F$: $d_1(x) = y(x)d(x)$ and $d(x)$ = z(x)$d_1(x)$
$\Rightarrow deg(d_1(x)) \geq deg(d(x))$ and $deg(d(x)) \geq deg(d_1(x))$
$\Rightarrow \deg(d_1(x))$ = $\deg((d(x))$
$\Rightarrow \deg(y(x))$ = $\deg(z(x))$

This implies that $y(x)$ and $z(x)$ are constants in F and since $d(x)$ and $d_1(x)$ are monic polynomials, then $y(x)$=$z(x) = 1$, and $d_1(x) = d(x)$. Therefore, the monic greatest common divisor $d(x)$, of $n(x)$ and $m(x)$ in F is unique and hence, Theorem 2.

Theorem 3: Let $F = GF(2^8) = GF(P^n)$ be a field, then there exists an irreducible polynomial of degree n over Z_p

proof: As F is a field, let g be a generator element in F. Also, let $p(x)$ be a minimal polynomial of degree n in F. By the property of the generator element g, we have that every element in F occurs as a power of g and as such, the minimal polynomial $p(x) = p_g(x)$. Let

$$(deg(p_g(x))) \tag{11}$$

By Theorem 1, there exists polynomials say $n(x))$, $r(x)) \in F$ such that for any constant c, $x^c = n_c(x)p_g(x) + r_c(x)$ with either $r_c(x) = 0$ or $deg(n_c(x)) < deg(p_g(x)) = m$. Substituting g, $g^c = n_c(g)p_g(g) + r_c(g)$ and as $p_g(x)$ is a minimal polynomial, we have $g^c =_c (g).0 + r_c(g)$
$\Rightarrow g^c = r_c(g)$. But as g is a generator element in $F = GF(p^n)$, we have that $g^{p-1} = 1$ and as such, the highest number of the distinct powers of g is $p^n - 1$ and by 11, we have that the highest number of the distinct powers of the generator $g = p^m - 1$, which implies that $n \leq m$. Also, as $p_g(x)$ is a minimal polynomial in F, for any two polynomials say $j(x)$ and $z(x)$ in F, $j(g) = z(g)$.
$\Rightarrow j(g)$ - $z(g)$ = 0
$\Rightarrow j(x)$ - $z(x)$ = 0

Since $deg(j(x) - z(x)) < deg(p_g(x))$, then the number of elements in $F = GF(p^n)$ is at least as big as the number of polynomials in F with degree less than m. This implies that $m \leq n$. Whereas, $m \leq n$and $n \leq m$ implies that $m = n$. Therefore, $deg(p_g(x)) = n$ and since $p_g(x)$ is a minimal polynomial, $p_g(x)$ is then an irreducible polynomial in $F = GF(p^n)$.