Online Resource 1:
Introduction and Related Work

February 20, 2022

0.1 Introduction

Internet of Things (IoT) deployments hold the promise to revolutionize the technology landscape through the unprecedented connectivity of billions of devices, with the massive connectivity and application cutting across a variety of sectors and redefining the norms in transportation [1–3] businesses [4–8], healthcare, agriculture [9, 10] and homes [11, 12] to mention a few.

The National Institute of Standards and Technology (NIST)'s definition of cloud computing is given as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [13]. While IoT devices/deployments generates massive data in petabyte scale, storage and leveraging these data is hugely assisted by possibilities availed by cloud computing platforms. Cloud computing technologies continue to roll out robust cloud infrastructure in service to the massive connectivity promised by the actualization of the IoT. Leading cloud services providers including but not limited to Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, The Things Networks (TTN) provide robust cloud infrastructure in service to the massive deployments of the IoT for a variety of use-cases. However, the unprecedented deployment of devices in the IoT ecosystem is accompanied by the burden to secure the devices to ensure the safe use of the technology. As majority of IoT devices are constrained devices which are mostly deployed for use cases involving capturing/monitoring realtime situations and pushing the associated data onto safe storage in cloud platforms, the cost of encrypting IoT data and the need to ensure safe transportation of the data to the cloud pose a challenge. With the IoT requiring novel solutions for it's safe use, ensuring that the data generated by these devices is safe and securely transported to a choice cloud platform is a huge security concern. According to [13], Secure authentication unto cloud platforms is one of the challenges in cloud adoption. This is made worse by the constrained nature of the IoT devices in resources including power and processing capabilities. Client-side encryption which means that data is encrypted at the end of the device before onward transfer unto a cloud platform for storage or processing is advocated. According to [14], with client-side encryption, data is encrypted before it is transferred to a cloud platform to ensure that content is transferred and stored in encrypted format and that only clients with the appropriate decryption keys have access to non-encrypted information. Furthermore, the efficient use of classical encryption schemes for appropriate client-side encryption before cloud storage is an additional challenge given the scarcity of power and computing resources available for the constrained IoT device. Provisioning an IoT device onto a cloud platform entails the process of creating a unique identity on the cloud via requisite and secure authentication credentials, while client-side encryption is used to achieve encryption of data at the end of the device before it is sent unto cloud storage.

0.1.1 Motivation

According to [15], It is estimated that billions of IoT devices will be deployed by year 2020, however, very little to no information is present on ease of device provisioning. Secure authentication of IoT devices that are constrained in power, memory and processing resources is an ongoing challenge desiring novel solutions. Usually, these tiny IoT devices run by battery power, making it a daunting task to design security mechanism which is a best fit [16].

According to [16], some of the challenging problems in the implementation of the IoT include: key management, device authentication, user access control, privacy preservation and identity management to mention but a few. Many attacks including eavesdropping, Denial of Service (DoS), Man-in-the-Middle and certificate manipulation among others is a serious threat to the authentication of IoT devices and the constrained nature of the devices has imposed a serious challenge in designing counter measures to combat these attacks [16] . On another front, encryption-before-outsourcing is a widely recommended method to guarantee the confidentiality of user data [17] and the consequent 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 [18] and according to [19] , 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.

0.1.2 Contributions

Motivated by the challenges in literature; and few of which are highlighted in the motivation section above, this work investigates resource constrain on a sample IoT device (SAMG55 microprocessor), implemented a low-cost client-side encryption algorithm for data encryption as advocated in [18], and leverages the ATECC608A in effort to addresses the challenges of key management and device authentication as highlighted in [16], by securely provisioning the device on an IoT cloud services platform. The main contributions of this paper can thus be summarized as follows:

- Experimentation and analysis of resource constrain in IoT devices by comparing a PC and SAMG55 implementations of a Low-cost algorithm for client-side encryption to the standard AES128.
- Implementation and comparison a Low-cost algorithm (Based on the AES) to ligh-weight CLEFIA, experimentation of the avalanche effect test on the low-cost algorithm and using it as client-side encryption solution in provisioning the SAMG55 microprocessor.
- Secure provisioning of a sample IoT device (SAMg55 microprocessor) on AWS IoT core using the Amazon Web Services (AWS) Command Line Interface (CLI) programmatic access tools.

The investigation of resource constraint on the IoT device compared the implementations of the a low cost algorithm and the standard AES, on the SAMG55 microprocessor and a laptop computer to show the consequence of the scarcity of computing resources on IoT devices. The low cost Security algorithm for constrained IoT devices was detailed [20], wherein we presented a cryptanalytic overview of the consequence of reducing the complexity of the standard AES algorithm through round reduction, together with a mathematical justification. Our experimentation shows an increase of up to 657% in the encryption completion time on the IoT device in comparison to the PC due to resource constrain. The low-cost algorithm shows upto 50.3% reduction in the aforementioned encryption completion time

and so, was utilized for experimenting low cost client-side encryption and the device provisioned to the cloud.The idea experimented in the article aims to address the challenges of privacy and secure authentication within the body of security issues in the domain of IoT.

0.2 Related Work

0.2.1 Cloud Computing

According to [13], cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing deployment models range from: a private cloud deployment where the cloud services are provided for private use of a single organization with many users, a community cloud which is often deployed in the use-case of many organizations coming together to form a community of shared required cloud services, a public cloud which is open for public use in contrast to the private and community deployments models and often deployed by government or private business owners and finally, a hybrid deployment model which is often a combination of any two or all of the aforementioned deployment models. In [21, 22], cloud service models are discussed to range from the provision of software as a service, platform as a service and infrastructure as a service in cloud deployments; where software as a service provides room for users to rent software's on the cloud instead high spending in buying the software's, Platform as a Service (PaaS) provides a development platform services and Infrastructure as a Service (IaaS) which provides compute resources including network devices, memory and storage among others [22]. According to [13], cloud computing has gone beyond being just a technical solution to also include a business model through which computing power can be sold and rented. From a public cloud deployment stand point owned by businesses, Cloud computing is defined as the on-demand delivery of IT resources and applications via the internet with a pay as you go pricing model in [23]. The massive roll out of resources occasioned by cloud computing has led to the emergence of various cloud platforms as not just the choice for provisioning the IoT but a defector enabler towards the complete actualization of ubiquitous deployments of the IoT as according to [17], Cloud-assisted IoT has become an increasingly popular technological trend, as the performance of IoT applications can be greatly improved by delegating the cloud to manage massive IoT data. To this end, a massive leeway has been had been created for the massive provisioning of the IoT, with the constrained devices outsourcing among other things; storage of generated data on to the cloud. More so, the traditional security architecture is said to be broken as the user does not own the cloud [13] and so, creating the need for due diligence necessary for effectively harnessing the advantages of the cloud as utilized by IoT devices in outsourcing data and consequently, the need for encrypting data at the device-end before pushing it to the cloud. data stored in the cloud can be encrypted at rest or in flight, with encryption at rest being either at the end of the IoT device (Client-side Encryption) or on the cloud (Server-Side Encryption). However, even with the deployment of state of the art protocols such as the Transport Layer Security (TLS) for securing remote communications between the IoT devices and the cloud as a countermeasure, vulnerabilities remain and attacks can occur between an IoT device and the cloud during translation protocol of secure transport protocol in Constrained Application Protocol (CoAP) [24].

0.2.2 Device Authentication

The authors in [16] observed that some of the challenging problems in the implementation of the IoT include: key management, device authentication, user access control, privacy preservation and identity management to mention but a few. According to [25], authentication of IoT devices is crucial as security and privacy stand as vital issues in connecting IoT devices which send information to and from users and offload information in the cloud. However, traditional security mechanisms consume too much energy and thus the much needed research of cheaper security mechanisms for constrained IoT devices [25]. In [13], secure authenticating an IoT device onto a cloud platform is highlighted as one of the major issues affecting cloud adoption. The authors in [26] observed that as a resulting consequence of less storage capacity, memory and processing capability, many IoT devices have to be operated on lower power and hence, the security measures fail here and the devices become the victim of expensive cryptographic processes. In [26] a distributed algorithm is proposed to be used in the IoT structure in order to reduce the security risks that confronting low-powered devices was proposed. In attempt to address issues bothering on data security in the IoT paradigm, Named Data Networking (NDN) have also been used as signature schemes to aid authentication mechanism in the IoT. However, the authors in [27] highlighted the drawbacks of applying the NDN-IoT schemes as potentially requiring additional encryptions to be carried out by constrained IoT devices and thus, imposing the problems of cryptography-based authentication and vulnerability to impersonation attackers with higher processing powers that are capable of reconstructing authentication keys. They proposed a solution that integrates the lightweight and unforgeable physical-layer identity (PHY-ID) into the existing NDN signature scheme. Keys used for establishing communication sessions are traditionally negotiated using key agreement protocols of public keys and private key pairs. However, the authors in [28] observed that embedded systems are limited in their capability to implement public key encryption and client- side authentication. Proposing a solution with respect to the constrained characteristics of these devices, they proposed a protocol that seeks to remove the need for public key or certificate-based authentication by using Physical Unclonable Function-based identity. In [19], the small key size and computational efficiency of Elliptic Curve Cryptography is advocated as preferable for better security solutions over other Public Key Cryptography, with respect to the constrained resources of power, processing and memory of the devices. According to [16], authentication aims to identify the identity of a Thing, and it's detailed in a two-step process viz: the presentation of an identity and verification of the identity created, whereas one of the major challenges for constrained IoT devices remains the secure management of these authentications keys. Consequently, deploying constrained IoT devices with a more secure management of security keys which are used during authentication is highly advocated.

0.2.3 Client-side encryption and Constrained IoT Devices

client-side encryption is used to achieve encryption of data at the end of the IoT device before it is sent onto cloud. According to [29], a study by HP estimates that about 70% of devices don't encrypt data in communications over networks. Within the context of the IoT, this is largely due to the constrains of limited computing capabilities of the devices as according to [30], the integrated circuits (ICs) deployed in IoT based infrastructures have strong constraints in terms of size, cost, power consumption and security unlike in desktop computers, tablets, and so on, IoT devices are unable to allocate considerable memory and processing energy just for security functions [30]. The authors in [17] observed that to

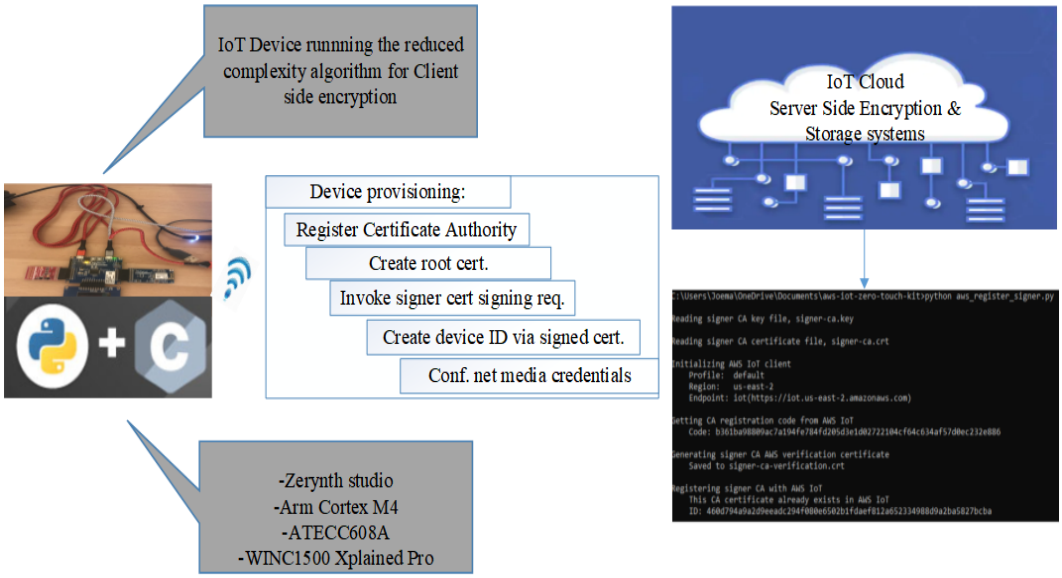

Figure 1: Experimental setup

protect the confidentiality of data outsourced from IoT devices to the cloud, cryptographic mechanisms are usually employed to encrypt the data in such a way that only the user designated by the data owner can decrypt the data. They proposed a privacy-preserving data sharing scheme in cloud-assisted IoT which employs identity-based encryption and linear secret sharing that both preserves privacy of the IoT data pushed to the cloud as well as allow for flexible sharing of encrypted data between connected devices. The authors in [30] highlighted the main challenges identified in the deployments of IoT devices as resilience of the deployed infrastructure, confidentiality, integrity of exchanged of exchanged data, user privacy and authenticity among others. According to [31], since more devices are being programmed to exchange data autonomously in IoT deployments, the importance of security and authenticity of such transmitted data is very crucial and thus requiring strong security approaches to prevent both passive and active attackers. According to [30], the insurance of privacy and data protection remains a challenge in IoT deployments desiring of solutions. They discussed the challenges, implementation and future applications of Light Weight Cryptographic schemes in securing constrained IoT devices. Taking the constrained characteristic of the IoT devices into consideration, [32] proposed varying levels of security measures dependent on the confidentiality requirements of the data. [31] proposed a secure communication scheme for IoT devices which applies the Diffie-Hellman algorithm for authentication and uses the AES and Message Digest (MD)5 algorithms for encryption and validation respectively, of transferred data.

0.2.4 Light Weight Cryptography

According to [33], Lightweight cryptography is generally defined as the cryptography for resource constrained devices, for which Radio Frequency Identification (RFID) tags are

mentioned as examples. Consequent upon the constraints on low power devices in terms of area, processing capabilities, memory and scarce power resources, Light weight cryptography emerged in efforts to ensure the security of these devices in the digital communication space. As rightly put by [34], Lightweight Cryptography (LWC) or protocols are tailored for implementations in constrained environments including RFID tags, sensors, contact less smart cards, health care devices and so on. The development of lightweight cryptographic protocols therefore, is chiefly anchored on the need to develop cheaper security schemes that are compatible with the constrained nature of these devices and without compromise to security. In [29], the performance analysis of two lightweight ciphers: CLEFIA and PRESENT was presented with respect to security strengths, throughput and resource utilization, which had the latter outperforming the former in terms of memory usage, security, and the former outperforms the latter in terms of throughput. PRESENT is a lightweight algorithm with a Substitution Permutation Network (SPN) structure, and utilizes thirty one rounds of:XOR RoundKey, S-box layer and P-layer, with a final (32nd) round which XORs the STATE produced from the first thirty one rounds and the round key. It carries out message encryption in sixty four (64) bits blocks and and supports key lengths of sixty four (64)bits and one hundred and twenty eight (128)bits. The efficiency of CLEFIA in comparison to other conventional ciphers such as the AES, Camelia and Seed is detailed in [34], wherein the efficiency of lightweight ciphers -defined as a ratio of throughput and gate size, is presented with respect to energy consumption.

Bibliography

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] O. Sohaib, H. Lu, and W. Hussain, "2017 12th ieee conference on industrial electronics and applications (iciea)," 2017, pp. 419–423.

[6] H. Yu and X. Zhang, "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.

[7] H. Desai, D. Guruvayurappan, M. Merchant, S. Somaiya, and H. Mundra, "2017 fourteenth international conference on wireless and optical communications networks (wocn)," 2017, pp. 1–4.

[8] P. Gyeltshen and K. Osathanunkul, "2018 international conference on digital arts, media and technology (icdamt)," 2018, pp. 120–125.

[9] R. Dagar, S. Som, and S. K. Khatri, "2018 international conference on inventive research in computing applications (icirca)," 2018, pp. 1052–1056.

[10] K. T. E. Keerthana, S. Karpagavalli, and A. M. Posonia, "2018 international conference on emerging trends and innovations in engineering and technological research (icetietr)," 2018, pp. 1–7.

[11] L. C. Souza, J. J. P. C. Rodrigues, G. D. Scarpioni, D. A. A. Santos, V. H. C. de Albuquerque, and S. K. Dhurandher, "2018 international conference on advances in computing, communications and informatics (icacci)," 2018, pp. 249–253.

[12] K. Hayashi and H. Suzuki, "2019 ieee international conference on consumer electronics (icce)," 2019, pp. 1–2.

[13] S. Aldossary and W. Allen, "Data security, privacy, availability and integrity in cloud computing: Issues and current solutions," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 4, 2016. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2016.070464

[14] E. Henziger and N. Carlsson, "Delta encoding overhead analysis of cloud storage systems using client-side encryption," in *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2019, pp. 183–190.

[15] O. Ali, M. K. Ishak, L. Wuttisittikulkij, and T. Z. B. Maung, "2020 international conference on electronics, information, and communication (iceic)," 2020, pp. 1–5.

[16] A. K. Sahu, S. Sharma, S. S. Tripathi, and K. N. Singh, "2019 international conference on information technology (icit)," 2019, pp. 217–221.

[17] 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.

[18] 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.

[19] 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.

[20] J. N. Mamvong, G. L. Goteng, B. Zhou, and Y. Gao, "Efficient security algorithm for power-constrained iot devices," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5498–5509, 2021.

[21] I. Nowrin and F. Khanam, "2019 international conference on applied machine learning (icaml)," 2019, pp. 183–186.

[22] T. L. Mokgetse and R. Sridaran, "2019 6th international conference on computing for sustainable global development (indiacom)," 2019, pp. 1218–1222.

[23] J. Baron, H. Baz, T. Bixler, B. Gaut, K. E. Kelly, S. Senior, and J. Stamper, *AWS certified solutions architect official study guide: associate exam.* John Wiley & Sons, 2016.

[24] H. Boujezza, H. Kaffel-Ben Ayed, and L. A. Saïdane, "2017 13th international wireless communications and mobile computing conference (iwcmc)," 2017, pp. 423–428.

[25] S. Sahoo, S. S. Sahoo, P. Maiti, B. Sahoo, and A. K. Turuk, "2019 6th international conference on signal processing and integrated networks (spin)," 2019, pp. 1024–1029.

[26] A. S. Rachini and R. Khatoun, "2020 sixth international conference on mobile and secure services (mobisecserv)," 2020, pp. 1–5.

[27] P. Hao and X. Wang, "Integrating phy security into ndn-iot networks by exploiting mec: Authentication efficiency, robustness, and accuracy enhancement," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 5, no. 4, pp. 792–806, 2019.

[28] M. S. E. Quadir and J. A. Chandy, "2020 ieee international conference on consumer electronics (icce)," 2020, pp. 1–6.

[29] M. Jangra and B. Singh, "Performance analysis of clefia and present lightweight block ciphers," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 8, pp. 1489–1499, 2019.

[30] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "2019 ieee 5th world forum on internet of things (wf-iot)," 2019, pp. 707–710.

[31] K. Quist-Aphetsi and M. C. Xenya, "2019 international conference on cyber security and internet of things icsiot," 2019, pp. 88–92.

[32] S. Rajashree, P. Gajkumar Shah, and S. Murali, "2018 ieee international conference on internet of things (ithings) and ieee green computing and communications (greencom) and ieee cyber, physical and social computing (cpscom) and ieee smart data (smartdata)," 2018, pp. 219–221.

[33] S. B. Sadkhan and A. O. Salman, "A survey on lightweight-cryptography status and future challenges," in *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, 2018, pp. 105–108.

[34] M. Katagi, S. Moriai *et al.*, "Lightweight cryptography for the internet of things," *Sony Corporation*, vol. 2008, pp. 7–10, 2008.