SHAAES BASED ON CHAINING BLOCK CODE AND GALOIS COUNTER MODE ENCRYPTION MODES FOR PRIVACY OF SMART FARMING SYSTEMS

[1]Alfa, Abraham Ayegba, [2]Aro, Tayo Oladele, [3]Adunni, Oyenike Olukiran, [4]Iliya, Danjuma Zakwoi, [5]Awe, Oluwayomi, [6]Ayodeji, Ayodeji

[1,2]Computer Science Department Confluence University of Science and Technology, Osara
[3]Computer Science Department, Ladoke Akintola University of Technology, Ogbomosho
[4]Computer Science Department, Niger State College of Education, Minna
[5]Computer Science Department, University of Lagos, Lagos
[6]Computer Science and Mathematics Department, University of Stirling, UK.

E-mail: talk2danjumazakwoi@gmail.com

Abstract

In smart farming, IoT plays a dominant role in diverse data generation and transmission in applications such as irrigation estimation, soil and environmental monitoring, food supply chain, and field monitoring. The current architecture of IoT is mainly centralized and single-point controlled; thereby opening up privacy and security lapses. Several approaches have favoured advanced encryption of data for the purpose of preserving privacy during transmission and storage. The top challenges sparingly reported by previous works include the security of physical and logical components of IoT systems; software and hardware interoperability; energy requirements; processing/storage capacity, and network architectures/scalability. This paper performs a comparative analysis of encryption modes of Chaining Block Code (CBC) and Galois Counter Mode (GCM) with SHA1-256 and AES246 (SHAAES) algorithms in preserving the privacy of IoT data. It was found that advanced cryptographic schemes interleaved with hardening schemes (such as CBC and GCM) offer great benefits. The outcomes revealed that the SHAAES scheme based on CBC was better in for speed of encryption (8.34%) and decryption (43.42%); storage consumption for secret key sizes (50.00%) and ciphertext sizes (26.88%) against GCM. This implies that the GCM approach offers the highest privacy protection but is less effective due to sluggish speed and memory utilization. Though, future works could consider modifications to the complex processes of traditional cryptographic schemes to make them simpler (lightweight) and easily applicable to resource-constrained devices.

Keywords: CBC, GCM, Encryption, Privacy, Smart Farming, IoT, Memory, Speed.

1 Introduction

Smart farming utilizes the idea of precision farming to raise farm produce through the understanding and knowledge of the variability of a crop field. This entails the analysis of the environmental factors and distribution of the different inputs based on the specificity of the farmland or (or site). There are great prospects for better yields, and optimizing farming efforts including higher profitability, wastage reduction, higher productivity. Though, it is nearly impossible for farmers to obtain full-grasp of the various variability linked to the environment

because of large inherent uncertainties. The smart farming practice offers provide farmers the opportunity to simplify and automate the process of acquiring and analysing farm data, which leads to faster, intelligent and automated decision making (Bala *et al*., 2021).

Smart farming utilizes modern information and communication tools in agricultural practices popularly referred to as the third green revolution. One issue at the front burner of farming practices across the world is the global warming phenomenon. In part, smart agriculture drive targeted the wireless sensor network in the attempt to deal with the developing problems of global warming. Aside that, many farmers are unable to benefit maximally from smart farming technologies for effective farming practice in most developing economies. Crop yield depends greatly on the ability of farmers make faster and accurate decisions. Notwithstanding, accurate appropriate decisions by farmers need right information/knowledge or information about different contiguous factors such as soil condition, weather, precise amount of fertiliser to be applied, sunshine, water-filed property, rainfalls, topography and infiltration. Consequently, sensors have potential to effectively collect the farming environmental parameters for the purpose of making smarter and faster decision by means of computer-based solutions (Surai, Kundu, Ghosh, and Bid, 2018).

The spate of climate change globally has further informed the greatest desire of governments to safeguard food security through maintenance and growth agricultural production. This rapid climate changes in various abiotic factors including rainfall, drought, temperature, flooding, and solar radiations continue to adversely impact on rice production at different stages of growth (Hussain *et al.,* 2020). The information provided by crops can become veritable tool for modern agricultural practice in the quest for environmental protection, food production sustainability, cost-savings and improved decision making (Saiz-Rubio and Rovira-Más, 2020). The IoT is the cutting-edge Internet growth integrating billions of Internet-enabled sensors, displays, cameras, smart phones, wearable, and others devices for the purpose of communicating through the Internet backbone (Jayaraman *et al.*, 2017).

IoT is the bane of the Internet project because; it empowers end-users, machines and everyday Things to sense, communicate and interact with their outside world. The IoT are premised on offering humans more convenient, safe and increased quality of life through wide-ranging applications including smart homes, Industrial IoT, Internet of Farming, smart city, health, and others (Berrehili and Belmekki, 2017; Brandão, Mamede, and Gonçalves, 2018). There are key technological shortfalls of IoT including the trade-offs between energy consumption, size and weight of devices, autonomy and wireless communication coverage, scalability, efficiency and hardware constraints (Nóbrega *et al.*, 2019). There are two key problems limiting IoT-based applications including: the insecure ad hoc exchanges and inability to establish temporary session keys. There are renew interests for symmetric cryptography especially lightweight ciphers such as Present; this is dissimilar to asymmetric cryptography, which are unsuitable for constrained devices metrics such as chip area, code size, energy dissipation, and runtime. Consequently, there is the need to remove key exchanges or pre-shared keys problems through less-expensive asymmetric schemes to enhance security of applications in real-world scenarios (Buchmann *et al.*, 2016).

There are exist issues of privacy due to widespread nature and vulnerability of underlying IoT networks (Berrehili and Belmekki, 2017). In fact, things progression happens more speedily adding to the concerns and risks such as effective management of huge quantity of data, low process power, high energy dissipation, security threats, and huge data encryption and decryption technique suitability (Singh *et al*., 2017). IoT devices have limited computing capacity, low power consumption and low volume, which have compounded the complexity of implementing reliable cryptographic methods available (Kuznetsov *et al.*, 2019). Encryption strategies have been deployed for the securing data transmissions and diverse transactions in Blockchain applications (Hassan, Rehmani, and Chen, 2019). As a result, Buchmann *et al*. (2016) enlisted the requirements of encryption approaches appropriate for IoT devices to include: single execution per session, shorter keys and reduced size of codes, faster encryption, key generation and decryption operations. While, ensuring that these kinds of encryption schemes must be derived from lattices, number theory and codes cryptography. Again, efforts must be geared towards low-resource devices and hardware implementation considerations.

In this paper, two encryption modes-based hybrid cryptographic algorithms were investigated to ascertain their level of privacy guarantees for smart farming systems. The remaining sections are organized as follows: section two provides the related works, the research methodology is outlined in section three, the section presents the results and discussion, and the section five contains the conclusion.

1.1 Security Outlook of Smart Farming Systems

The speedy development in IoT technology has facilitated tangible and intangible values to be entrusted in IoT networks including physical assets, and digital sensitive data (Papageorgiou *et al.*, 2020). The process of collecting data, storing data and utilizing data are prone to privacy concerns in big data, IoT and cloud computing technologies. The means of providing protection in terms of privacy of cloud data remain an open area of research with solution deserving urgency (Maohong, Aihua, and Hui, 2018). Cloud data storage and transactions are susceptible to fraud, lack of transparency among parties, corruption and mismanagement especially in distributed ledger databases and centralized storage architectures (Ajao *et al.*, 2019). In particular, IoT systems are susceptible to threats and attacks in the following ways: devices, connectivity medium, computing, storage and microservices (Al-masri *et al*., 2020).

Wireless technology is the backbone for IoT, which is utilized commonly for real-time collaborations with high efficiency in areas such as military, precision monitoring, remote monitoring, commercial, smart home and other fields. The security challenge of IoT due to the Internet connectivity are worsening due to trust and malicious tendencies. Aside these, the physical features of IoT have constrained many existing security solutions including: computational, power, transmission range and memory are short-leaved (She *et al*., 2019). In fact, another conventional approach for securing IoT networks utilized Public Key Infrastructures systems, though, incapable of meeting the peculiarities of IoT components including centralized authority for public key validation, exploitations and singular points of failure (Papageorgiou *et al*., 2020).

However, public blockchain technology has capacity to safeguard the privacy of data in IoT and resource constrained devices not without its shortcomings such as large bandwidth overhead, extended computation, latency and restricted scalability (Giannoutakis *et al*., 2020; Mohanty *et al*., 2020). The target of security functions for IoT could be at the network edge (local level) or at the physical hardware/software level (Al-masri *et al*., 2020). Aside from this, the middleware software-oriented architecture of publish/subscribe enables interoperability of systems such as IoT and BCT (Abou-Nassar *et al.*, 2020). The user needs to sign a message (or transaction) with a private key of the user, and the public key checks and verifies the access privileges to BCT. The Elliptic Curve Digital Signature Algorithm (ECDSA) is effective for creating random private keys for the purpose of signing messages, and a matching public key for verifying/checking signatures. Notably, ECDSA started Public Key Infrastructure (PKI) for Internet applications and open-source projects. It offers high bit security due to the capability to calculate a point multiplication and is incapable of reversing (or computing the multiplicand with original and product points). It is public key cryptography and the cryptography for Bitcoin Blockchain (that is, private and public keys generations) and secure communications, critical infrastructure, protected Internet exchanges, smart devices, Wireless Fidelity (WiFi,) and several BCTs. In general, Blockchain Technology is well thought-out as a disruptive technology, and renowned for cryptographic-founded algorithms but, vulnerable to Quantum Computing attacks (Campbell, 2019).

The forms of cryptography deployed by Distributed Ledger Technology (such as blockchain technology) target the eminent issues of Quantum Computing including post-quantum digital signature, public key encryption, and Key Encapsulation Mechanism (KEM) Encryption. The class of Signature generates private keys with lattice-grounded approaches, which have verifiable hardness, higher space for a message, smaller public key sizes, and minimal overheads. Though Ring Learning with Errors (RLWE) and Learning with Errors belongs to the lattice group, the former is more effective for IoT devices.

2. Related Works

The mode of encryption systems requires public or private keys to be broadcast through the network infrastructure and participants alongside the encrypted messages. This approach is faced with the problem of privacy leaks and compromises. By original intention, the rights of exclusive access and usage of data rest on owners of keys or users or service providers in case of cloud services. The growths of untrusted server, cloud operators and providers have further compounded the anonymization problems because; it is possible to retain, manipulate and link users' transactions with their identity in a long run for personal data available on the cloud. (Acar *et al.*, 2018) identified Homomorphic Encryption (HE) as capable of dealing with trust issues caused by third party manipulation of users' data encrypted in the cloud but, it makes decryption impossible.

Patel, Oza, and Agrawal (2019) noted that, ciphertexts require HE techniques in addition to the public keys based traditional encryptions in order to allow direct operations on them. In particular, data broadcasts, retrieval, storage and aggregation need privacy protection

application of homomorphic cryptosystems in the aspect of cloud computing and wireless sensor networks. HE in itself alone cannot guarantee privacy preservation but, it has a lot of potential in concealing data and increasing confidentiality of encrypted ciphertexts during diverse computations.

One main technique for introducing threshold functionality to a universal group of non-threshold cryptographic approaches was initiated by (Boneh *et al.*, 2018). The concept allows a secret key to be subdivided into arbitrary sizes of shares that can be utilised by parties of threshold without the need for complete key rearrangement. The first step built the threshold fully-homomorphic encryption technique (ThFHE) using learning with errors (LWE) problem. Second step makes use of universal Thresholdizer for generating majority of distinct threshold systems. Lastly, the new ThFHE generates threshold functionality from the universal threshold, which are appended to systems including CCA-Secure public-key encryption, pseudorandom functions, signature-based schemes, and other several primitives. The benefit of applying ThFHE to lattice signature system is the single-round threshold signature approach from LWE problem domain. This new framework offers the opportunity for resolving the age long challenge of attaining one-round threshold signatures in lattices.

The outsourced data privacy-preservation for user-specific services was investigated by Pagnin *et al.* (2018). The cloud warehouse data about users in which the service providers carryout computational function in order to meet user-centric services. These operations cannot guarantee privacy, that is, servers are unable to access the plaintexts or service provider being incapable of decrypting complete data unless user-approved computations. The new security solution is based on the labelled homomorphic encryption method (LEEG), which supports FEET algorithms to form a lightweight protocol known as HIKE. The HIKE provides secure and private safekeeping, computation, non-disclosure of users' data in efficient and succinct ways. Nevertheless, HIKE is a weak countermeasure for malicious server attacks because it is built on semantic-secure homomorphic encryption approach. More importantly, HIKE has lots of potential as cryptographic protocol for real-time application privacy.

Safe storage status of data can be achieved through prior encryption. The task of encrypting data has given rise to much vulnerability rendering it unfit for ciphertexts operations. According to Gai and Qiu (2018), a fully homomorphic encryption enables varying computation to be performed on ciphertexts. Consequently, blended arithmetic (that is, addition and multiplication) on real quantities was proposed known as fully homomorphic encryption for blended operation (FHEBO) model. The goal was to implement blended arithmetic operations on cloud in a less complicated manner. Aside a data owner-centric technique and mathematical computation of Tensor-based FHE ensured data are encrypted remotely prior to broadcast to the receiver. There are still problem of vulnerable channels and cloud architecture not leaving out complex blend operations, which can cause overheads.

The capability of embedding image data in communication system and embedding device are emerging. Lightweight stream encryption (LWSE) algorithms for images have developed for many desktop PCs. The emphasis on real-time attribute of available LWSE such as memory

capacity and time of execution are undesirable for low power embedded devices built on ARM7 core. Janakiraman *et al.* (2018) proposed a change to LWSE algorithm by inserting shuffling process on the plain image before encryption. The outcomes showed that the modified LWSE were supportive of secure embedded hardware in terms of code size and execution time for real-time applications. In numerous IoT applications, the reliability and efficiency are a significant measure in that the aggregator persistently gathers and analyses data, a break in data transmission impacts adversely on the performance of the system.

The introduction of encryption scheme into the process of data analysis raised concerns about complex computation, increased demands on the CPU load, temperature of device and broadcast delays within channels. Consequent upon this, encryption of data in networks is capable of imposing timing overheads in IoT; therefore, undesirable regardless of the security benefits. Though, the findings by Richards *et al.* (2019) showed that utilising 128-bit key length for Cipher-Block Chaining (CBC) encryption was 1.24 times longer than Counter (CTR) and 2.54 times later than Electronic Codebook (ECB). Conversely, the decryption for CBC is 5.08 times more than CRT and 3.71 times later than ECB. The key sizes of 192 and 256-bits were produced relatively similar or longer timing for data encryption and decryption respectively. However, lightweight AES encryption algorithm more applicable for resource constrained Things and considered as the best security approach in terms of timing and speed of networks.

The sudden explosion of IoT devices in supporting several applications have not considered the security of their communication processes. There are enormous data collections through these devices leading to possible breaches or leakages of privacy of users (Wu and Wang, 2018). There is need to protect communication of data between IoT nodes and the servers using lightweight cryptographic system and dynamic key. With the issues of computation complexity, scalability, and execution time, resource and power consumption, pseudo stream cipher is introduced to minimise overheads in data encryption and key synchronisation. According to (Wu and Wang, 2018), mutual authentication, session key and updates were performed with multiple encryption key size and update cycle schemes for communication effectiveness and security. Sensor systems and communication networks have grown more speedily.

Fog devices have capability to offer low latency, real-time and quality of service, and location information in IoT application settings at network edge. Data aggregation opens up issues of data privacy preservation especially for fog computing; reason being that it is nearly impossible existing approaches to aggregate data of hybrid IoT devices into one (such as sum or mean) regardless of the support for homogenous IoT devices' data. To overcome this problem, Lu *et al.* (2017) proposed a lightweight privacy-preserving data aggregation technique (or LPDA) for fog computing-enhanced Things. Also, Chinese Remainder Theorem, Homomorphic Paillier encryption, and one-way hash chain techniques for the purpose of data aggregation and early filter injected false data attacks are performed at network edge. The results revealed that differential privacy technique offered more security, which is lightweight for communication overheads and cost of derivations. However, the proposed model requires further work with different scenarios (that is, decentralised architectures) and attacks models to build effectively new solutions.

The importance of IoT in facilitating exchanges among constrained objects, low resources, regulating process computation and decision making within the networks were highlighted by Singh *et al.* (2017). Few challenges were identified with IoT such as memory capacity, cost of performance, smaller battery, security and large energy dissipation. Consequently, a survey of lightweight cryptographic algorithms found that IoT issues can be resolved through scalable key size, architecture, number of rounds, and block size. But, the levels of security offered by the encryption scheme were less secure, unsafe or moderate requiring further improvements especially for the target application of smart homes. In fact, these countermeasures cannot prevent security attacks on IoTs especially for emerging attacks in cyber-space. These concepts came about to address the scalability issues of IoT based system, which are particularly resource-constrained devices including short-lived memory, energy, and processing capability (Omrani *et al.*, 2018). Majority of these devices are connected to RFID tags, wireless sensor networks and larger IoT. The need to maintain confidentiality for these devices is desirable due to the fact that enormous of data were exchanged or transmitted across them. But, traditional cryptosystems (such as AES and DES) offered varying security solutions because the construct of ciphers are unsuited for resource-constrained devices (Kim and Kim, 2018).

One key problem facing society at present is the privacy and security of available data. There are issues surrounding collection, storage, integration and transformation of data to support the needs of diverse sectors and industry such as agri-food (Mushroom production) due to widespread deployment of evolving technologies. Apart from competitive advantage and increased produce, environment variables need to be regulated because of their direct relationship to production control system. One form of farming was understudied by (Branco *et al.*, 2019), which is extension mushroom farm distributed process control system sing IoT and Blockchain to facilitate distributed data collected on environment indicators to supplement production control system for mushroom farming. Again, there is improvement of farm management information system available to managers of farms. In the future research, precision farming should have comprehensive decision support system from subsystems with security in mind.

The evolving control system and technology ecosystem are short off in providing needed intelligence for rural farmers. Lack of precise information and communication negatively hampers farm production and management. To this end, (Hari Ram *et al*, 2015) suggested the use of IoT in place of conservative farming practice, which guides IoT based farming innovations. It became possible to raise farming processes, monitoring, welfare of farm and farmers, and unrestricted access to data on real-time basis. Consequently, there is greater leap towards food sustainability for developing countries by means of connected objects. The potential impact of IoT to advance farming sector in order to provide food for over 9.6 billion world population by 2050 was highlighted in the work by (Mat *et al*., 2019). It is on records that extreme weather and climatic conditions influence the quest for food. To enable farmers to cope with massive demands for produce, IoT based smart farming was proposed to enhance the productivity, and grow cleaner food to carter for exploding population. The complete architecture; processes and requirements for smart farming were envisage but, leaving out the

most important component, that is, privacy and security of data generated from IoT devices and transmitted across public vulnerable channels.

In another study in (Ahmed *et al*., 2018), the promise of fog computing and wireless networks to interconnect farm bases distributed in rural setup became feasible. To improve on the efficiency of this technique, a scalable network structure for controlling and monitoring farms in rural area was developed with a cross-layer based channel access and routing scheme. There are quite improvements in latency, sensing and actuating but, chances of tampering and manipulating data is probable.

3. Research Methodology

This paper proposes hybrid of two strongest cryptographic schemes (AES256 and SHA1-256) used commonly for resource constrained devices (Janakiraman *et al*., 2018; Halabi and Artail, 2019), which is known as SHAAES. The ECB and GCM encryption modes are widely ised to increase Hamming distance of ciphers. The hardening schemes of HE, Blowfish, and base64encode are used to fortify the resultant cryptographic algorithms. The performances of both encryption modes based encryption algorithms are measured using speed and memory complexities. This paper presents the optimal experimental setup for validating the proposed cryptographic scheme as shown in Table 1.

Table I. The Optimal experimental setups.

Parameter	Value
Hardware	
Processor	AMD E1-1200 APU, Radeon™ HD Graphics 1.40 GHz
RAM	4.00 GB
Hard Disk Drive (HDD)	282GB
System Type	64-bit Operating System, x64-based processor
Software	
Operating System	Windows 8 Single Language
Application IDE	Visual Studio Code 16
Cryptographic primitives	AES-256, base64code, Cipher Block Chaining (CBC), Galois/Counter Mode (GCM), SHA-1-256
Key exchange protocol	Diffie and Hellman algorithm

4. Results

The validation of the proposed hybrid encryption with hardening algorithm composed of high-performing cryptographic primitives of AES256 and SHA1-256 schemes. Two forms of hardening procedures were introduced (that is, CBC and GCM) whose outcomes are presented in Tables 2 and 3.

Table 2. The performance of the CBC hardening procedure.

Ciphertext	Ciphertext size (bit)	Secret key size (bit)	Encryption time (sec.)	Decryption time (sec.)
BfNFPRgfKF8Ke9kpoNAagmcI4/Hya5o/rq9/fq97ZiA=	44	29	1574	584
viRSYFTq1J0rRDLwfrXg3w==	24	29	2653	756
BR8oAxAeV/cmXWRoYUzxjA==	24	29	1356	598
iNKG9N05FtGF6AEeJnwLhw==	24	29	1540	585
GzIH1TZ2Ft+TAz3unfbnaw==	24	29	1452	632
JiLPe4nGJzOnBIKk/ghaDg==	24	29	1591	643
dBbbtVUsFsH3/Z9hzSoH3TBMV04rxouwFQOuaOYMS9o=	44	29	1658	578
Ciqj0SCaQh5Oh/KyLf8yBfb6jUXsL6COOrbI4w81wII=	44	29	1690	693
0x9i8GrAA82N49n4mBWetq9FjWacMPfkC6GdVsdAFyw=	44	29	1616	572
gv/yIop0HyLy7AzjnrCBGA==	24	29	1592	547

Table 3. The performance of the GCM hardening procedure.

Ciphertext	Ciphertext size (bit)	Secret key size (bit)	Encryption time (sec.)	Decryption time (sec.)
R52AMbobURxDY0vdrJf8PWZPBloPdrh8tMhfYqlHgvSj3GmaBy0JwulvBZJQxbFwVuBfdNzpL8VoNiGRjw==	84	29	20050	1034
C5MmzQCh6IVHeL/REudAUNE50Kiv0sJkBBJLk/69ixEhq631V5q0Q4Hk+rBEzW0U6A==	68	29	18101	872
OnPQrVmYo6OIRayWNgqlUP9X4mh5QrhMEdksQy6r28K1nerNp4f2a7kb+iBQidFF	64	29	18039	655
UroPDFvHGdJ5ks++00CAAy2CMWqz8AtJn7FXToseqfQN6g0JCG1JIJUxMphvooZr	64	29	17762	722
NhZ5NX6cCiseyNgFy8I1lObOPT5r9c8nique22emJw0rUQrAvgejAYWAz/iWEHtvLUJtPQ==	72	29	17684	686
y2GjqOwM8CSTEc6IUm9b/8lMDapcDM+aa+pEI42HDP0izVlAeA4wiWClEOgGKzbHxeehTOLLNQ==	76	29	17576	807
jnkhEIJOjcHSFe3pa/nb1v/d4OYDT3gbncmfg+QAjUVNubadXpk8PVvQn5lbgoJvn3IyvzjO6xAtZUYJyLnll2on	88	29	18015	909
hIgwdUVrlCFq/nEe5rB+bgm0EOyNNXtRWNMQhgbCz5nEKcAKVjgINkW/HhocH4RI6Aw+8HitwyxTicja33sfunjz95GJ8vjSRf8Y	100	29	17498	855
zHIZY+3YF89EBZ/TwWfNsrJhR99WnbCgOPEP1gPQ7zrpFRYhk/iMu	100	29	20119	805

ZeK3k7at3cfn4cZnuVJEdO8cYt2+dH9Ii4wyDiWBgs/K6Q=				
ttB3dXgWNU78dJ+ck+4dTSDIMOEzud+5SB+KgRoKXf/vLzQMhw4fQMt5gCdUNyRXwt3onw==	72	29	19009	720

The average performances of the CBC and GCM hardening processes of the SHAAES scheme proposed by this study to overcome the privacy of smart farming systems are shown in Figure 1.

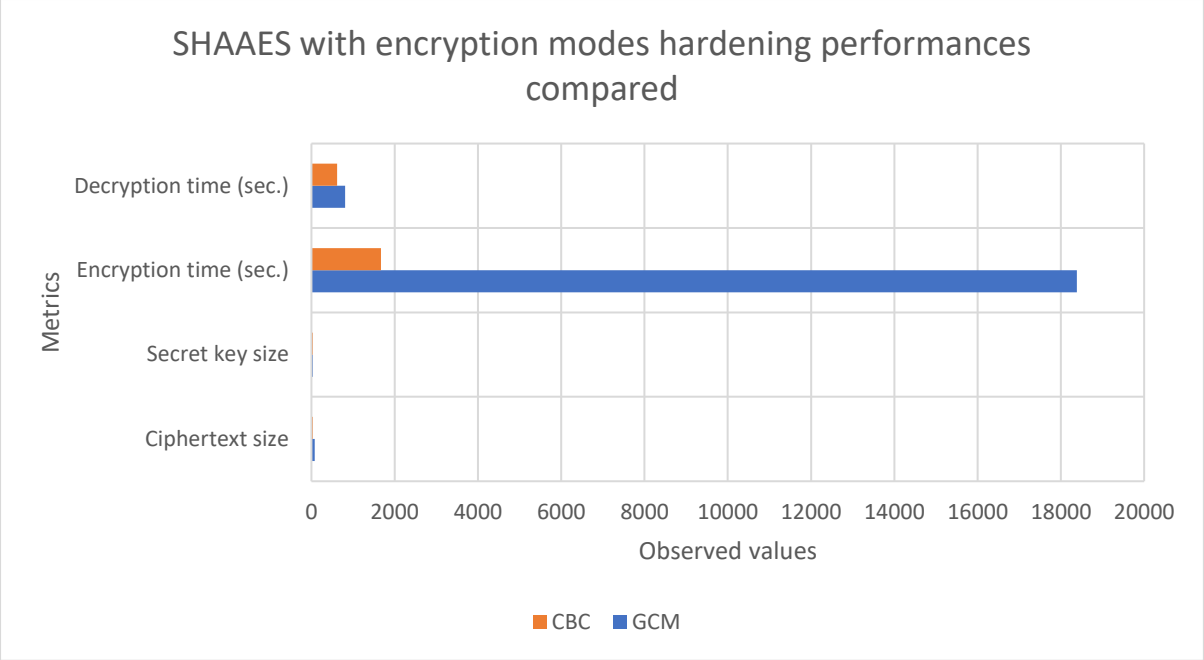

Figure 1. SHAAES with encryption modes performances compared.

From Figure 1, the CBC based SHAAES scheme was best in terms of speed of encryption (8.34%) and decryption (43.42%) as well as memory consumption for secret key sizes (50.00%) and ciphertext sizes (26.88%) when compared to GCM approach. The security provided by GCM was highest though, ineffective for protecting resources constrained devices used to power smart farming systems.

5, Conclusion and Recommendations

This paper underscored the numerous potentials of IoT and associated wireless Technologies in supporting smart farming processes around the world. Nevertheless, a number of factors have been identified as impacting on the effectiveness of these technologies including: low technical know-how, lack of required settings, insecurity of channels, energy consumption, scalability, efficiency, hardware constraints, low resource devices, large process requirements, and ineffective security solutions (such as encryption procedures). The topmost issue inhibiting against the IoT usage in farming is privacy, which is further their compounded hardware and software constraints.

The quest to make encryption solutions relevant for IoT based systems brings lightweight cryptography schemes to the interests of academics. Though, lightweight cryptography

schemes are weak and susceptible to attacks and breaches, encryption mode, hybrid encryption algorithms, and hardening procedures have the capability to increase the security status (such as complexity, diffusion state, and confusion state). The results obtained revealed the superiority of CBC based SHAAES scheme over GCM in terms of speed and memory complexities. In the future, more lightweight cryptosystems can be developed using the proposed approach to protect the privacy of smart farming.

References

Abou-nassar, E. M., Iliyasu, A. M., El-kafrawy, P. M., Bashir, A. L. I. K., & El-latif, A. A. A. B. D. (2020). DITrust Chain: Towards Blockchain-based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access*, *4*, 1–17.

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A Survey on Homomorphic Encryption Schemes. *ACM Computing Surveys*, *51*(4), 1–35.

Ahmed, N., De, D., & Hussain, I. (2018). Internet of Things (IoT) for Smart Precision Agriculture & Farming in Rural Areas. *IEEE Internet of Things Journal*, *5*(6), 4890–4899.

Ajao, L. A., Agajo, J., Adedokun, E. A., & Karngong, L. (2019). Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil & Gas Industry. *Multidisciplinary Scientific Journal*, *2*(3), 300–325.

Al-masri, E., Kalyanam, K. R. A. J., Batts, J., Kim, J., Singh, S., Vo, T., & Yan, C. (2020). Investigating Messaging Protocols for the Internet of Things (IoT). *IEEE Access*, *8*, 94880–94911.

Bala, J. A., Folorunso, T. A., Olaniyi, O. M., & Daniya, E. (2021). Design of an Agribusiness Innovative & Autonomous Robot System for Chemical Weed Control for Staple Food Crops Production in Sub-Saharan Africa. In Che, F. N., Strang, K. D., & Vajjhala, N. R. (Eds.), *The Advances in Business Information Systems and Analytics (ABISA)* (pp. 234–262). IGI Global.

Berrehili, F. Z., & Belmekki, A. (2017). Privacy Preservation in the Internet of Things. In *International Symposium on Ubiquitous Networking* (pp. 163–175). Springer, Singapore.

Boneh, D., Gennaro, R., Goldfeder, S., & Jain, A. (2018). In Shacham, H., & Boldyreva (eds.) *Advances in Cryptology – CRYPTO-2018: 38th Annual International Cryptology Conference, Proceedings, Part II* (Vol. 10992). Springer.

Branco, F., Moreira, F., Martins, J., Au-Yong-Oliveira, M., & Gonçalves, R. (2019). Conceptual Approach for an Extension to a Mushroom Farm Distributed Process Control System: IoT & Blockchain. In Á. Rocha et al. (Ed.), *WorldCIST'19 2019, AISC 930* (pp. 738–747).

Brandão, A., Mamede, H. S., & Gonçalves, R. (2018). Systematic review of the literature, research on blockchain technology as support to the trust model proposed applied to smart places. *Advances in Intelligent Systems and Computing*, *745*, 1163–1174.

Buchanan, W. J., Li, S., & Asif, R. (2018). Lightweight cryptography methods. *Journal of Cyber Security Technology, 1*(3-4), 187-201.

Campbell, R. E. (2019). Evaluation of Post-Quantum Distributed Ledger Cryptography. *The Journal of British Blockchain Association, 2*(1), 7679.

Gai, K., & Qiu, M. (2018). Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers. *IEEE Transactions on Industrial Informatics*, *14*(8), 3590–3598.

Giannoutakis, K. M., Spathoulas, G., Collen, A., Anagnostopoulos, M., Votis, K., & Nijdam, N. A. (2020). A Blockchain Solution for Enhancing Cybersecurity Defence of IoT. In *2020 IEEE International Conference on Blockchain* (pp. 490–495).

Halabi, J., & Artail, H. (2019). A Lightweight Synchronous Cryptographic Hash Chain Solution

to Securing the Vehicle CAN bus. In *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)* (pp. 1-6).

Hari Ram, V. V., Vishal, H., Dhanalakshmi, S., & Meenakshi Vidya, P. (2015). Regulation of water in the agriculture field using the Internet of Things. In *2015 IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR)* (pp. 112–115).

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain-based IoT systems: Integration issues, prospects, challenges, & future research directions. *Future Generation Computer Systems*, *97*, 512–529.

Hussain, S., Huang, J., Huang, J., Ahmad, S., Nanda, S., Anwar, S., Shakoor, A., Zhu, C., Zhu, L., Cao, X., Jin, Q., & Zhang, J. (2020). Rice production under climate change: Adaptations and mitigating strategies. In Fahad S. et al. (eds), *Environment, Climate, Plant and Vegetation Growth* (pp. 659-686). Springer, Cham.

Janakiraman, S., Sree, K. S., Manasa, V. L., Rajagopalan, S., Thenmozhi, K., & Amirtharajan, R. (2018). On the Diffusion of Lightweight Image Encryption in Embedded Hardware. In *2018 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.

Jayaraman, P. P., Yang, X., Yavari, A., Georgakopoulos, D., & Yi, X. (2017). Privacy-preserving the Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. *Future Generation Computer Systems*, *76*, 540–549.

Kim, Y. S., & Kim, G. (2018). A Performance Analysis of Lightweight Cryptography Algorithm for Data Privacy in IoT Devices. In *9th International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 936-938). IEEE.

Kuznetsov, O., Potii, O., Perepelitsyn, A., Ivanenko, D., & Poluyanenko, N. (2019). *Lightweight Stream Ciphers for Green IT Engineering*. In *Green IT Engineering: Social, Business and Industrial Applications* (pp. 113-137). Springer, Cham.

Lu, R., Heung, K., Lashkari, A. H., & Ghorbani, A. A. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access, 5,* 3302-3312.

Maohong, Z., Aihua, Y., & Hui, L. (2018). Research on security and privacy of big data under cloud computing environment. In *Proceedings of the 2nd International Conference on Big Data Research* (pp. 52–55).

Mat, I., Kassim, M. R. M., Harun, A. N., & Yusoff, I. M. (2019). Smart agriculture using the Internet of Things. *2018 IEEE Conference on Open Systems (ICOS)* (pp. 54–59).

Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Generation Computer Systems*, *102*, 1027–1037.

Nóbrega, L., Gonçalves, P., Pedreiras, P., & Pereira, J. (2019). An IoT-Based Solution for Intelligent Farming. *Sensors*, *19*, 1–24.

Omrani, T., Sliman, L., Becheikh, R., Belghith, S., & Hedia, B. Ben. (2018). Towards an ultra-lightweight cryptosystem for IoT. In *International Conference on Soft Computing and Pattern Recognition* (pp. 614-621). Springer, Cham.

Pagnin, E., Brunetta, C., & Picazo-Sanchez, P. (2018). HIKE: Walking the privacy trail. In *International Conference on Cryptology and Network Security* (pp. 43-66). Springer, Cham.

Papageorgiou, A., Loupos, K., Mygiakis, A., & Krousarlis, T. (2020). DPKI: A Blockchain-Based Decentralized Public Key Infrastructure System. In *IEEE 2020 Global Internet of Things Summit (GIoTS)* (pp. 1–5). IEEE.

Patel, N., Oza, P., & Agrawal, S. (2019). Homomorphic Cryptography and Its Applications in Various Domains. In *International Conference on Innovative Computing and Communications* (Vol. *55*, pp. 269–278).

Richards, D., Abdelgawad, A., & Yelamarthi, K. (2019). How Does Encryption Influence

Timing in IoT? In *2018 IEEE Global Conference on Internet of Things (GCIoT)* (pp. 1-5). IEEE.

Saiz-Rubio, V., & Rovira-Más, F. (2020). From smart farming towards agriculture 5.0: A review on crop data management. *Agronomy*, *10*(2), 1-21.

She, W., Liu, Q., Tian, Z., Chen, J.-S., Wang, B., & Liu, W. (2019). Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks. *IEEE Access Special Section on Mobile Service Computing with Internet of Things*, *7*, 38947–38956.

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing,* 1-18.

Surai, S., Kundu, R., Ghosh, R., & Bid, G. (2018). An IoT Based Smart Agriculture System with Soil Moisture Sensor. *Journal of Innovation and Research*, *1*(1), 39–42.

Wu, Y., & Wang, J. (2018). A Lightweight Cryptographic Scheme with Dynamic Key. *2018 10th International Conference on Communication Software and Networks (ICCSN)* (pp. 232-236). IEEE.