International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I8P219

Volume 70 Issue 8, 185-193, August 2022

Review Article

Cryptographic Algorithms for IoT Privacy: A Technical Review

Akinsanmi Joel Akinboboye[1], Ayodele Sunday Oluwole[2], Olaitan Akinsanmi[3], Abiodun Ernest Amoran[4]

[1,2,3,4]*Department of Electrical & Electronics Engineering, Federal University Oye Ekiti Nigeria*

Received: 13 June 2022 Revised: 30 July 2022 Accepted: 10 August 2022 Published: 22 August 2022

Abstract *- The Internet of Things (IoT) introduction into global ecosystems has enabled many passive objects to become sentient, making them more helpful in the ecosystem. As a result, these intelligent items make up the Internet of Things (IoT) network, and they can send massive amounts of data across the web. The network is often exposed to so many security challenges due to the interconnections of millions of intelligent objects across the area, particularly the privacy concerns on the network and the movement of users' data. The cryptographic algorithms were examined to address this highlighted privacy concern in the IoT network; this was done in terms of authentication, data integrity, and access control to data transmitted across the network. In this paper, the review of various types of Symmetric and Asymmetric algorithms and different research works on the cryptographic algorithm as per how it could be used to solve the IoT privacy issues were extensively carried out. The final part of the review work is the conclusion on the observations made is drawn to give directions to the future works required on the subject matter.*

Keywords *- Cryptographic algorithms, Internet of Things, Asymmetric cryptography, Symmetric cryptography, IoT privacy, Hill Cipher.*

1. Introduction

Internet of Things, also known as IoT, is a global network structure that will improve people's lives, company productivity, and government efficiency. Businesses can use this IoT network to exploit, analyze, and make decisions on the massive amount of data generated through the interconnections of numerous devices. The Internet of Things aspires to make a long-held ideal of changing everyday objects into intelligent devices capable of gathering, trading, and making decisions on their reality. Equipment is becoming more computerized and networked, building connectivities between machines, humans, and the Internet, allowing for better productivity, enhanced energy efficiency, and increased profitability.

Now the question is: how secure is the network as it grows, and how secure is the integrity of the massive data generated, given that everything will be connected to the Internet simultaneously? Security is no longer an option in the new technological invasion we are witnessing today. According to (Lama, 2020), in 2019, a list of data breaches and cyber-attacks occurred, reaching a 114.6million records leakage as of August 2019. This figure will keep increasing with more devices being connected every minute across the world. The increased size of the data exchanged within IoT networks has raised the necessity to find new security solutions that adapt to this enormous level of change.

With this in mind, it is observed that at this high growth rate across the globe, the Internet of things (IoT) is beginning to pose significant dangers to the network and user data. IoT device networks rely on software, services, and protocols to link devices to the outside network. As a result, many IoT vulnerabilities arise from insecure interfaces within and outside the network. The Internet, application APIs, mobile interfaces, and the cloud are connected to IoT devices, resulting in data breaches and compromises.

Cryptographic technology is one of the most dependable Privacy and security solutions used in IoT networks to address privacy and security concerns. Cryptography consists of two major components: an encryption/decryption technique and a key to prevent unauthorized data access. Various known cryptographic algorithms are currently available, as seen in subsequent sections. It is important to note that none of these Cryptographic algorithms can be referred to as one-size-fix-all for the problems of IoT privacy. Each of the algorithms has one advantage or the other over each other, depending on which solution the research focuses on; decisions are often taken to see how to improve any chosen algorithms that can be enhanced to resolve the focused issue.

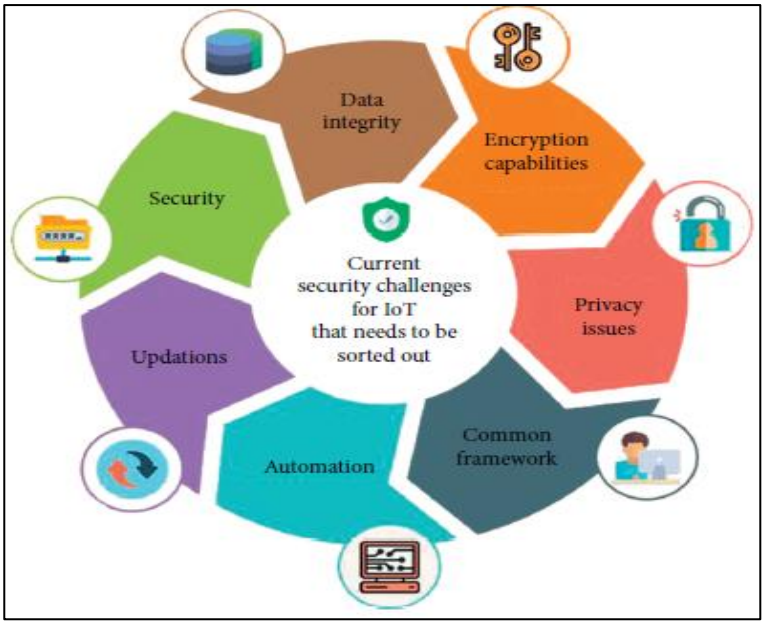

Fig. 1 Security challenges of IoT at a glance (Source: Khadam *et al.*, 2020)

2. Review of Encryption Methods

This section looks at the various cryptographic research activities in IoT privacy solutions. This section examines the concept of cryptography, its terminologies, and the many research studies conducted. The reviews will be used to make observations and suggestions to find an Algorithm that can be mathematically changed to boost processing speed, which is the purpose of the research.

2.1. Cryptography

One of the most effective ways to ensure network security is through cryptography. It protects important data and files from unauthorized access. The science of encrypting data and the development and study of mathematical algorithms enable secure communication in the face of millions of attackers. Cryptography's basic function is the capacity to send information between participants in a way that prevents others from reading it. Cryptography's four main goals are confidentiality, data integrity, entity authentication, and data origin authentication. Both an algorithm and a secret value are used in cryptographic systems. The key is the value that is kept secret. Including a key to an algorithm is necessary since it is difficult to develop new algorithms continually, and it will allow for reversible information scrambling. Cryptographic techniques are divided into two major categories viz: Symmetric and Asymmetric.

2.1.1. Symmetric Cryptography

The encryption and decryption operations of symmetric cryptography employ the same key. Another name for it is secret-key cryptography. This type of cryptography is more user-friendly and faster. The key is also securely exchanged between the two parties. Symmetric cryptography, on the other hand, has a serious problem: if the key is disclosed to an intruder, the message can be easily manipulated, which is a risk factor.

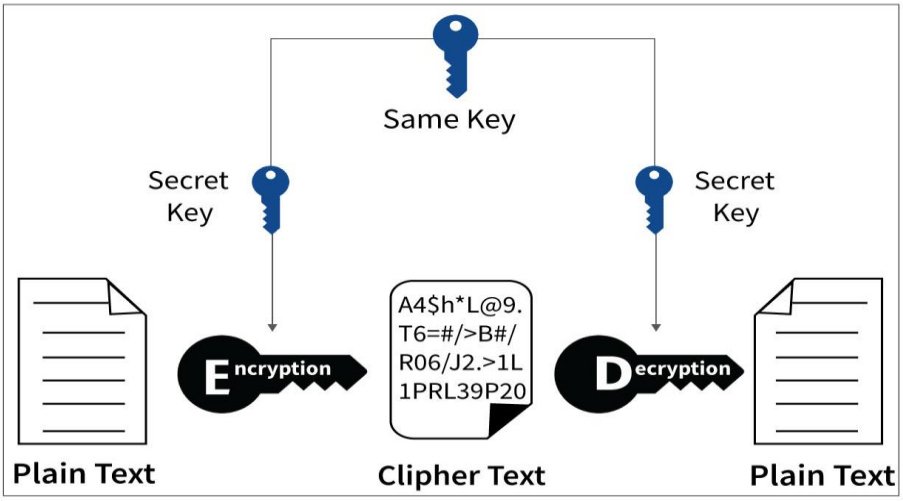

Fig. 2 Symmetric cryptography diagram

2.1.2. Asymmetric Cryptography

Asymmetric cryptography, often known as public-key cryptography, uses a pair of linked keys - one public key and one private key - to encrypt and decrypt a message and protect it from unauthorized access or use. The public key is used for encryption, whereas the private key is used for decryption (sometimes known as the secret key). Because of the key length, this method of cryptography has a disadvantage in terms of encryption speed. In addition, if not properly handled, key management might be a problem

.

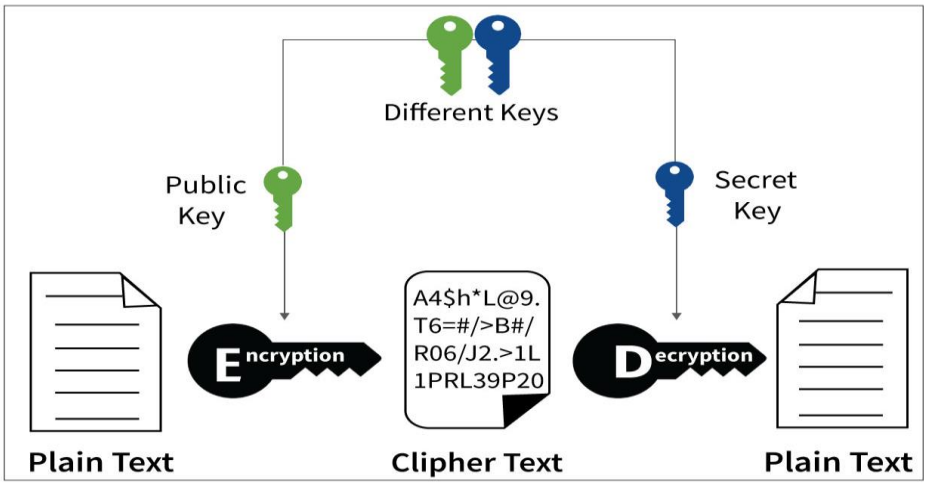

Fig. 3 Asymmetric cryptography diagram

Keys

A key is a value used with a cryptographic algorithm to generate a unique ciphertext.

The encryption key is used for encryption, and the decryption key is used for decryption. The bigger the key size (measured in bits), the more secure the communication. There are two methods to utilize a key: privately or publicly. In the previous Symmetric Encryption session, the key was utilized as a private or single key for encryption and decryption. As explained in the last session, the key is utilized as a private or public key for encryption and decryption in asymmetric encryption.

Encryption

Encryption is a method of changing data (known as plaintext) into an unreadable format (Called ciphertext). The rewritten message is notably different from the original. A hacker cannot access the data because the sender encrypts it. To encrypt data, key algorithms are often utilized. To prevent data from being stolen, it is encrypted. On the other hand, many well-known corporations encrypt data to keep their trade secrets hidden from competitors.

With a symmetric algorithm, encryption and decryption are denoted by:

Ek(M) = C

Dk (C) =M

The two types of symmetric algorithms are as follows. Stream algorithms or stream ciphers are algorithms that act on plaintext one bit (or sometimes byte) at a time. Others work in groups of bits on the plaintext. The methods are called block algorithms or block ciphers, and the groups of bits are called blocks. The typical block size for current computer algorithms is 64 bits, which is large enough to prevent analysis but small enough to be practical. (Algorithms used to work on plaintext one character at a time before computers.) It is similar to a streaming algorithm that operates on a stream of characters).

Decryption

Decryption is the inverse of encryption. It converts encoded/encrypted data (ciphertext) into a form (plaintext) that can be read and understood by a human or a computer. This method entails decrypting the text by hand or using the same keys to encrypt the original data.

Encryption using public key K is denoted by:

$E_k(M) = C$

Even though the public key and private key are different, decryption with the corresponding private key is denoted by: $D_k (C) = M$

Plaintext

This is the data that humans and machines can read directly. Plaintext is a term that dates back before computers when hardcopy text was the only type of text that was encrypted. It's now associated with various media, including music, movies, and computer programs.

Ciphertext

An original communication (plaintext) is transformed into ciphertext by encryption methods or ciphers. The cipher would be required to decrypt the data so that it could be read and understood by humans.

Cipher

The mathematics (or algorithm) responsible for converting plaintext to ciphertext and ciphertext back to plaintext is known as ciphertext. It's sometimes used

interchangeably with the word 'code,' albeit the two terms don't always signify the same thing. When it's broken down into blocks, it's called a block cipher. A block cipher turns a block of plaintext bits into a block of identical ciphertext bits. The block size is predetermined in the proposed architecture. The strength of the encryption algorithm is unaffected by the block size chosen. The length of the key determines the cipher's strength.

The block cipher is depicted in figure 2.9.

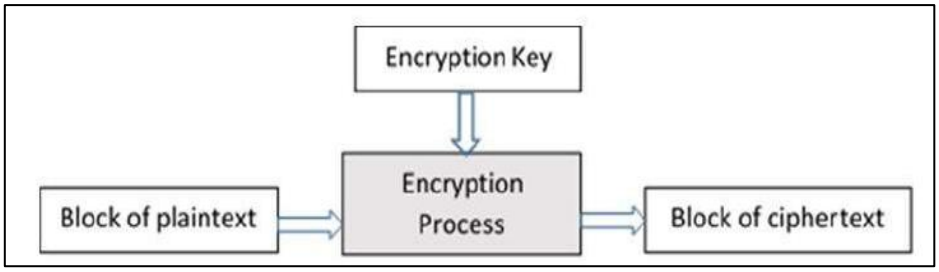

Fig. 4 Basic scheme of a block cipher

3. Encryption Algorithms

There are a host of different encryption algorithms available today. Some of them are briefly discussed in this section.

3.1. Data Encryption Standard (Des)

The Data Encryption Standard (DES) algorithm was developed by an IBM team in the early 1970s and adopted by the National Institute of Standards and Technology (NIST). After breaking plain text into 64-bit blocks, the technique uses 48-bit keys to convert it to ciphertext. It is the world's oldest and most widely used modern encryption method. The data is encrypted and decrypted using the same key because it's a symmetric-key approach. The encryption and decryption keys would be different if it were an asymmetrical algorithm.

3.2. Triple Data Encryption Standard

The symmetric key-block cipher Triple Data Encryption Standard (DES) employs three copies of the DES cipher. The key size is increased in Triple DES to provide extra protection through encryption capabilities. Each block contains 64 bits of data. Bundle keys are made up of three keys that are each 56 bits long. There are three keying choices in data encryption standards:

- Every key is self-contained.
- Keys 1 and 2 are two distinct keys.
- The three keys are identical.

The final option is Triple DES. Even though the triple DES key is 168 bits long, the key security is just 112 bits. It's important to remember that Triple DES is the successor of the Data Encryption Standard (DES) algorithm, which was created in reaction to DES's flaw. It used to be the most widely used symmetric algorithm in the business, but it's now being phased out. It's commonly used to encrypt UNIX passwords and ATM PINs.

3.3. Advanced Encryption Standard (Aes)

The Advanced Encryption Standard (AES) is a widely used encryption method by the US government and other organizations. Despite being highly effective in the 128-bit version, AES uses 192- and 256-bit keys for demanding encryption applications. AES is usually regarded to be resistant to any attacks save brute force. Regardless, many internet security experts believe that in the not-too-distant future, AES will become the de facto standard for encrypting data in the private sector.

3.4. Rivest-Shamir-Adleman (Rsa)

Rivest-Shamir-Adleman (RSA) encryption is a widely used asymmetric encryption algorithm across many products and services. Asymmetric encryption uses a mathematically related key pair to encrypt and decrypt data. The key pair is created using a private and public key, with the public key accessible to anybody and the private key being a secret known only to the key pair creator. Data can be encrypted with the private or public key and then decrypted with the other key in RSA. One of the reasons why RSA is the most widely used asymmetric encryption method is because of this.

RSA has several flaws that attackers could exploit, despite its viability in many scenarios. One of these concerns is the encryption procedure's usage of a long key. While certain algorithms, like AES, are impossible to break, RSA relies on its key size to be difficult to crack. The more secure an RSA key is, the longer it is. Researchers utilized prime factorization to crack a 768-bit key RSA method, but it took two years, thousands of man hours, and a massive amount of computing power; thus, current RSA key lengths are still safe.

3.5. Blowfish

Bruce Schneier created Blowfish, a variable-length key block cipher. It does not meet all of the abovementioned standards for a new cryptographic standard: It's only appropriate for applications where the key isn't changed frequently, such as a communications link or an automatic file encryptor. When implemented on 32-bit microprocessors with substantial data caches, such as the Pentium and the Power PC, it is significantly quicker than DES.

3.6. Twofish

Bruce Schneier also created the Twofish encryption algorithm. With 256-bit keys and 128-bit block size, it's a symmetric key block cipher. It's related to AES (Advanced Encryption Standard) and Blowfish, an older block cipher. Twofish came close to becoming the industry standard for encryption, but AES ultimately prevailed. It has a few traits that distinguish it from most cryptographic protocols. For starts, it employs pre-computed, key-dependent S-boxes. An essential component of every symmetric key replacement scheme is an S-box (substitution-box). In Twofish's block cipher, the S-box is employed to conceal the relationship between the key and the ciphertext. Twofish uses a key-dependent, pre-computed S-box, which implies the S-box has previously been computed but is decrypted with the cipher key.

3.7. Hill Cipher

The Hill cipher is a polygraphic substitution cipher based on Linear Algebra principles. Lester S. Hill, a well-known American mathematician, devised and improved it in 1929. Hill Cipher is Digraphic. However, it may be expanded to multiply any letter size, adding greater complexity and reliability for better application.

The Hill cipher is a more mathematical cipher than others since it uses modulo arithmetic, matrix multiplication, and matrix inverses. Because the Hill cipher is also a block cipher, it can theoretically function with blocks of any size. In later sessions, more emphasis will be placed on this.

4. Review of Previous Works

This section looks at some cryptographic algorithm research works in privacy solutions for the Internet of Things. The reviews will make observations and comments about which algorithms should be improved to increase processing performance.

Nicolas Sklavos *et al*. (2016) worked on the paper titled "Cryptography and security in Internet of Things (IoT): Models, Schemes and implementation." They concluded that a thorough examination is required to ensure they can be applied in the IoT resources described because cryptographic models and security techniques are not well defined. They further advised that more work should be done on the Algorithms. There was no mention of the Algorithms used or why they were used. In their work, Samah Osama M. Kamel and Nadia H. Hegazi (2018) submitted that power and time are two key requirements of a cryptographic security system. It has been noted as a significant negative in cryptographic technology. The researchers found the cryptographic technology's flaws in this study. Still, no further work on how to remedy the issue has been done, even though the technology is critical for ensuring the privacy of the IoT network.

Mohammed El-hajj et al. (2018) concluded that the real problem of a cryptographic system does not cost; rather, it is the total protocol completion time, and this process consumes a lot of energy. They suggested another method for power consumption in IoT devices, but The observed protocol completion time problem was not addressed, and no solution was presented.

According to their findings, cryptographic approaches cost a large amount of power for resource-constrained IoT devices. They suggested an alternative encryption algorithms' power consumption when utilized on an IoT device must be investigated. At the end of the analysis, they discovered that the problem is not computationally cryptographic costs but rather the total protocol completion time, which includes energy consumption. The observed protocol completion time problem was not addressed, and no solution was presented.

Mary Shamala *et al.* (2021), in their work on "Lightweight Cryptography Algorithms for Internet of Things-enabled Networks: An overview," examined the performance of existing lightweight algorithms and touched on some of the research challenges that future IoT research should address. These researchers stated that more investigation into the algorithm's performance is required.

Pereira *et al.* (2017) worked on "Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems." The researchers looked at symmetric cryptographic primitives that performed various security roles in operating systems and IoT and WSN-based platforms. They noted that some previous research in the literature focused on "very primitive implementations" on a single platform or operating system. The research fails to analyze the cryptographic methods with the fastest protocol completion time.

Al salami *et al.* (2016) based their work on encryption methods for smart homes that maintained owners' privacy. Although the research suggested low-cost, high-efficiency encryption methods, they could not identify an efficient time-consuming algorithm.

Worthman (2015), in his article titled "Lightweight Cryptography for The IoE," concluded that combining lightweight primitives with cutting-edge technology would overcome IoT constraints such as size, speed, simplicity, code size, execution time, and memory metrics. Constraints were identified in this paper, but their findings were not described explicitly.

Biryukoy *et al.* (2017) addressed the necessity to review the specialized algorithms for ultra-lightweight cryptography and IoT cryptography after a full review of lightweight cryptologic primitives and a list of the pros and downsides of IoT. An Article by Computer society (2015) on the Internet of Things noted that developing effective and acceptable solutions to IoT security challenges that are well relevant to the volume and complexity of the concerns may necessitate a collaborative approach to security.

Abomhara and Geir (2014), in their work, posited that privacy and security are critical facilitators of technologies and, as a result, are among the most pressing IoT network concerns. The shortcoming is that there were no solutions to the highlighted obstacles to IoT systems.

Gope *et al.* (2013), in their paper, said implicit cryptography technique for secure routing was proposed as a replacement block cipher cryptological radial key rule. It merged a freelance method with a computationally safe mathematical model. A key distribution mechanism was utilized on a secure policy-based routing system. It was solely for document conversion.

In their work, Anand et al (2013) mentioned that identity-based cryptography approaches and applications were investigated. They looked at how identity-based cryptography is used in a variety of networks. The subject is also used in mobile and other wireless networks. They also discussed the circumstances in which identity-based total cryptography was used and the benefits and downsides of this method. The most notable constraint of this research was that the available techniques were limited to a single block, a fault line through which crackers can strike.

Verma *et al.* (2012) believe that a companion excellent value radial key cryptography rule was proposed for information security. Compared to specific radial key methods, this block cryptography rule is much faster and provides more advanced protective functions. In terms of achieving confidentiality, it operates similarly to message authentication. It outperforms other cryptography methods regarding overall performance and time consumption; packet length may alter on any given occasion. It became equally as clever whenever there was a shift in information, such as a picture, music, or video, rather than text. Using dynamic key length, it was also discovered that a longer key length causes changes in time and battery (energy) usage.

Wang *et al.* (2010) investigated one or multicore advanced cryptography conventional architectures for adaptable security. They developed a sophisticated cryptography common processor as a major building block for customary cryptography. Each processor delivers block cipher schemes with a new key growth style for the first advanced cryptography rule. The memory controller of every powerful cryptographic typical processor was designed for maximum overlapping between information transit and the host CPU in a multicore design. This concept used high-speed systems and information technologies to reduce the input-output and information measurement disadvantages. However, the major disadvantage of the work is that every conventional CPU require a separate memory controller.

Hossein Shafagh (2013), in his thesis on "Leveraging Public-key primarily based Authentication for the Internet of Things," concluded that according to the findings, cryptographic primitives are preferred for meeting security goals for exchanged messages and within devices. There is no mention of which algorithms will be examined in this section.

Sharma and Jiwala (2011) worked on Identity Based Secure Key Generation Protocol as one of the projects. They obtained the personal key for consumers in this study through a distributed manner, and this theme implies a substantial amount of communication overhead. The proposed theme reduces the number of authorities required to compute the generic public and private key pair. A key written agreement was the weakness of ID-based cryptography.

Ajay Kumar (2014) worked on cryptography rule optimization for Secured Communication; the work claimed that the misuse of the Hill Cipher rule's performance is acceptable in various reasonable applications. The workers claim that a rule with higher security and shorter time intervals were required for cryptography optimization. Therefore, a new cryptography optimization rule was proposed and compared with other existing rules. The proposed algorithm's output was greater than that of other encryption algorithms. If several keys are frequently utilized, many systems can be streamlined. The work suggested that future work be devoted to reducing the complexity of the proposed rule so that it could be implemented more quickly.

Reetu *et al.* (2016) projected that performance would be adequate in a wide range of applications in their research paper "An Efficient Approach for Secure Data Hiding Using Cryptography Using the Hill Cipher." When comparing the proposed algorithm to existing encryption approaches, it was determined that the proposed method had a greater throughput. They recommended that more studies be done in the future to lower the complexity of the proposed algorithm, which would invariably improve processing speed.

4.1. Research Gaps

Based on the prior literature reviews, the essence of this study project can be stated as follows:

- According to the author, using cryptographic models and security procedures is not well known (Sklavos et al, 2016); a thorough analysis is required to verify which could be utilized in the available IoT resources.
- According to Authors (Samah *et al.,* 2018), the major shortcoming of cryptographic technology is that cryptographic security systems require more power and processing time.
- Several academics suggested that future studies focus on improving cryptographic algorithms to provide a faster processing time for the encryption and decryption of data travelling across IoT networks, hence ensuring the Privacy of IoT networks.

5. Conclusion

For the ever-expanding IoT network, cryptography is a reliable security solution; thus, it's critical to keep an eye on how the security solution algorithm evolves. This topic prompted a review of numerous research papers on cryptography's significant power and processing time weaknesses. This work aims to review the various positions on this subject matter to explore how Encryption technologies may be modified to increase processing speed, which will go a long way toward ensuring the privacy of the IoT network. It is important to note that this is a ceaseless process; as the IoT Network expands, more efforts shall be required to improve the processing speed.

References

[1] Abomhara M. and M. K. Geir, "Security and Privacy in the Internet of Things: Current Status and Open Issues," *IEEE Int. conf. on Privacy and Security in Mobile Systems (PRISMS)*, pp. 1–10, 2014.

[2] Addo, *et al*., "A Reference Architecture for Improving Security and Privacy in Internet of Things Application," *International Conference on Mobile Services, IEEE,* Alaska, 2014.

[3] Aggarwal, C. C., Ashish, N., & Sheth A, "*The Internet of Things: A Survey from the Data-Centric Perspective*," In C. C. Aggarwal (Ed.), Managing and Mining Sensor Data, US: Springer, pp. 384–428, 2013..

[4] Ajay Kumar, "*Optimization of Encryption Algorithm for Secured Communication*," A MEng Degree Thesis Report Submitted to Dept of Electrical and Communication Engineering at Thapar university, Patiala, 2014.

[5] Akinsanmi O, "Internet Facilities on Global System for Mobile Communication (GSM) Device," *J. of Sust. Dev.*, pp. 1-12, 2017.

[6] Alaba, F.A., Othman, M., Hashem, I.A.T. and Alotaibi F, "Internet of Things security: A Survey," *J. of Net. and Comp. Appl.*, 88, pp. 9-29, 2017.

[7] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of Things: A survey on Enabling Technologies, Protocols, and Applications," *IEEE Comm. Surv. & tut.*, vol. 17, no 4, pp. 2346-2378, 2015.

[8] Al-Salami, S., Baek, J., Salah, K. and Damiani E, "Lightweight Encryption for a Smart Home," In 11th IEEE *Int. Conf. on Availability, Reliability, and Security (ARES)*, pp. 380-389, 2016.

[9] Anand D., V. Khemchandani and R. K. Sharma. (). "Identity Based Cryptography Techniques and Applications", International Conference on Computational Intelligence and Communication Networks, vol. 1, pp. 342-349, 2013.

[10] NehaPriya, "Cybersecurity Considerations for Industrial IoT in Critical Infrastructure Sector," *International Journal of Computer and Organization Trends*, vol. 12, no. 1, pp. 27-36, 2022. *Crossref*, https://doi.org/10.14445/22492593/IJCOT-V12I1P306

[11] AncaJurcut, *et al*., "Security Considerations for Internet of Things: A Survey," 2020.

[12] AnnapoornaShetty, *et al*., "A Review on Asymmetric Cryptography - RSA and El Gamal Algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, 2014.

[13] Aoiki, K. *et al*., Camellia, "A 128-bit Block Cipher Suitable for Multiple Platforms—Design and Analysis," In *International Workshop On Selected Areas In Cryptography, Springer*, pp. 39–56, 2000.

[14] Ashton, K *et al*., "That Internet of Things' Thing," RFID Journal, vol. 22, no. 7, pp. 97–114, 2009.

[15] Babar S., *et al*., "Proposed Embedded Security Framework for Internet of Things (IoT)," *2nd Int. IEEE Conf. In Wire. Comm., Vehic. Techn., Info. Theory and Aero. & Electron. Sys. Tech. Wireless VITAE*, pp. 1-5, 2011.

[16] Biryukov A. and L. P. Perrin, "State of the Art in Lightweight Symmetric Cryptography," Bonetto R., N. Bui, V. Lakkundi, 2017.

[17] A. Olivereau, A. Serbanati, M. Rossi, "Secure Communication for Smart Iot Objects: Protocol Stacks, Use Cases, And Practical Examples," *In IEEE Int. Symp. on a World of Wire., Mob. and Mult. Net.* (WoWMoM'12), San Francisco, CA, pp. 1-9, 2012.

[18] Chahar R. K., G. Datta and N. Rajpal, "Design of a New Security Protocol," *IEEE International Conference on Computational Intelligence and Multimedia Applications*, vol. 4, pp. 131-134, 2007.

[19] Chen L, *et al*., "*Report on Post-Quantum Cryptography*," US Department of Commerce, National Institute of Standards and Technology, 2016.

[20] Cracking, D, "*Secrets of Encryption Research*," Wiretap Politics, and Chip Design, Electronic Frontier Foundation, 1998.

[21] CzeslawKoscielny, "A new approach to the Elgamal Encryption Scheme, Academy of Management of Legnica, Faculty of Computer Science, ul. Reymonta 21, 59–220 Legnica, Poland," *Int. J. Appl. Math. Comput. Sci*, vol. 14(2): 265-268, 2004.

[22] Daemen, J, "*Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis*," PhD thesis, Doctoral Dissertation, KU Leuven. 1995

[23] S.Vishnupriya, "Edge Computing Based IoT for Smart Cities," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 1, pp. 16-21, 2020. *Crossref*, https://doi.org/10.14445/23488387/IJCSE-V7I1P104

[24] Daubert J., *et al*., "A View on Privacy & Trust in IoT," *In IEEE Int. Conf. on Comm.*, ICC , London, GB, 2015.

[25] DiaaSalama, *et al*., "Performance Evaluation of Symmetric Encryption Algorithms", *International Journal of Computer Science and Network Security*, vol. 8, no.12, 2008.

[26] DiaaSalama, *et al*., "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", *International Journal of Network Security*, pp.77-88, 2010.

[27] Dominikus, S. Medassist, "A Privacy Preserving Application using Rfid Tags," *International Conference on RFID-Technologies and Applications (RFID-TA), IEEE*, Spain, 2011.

[28] Elgamal, T, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, vol. 31, pp. 468–473, 1985.
[29] El-hajj M. *et al*., "Analysis of Cryptographic Algorithms on IoT Hardware platforms," *Int. Conf. on Cyber Security in Networking*, CSNet, 2018.
[30] Eschenauer L and V. D. Gligor, "A Key Management Scheme for Distributed Sensor Networks", *ACM conference on Computer Security*, vol. 2, pp. 41-47, 2002.
[31] Ferguson, *et al*., "Cryptography Engineering," *Design Princi*, 2010
[32] Fink, G. A, *et al*., "Security and Privacy Grand Challenges for the Internet of Things," *International Conference on Collaboration Technologies and Systems (CTS)*, Georgia, 2015.
[33] Funke S., *et al*., "End-2-End Privacy Architecture for IoT," *Int. IEEE Conf. on Comm. and Network Security CNS*, San Fransisco, 2015.
[34] Gama K., L. Touseau, and D. Donsez, "Combining Heterogeneous Service Technologies for Building an Internet of Things Middleware," *Comp. Comm.*, vol. 35, no. 4, pp. 404-418, 2012.
[35] Gope P., A. Singh, A Sharma and N. Pahwa, "An Efficient Cryptographic Approach for Secure Policy Based Routing", *IEEE Journal on Selected Areas in Communications*, vol. 1, pp. 357-364, 2013.
[36] Gusmeroli S., S. Piccione, and D. Rotondi, "A Capability-Based Security Approach to Manage Access Control in the Internet of Things," *Math. and Comp. Model*, vol. 58, no. 5, 2013.
[37] Preetha S, Sagar J, Krishna Pooja P, "Security Issues Faced by Internet of Things: A Survey," *International Journal of Recent Engineering Science*, vol. 7, no. 3, pp. 1-6, 2020.
[38] Halkidis S. T., N. Tsantalis and A. Chatzigeorgiou, "Architectural Risk Analysis of Software Systems Based on Security Patterns", *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 3, pp. 129-142, 2008.
[39] Hatzivasilis, G. *et al*., "C. A review of Lightweight Block Ciphers," *Journal of Cryptographic Engineering*, vol. 8, no. 2, pp. 141–184, 2018.
[40] He W., Y. Huang, K. Nahrsted and W. C. Lee, "A Self-contained Public Key Management Scheme for Mission Critical Wireless Ad Hoc Networks", *IEEE International Conference on Pervasive Computing and Communications*, vol. 1, pp. 1-11, 2007.
[41] HimaniAgrawal and Monisha Sharma, "Implementation and Analysis of Various Symmetric Cryptosystems", *Indian Journal of Science and Technology*, vol. 3, no. 12, 2010.
[42] HosseinShafagh, "*Leveraging Public-key based Authentication for the Internet of Things*," A Master Thesis of RWTH Aachen University, Germany, 2013.
[43] [Online]. Available: *https://acv-vc.medium.com/internet-of-things-connecting-the-future-7b0f260c0fce*
[44] [Online]. Available: https://en.wikipedia.org/wiki/Hill_cipher
[45] A Publication of Insider Intelligence, 2020. [Online]. Available: https://www.businessinsider.com/iot-security-privacy?r=US&IR=T.
[46] [Online]. Available: https://www.cnbc.com/2015/06/03/tim-cook-takes-the-offensive-on-privacy-report.html.
[47] [Online]. Available: https://www.coolnsmart.com/quote-if-you-reveal-your-secrets-to-the-23592/
[48] [Online]. Available: https://www.techopedia.com
[49] [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and security/iot/magazine/internet-threats
[50] [Online]. Available: https://www.whatshouldireadnext.com/quotes/marlon-brando-privacy-is-not-something-that
[51] Ismail I.A, Mohammed A. and D. Hossam, "How to repair the Hill cipher", *Journal of Zhejiang University Science*, vol. 1, pp. 2020-2030, 2006.
[52] Islam M. N, Mia M. M. H, Chowdhury M. F. I. and Matin M.A, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology," *International Conference on Software Engineering, Artificial Intelligence Networking and Parallel Distributed Computing*, vol. 1, pp. 290-294, 2008.
[53] Jamil T, "The Rijndael Algorithm", *IEEE Potential*, vol. 1, pp. 1-4, 2004.
[54] Johansson, T, *et al*., "Advances in Cryptology–EUROCRYPT," *32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Athens, Greece, Proceedings, Springer, vol. 7881, 2013.
[55] Jung. W. Lo, M. S. Hwang and C. H. Liu, "An Efficient Key Assignment Scheme for Access Control in a Large Leaf Class Hierarchy," *Journal of Information Sciences Elsevier Science*, vol. 4, pp. 915-925, 2003.
[56] Junqing Zhang, Alan Marshall, Roger Woods, Trung Q. Duong, "Design of an OFDM Physical Layer Encryption Scheme," *IEEE Trans. on Veh. Tech.* vol. 66, no. 3, 2017.
[57] Karandikar Y., X. Zou and Y. Dai, "An Effective Key Management Approach to Differential Access Control in Dynamic Environments," *Journal of Computer Science*, vol. 1, pp. 540-551, 2006.
[58] Kim H.W. and S. Lee, "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System", *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 214-224, 2004.
[59] Kliarsky A, "*Detecting Attacks Against the Internet of Things*," SANS Institute InfoSec Reading Room, 2017.
[60] Koblitz N., "Elliptic Curve Cryptosystems," *Journal of Mathematics of Computation*, Published by American Mathematical Society, vol. 48, no.177, pp. 200-209, 1987.

[61] Krawczyk H., *et al*., "The Order of Encryption and Authentication for Protecting Communications," 2001, [Online]. Available: http://eprint.iacr.org/2001**.**

[62] Okah C., Matthias D., Nwiabu N., "A Real-Time Encryption Algorithm For User Data Preservation In Mobile Computing," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 3, pp. 1-11, 2020. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V7I3P101

[63] Lai,C.,H. CPAL, "A conditional Privacy-Preserving Authentication with Access Linkability for Roaming Service," *Internet of Things Journal, IEEE*, vol. 1, no. 1, pp. 45–57, 2014.

[64] Lama SLEEM, "*Design and Implementation of Lightweight and Secure Cryptographic Algorithms for Embedded Devices,"* A PhD Thesis Presented to Université Bourgogne Franche-Comté, 2020.

[65] Li J. H., B. Bhattacharjee, M. Yu and Levy, "A Scalable Key Management and Clustering Scheme for Wireless Adhoc and Sensor Networks", *Journal of Future Generation Computer systems, Elsevier Science publishers*, vol. 24, pp. 859-869, 2008.

[66] LidaXu, Wu He, Shancang Li, "Internet of Things in Industries: A Survey," *IEEE Trans.on Industrial Informatics*, 2014.

[67] Lipmaa H., P. *et al*., "CTR-Mode Encryption," *First NIST Workshop on Modes of Operation, Citeseer,* 2000.

[68] MebratuFanaBedasa, *et al*., "Data Encryption and Decryption by Using Hill Cipher Algorithm," *Control Theory and Informatics*, vol. 10, 2020.

[69] Miorandi D., S. Sicari, and F. D. Pellegrini, I. Chlamtac, "Internet of Things: Vision, Applications and Research Challenges," *Ad Hoc Networks*, vol. 10, no. 7, 2012.

[70] Mohamed N, *et al*., "Symmetric Encryption Using Pre-Shared Public Parameters for a Secure TFTP Protocol," *Journal of Engineering Science and Technology*, vol. 12, no. 1, 98–112, 2017.

[71] Morchon, O.G., *et al*., "A Comprehensive and Lightweight Security Architecture to Secure the Iot Throughout the Lifecycle of a Device Based on HIMMO," In: *Algorithms for Sensor Systems, Lecture Notes in Computer Science*, vol. 9536, pp. 111–129, 2016.

[72] NouraAleisa and Karen Renaud, "Privacy of the Internet of Things: A Systematic Literature Review," *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[73] Oluwole A. S. and V. M. Srivastava, "Modelling of RF Security System Using Smart Antennas," *IEEE Int. Conf. on Cyberspace Governance,* Cyber-Abuja, pp. 1-7, 2015.

[74] Oluwole A. S., *et al*., "Design of Automatic Gate Control using Infrared Remote with Password Protected," *Int. J. for Res. & Dev. in Tech*, vol. 2, no. 5, pp. 2349-3585, 2014.

[75] Samah M. O., C. Kamel, H. H. Nadia, "A Proposed Model of IoT Security Management System Based on A study of Internet of Things (IoT) Security," *Int. J. of Sci. & Eng. Res.* Vol. 9, no. 9, pp. 229-5518, 2018.

[76] Schaffers H, "Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation, in the Future Internet," *Lecture Notes in Computer Science,* Springer, Berlin/ Heidelberg, vol. 6656, pp. 430–446, 2011.

[77] Schneier, B, "*Applied Cryptography: Protocols, Algorithms, and Source Code*," In C. John Wiley& Sons, 2007.

[78] Maryann Thomas, S. V. Athawale, "Study of Cloud Computing Security Methods: Cryptography," *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 4, pp. 1-5, 2019. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V6I4P101

[79] ShahidRaza, *et al*., "Lithe: Lightweight Secure CoAP for the Internet of Things," *An IEEE Sensors Journal,* vol. 13, no. 9, 2013.

[80] Sharma D. and D. Jinwala, "Identity Based Secure Key Generation Protocol", *International Conference on Computer & Communication Technology,* vol. 9, pp. 415-402, 2011.

[81] Sicari S., A. Rizzardi, L.A. Grieco, A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Comp. Network.,* vol. 76, pp. 145-165, 2015.

[82] Singh S., P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced Lightweight Encryption Algorithms for Iot Devices: Survey, Challenges, and Solutions," *J. of Amb. Intel. and Hum. Comp.,* pp. 1-20, 2017.

[83] Sklavos N., *et al.*, "Cryptography and Security in the Internet of Things (IoT): Models, Schemes, and Implementations." *8th IFIP International Conference on New Technologies, Mobility and Security* (NTMS'16), 2016.

[84] Sundmaeker H, *et al*., "Vision and Challenges for Realizing the Internet of Things," *European Commission—Information Society and Media,* Brussels, Belgium, 2010.

[85] Tawalbeh L., F. Muheidat, M. Tawalbeh and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Appl. Sci.,* vol. 10, no. 4102, pp. 1-18, 2020.

[86] Verma S., R. Choubey and R. Soni, "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security", *International Journal of Emerging Technology and Advanced Engineering*, vol. 1, pp. 18-21, 2012.

[87] Wang M. Y., C. P. Su, C. L. Horng, C.W. Wu and C. T. Huang, "Single and Multicore Configurable AES Architectures for Flexible Security", *IEEE Transactions on Very Large-Scale Integration Systems*, vol. 2, pp. 540-552, 2010.

[88] Weber S.G. *et al*., "*Towards Trustworthy Identity and Access Management for the Future Internet*," in: 4th International Workshop on Trustworthy Internet of People, Things & Services, Trustworthy IoPTS'10, 2010.

[89] Worthman E, "Lightweight Cryptography for the IoE," *Light Primitives and New Technologies are Driving the Next Generation of Lightweight Cryptography*, 2015.