A Symmetric Scheme for Securing Data in Cyber-Physical Systems/IoT Sensor-based Systems based on AES and SHA256

Henry Blankson
Vellore Institute of Technology
Tamil Nadu 632014
India

Rajan Chattamvelli
Vellore Institute of Technology
Tamil Nadu 632014
India

ABSTRACT

Cyber-Physical Systems (CPS) and the Internet have undoubtedly simplified and enhanced the lifestyle of people in this present era. Internet of Things (IoT) is also being seen as the new technology that is changing human discernment about daily life. Countless cyber-physical devices generate a lot of sensitive data, which needs to be secured. All the applications of CPS/IoT fundamentally need symmetric keys for the encryption/decryption of sensitive data generated. This paper seeks to propose a symmetric scheme for securing data in a CPS using IoT sensor-based technology, which will be based on Advanced Encryption Standard**(**AES) and SHA256 encryption/decryption method.

General Terms

Algorithms, blockchain, digital certificate, encryption, federated learning,hybrid cryptosystems,symmetric cryptography.

Keywords

elliptic curve cryptography, encryption algorithm, hash function, hybrid cryptosystems, modified AES algorithm, symmetric cryptography

1. INTRODUCTION

In spite of the various advantages that CPS have brought, the security of the data gathered is a big issue [1]. The reliance on sensitive, private, unrelated nature of data and their deployments in large-scale renders the security of the data gathered to be very crucial. Internet of Things (IoT) is also a model that is gaining in popularity in recent years [2]. Sensors, humans, computing devices, or anything that gives or receives services may interact with each other through IoT [3]. Current research is not concerned with the production and acquisition of data, but rather the management and security of it, which include storage, analysis and confidence in the data gathered [4].

2. HASH FUNCTIONS

A hash function is a mathematical function that converts aninput value (a number, string, image, audio-clip etc.) into a numerical value. In cryptographic applications, it typically takes a set of characters (key) and maps it to a value of a particular length (hash value) [5]. It is also known as message digest algorithm as it takes an arbitrary message and produces a unique message digest of fixed length (called its digital footprint) that gets appended to the source message. One example of a hash function is SHA256, developed by the National Institute of Standards and Technology (NIST). The SHA256 algorithm is a cryptographic hash function that is used in digital certificates as well as in data integrity. It takes a message of random length less than 264 bits as input and produces an output of 256-bit message digest [6]. Due to the enormous rise in the amount of data being daily processed globally and locally by data networks, scientists are looking for techniques to increase data access and warrant that data be exchanged more securely [7]. The deployments of hash functions alongside with other security technologies can be used to solve this problem.

A symmetric scheme is a cryptographic concept that involves an encryption algorithm, a secret key and a decryption algorithm. Encryption and decryption in this type of scheme use the same key. The encryption algorithm is reversible and is an opposite of the decryption algorithm. A few familiar examples of symmetric encryption methods include the Digital Encryption Standard (DES), Triple-DES (3DES; which is a triple invocation of DES which is slower in speed but better in quality), BLOWFISH and IDEA. The main security aims are the privacy and authenticity of communicated data [8],[9].

CPS combine the dynamics of physical processes with that of an in-depth collaboration of control, communications, and computational (3C) technology within the whole integrated system [10]-[11]. The main representative of CPS applications include smart grids, medical devices, Industrial Control Systems (ICS), smart drones, and smart car. In their survey on CPS, [12] presented a catalog of threats, weaknesses, known attacks and existing controls. They concluded that the cyber-physical security framework must include how an attack of the physical domain of a CPS can result in unexpected results in the cyber territory and vice versa along with suggested solutions. A new CPS model was also proposed by [13]. In the proposed model, ways of using the algebraic theory of interaction and knowledge of insertion modeling to solve problems of analysis and fusion of CPSs were given.

IoT involves the interconnection of computing devices and electronic gadgets, embedded in modern devices via the Internet, thus enabling them to send and receive data. This is one of the leading technologies in the current digital transformation [14]. IoT relies on a combination of protocols, technologies and devices such as sensors (wireless), wearable and implanted sensors. The multiplicity of IoT can be viewed as a double-edged sword that gives luxury to users but can also lead to serious security threats and attacks [15]. **IoT** is a blending of “Things” (Machines and Objects) to the Internet and ultimately to each other, whereas **CPS** is a concept that combines the physical process, computation and networking.

IoT is similar to CPS, sharing the same basic architecture; whereas CPS gives a higher coordination and combination than IoT[4].

3. RELATED WORKS

3.1 Unification of CPS and IoT

CPS and IoT are two data centric technologies where a huge amount of data are generated on an ongoing basis.There exists a potential solution to process a huge amount of data efficiently and securely using their unification [4],[16]. To process such data efficiently, [4] proposed a potential solution, where an attempt was made to lay down a theoretical foundation to attain an inter-operability between the two technologies. The combination of the two technologies was found to increase the speed, efficiency, processing and functionality as compared to using the two technologies alone.

The Hochschulraum-Strukturmittel (HRSM) national funding platform under the Austrian Federal Ministry of Science, Research and Economy, initiated a joint CPS/IoT Ecosystem. This project proposes to bring the two technologies (CPS/IoT) closer by assessing the intersection points in theory and practice. The main funding agencies of the CPS/IoT Ecosystem were AIT, IST, TTTech and BMWFW. The major aim of this project was to provide an interactive educational platform that would include students, and provide them with opportunities to gain hands on experience in CPS/IoT. According to [17], the specific goals of the CPS/IoT ecosystem are to:

i. Assess enabling state-of-the-art technologies for CPS/IoT,
ii. Build industrial and educational demonstration platforms,
iii. Acquire smart applications for buildings, mobility, production and farming.

In an attempt to promote a unified measurement, science and standards foundation for assured and operation of CPS/IoT applications, the NIST in its special publication 1900-202 gave these major conclusions [16]:

i. The classifications of CPS and IoT are congregating over time to include a common emphasis on hybrid systems of interrelating analog, digital, human and physical components in systems engineered for function through integrated logic and physics.
ii. The recognition of this convergence can merge isolated fields and sectors for progress in application, shared research, and origination goals and opportunities.
iii. The hybrid nature of CPS/IoT systems has brought important suggestions for engineering, including cyber-physical security, design warrant, lifecycle management, synchronization and timing and more.

Finally, these major conclusions can enlighten research, benchmarks; commercial and legal policy and regulatory efforts designed to achieve the value to society using advanced CPS/IoT technologies.

3.2 AES vs DES

Aleisa (2015) compared the encryption/decryption standards for 3DES and AES and concluded that for security issues, AES is undoubtedly considered unbreakable in practical use. The flaws of DES and 3DES make them insecure and no longer of any use. The 1997 and 1998 attacks required a great deal of cooperation and very expensive to implement and so they are still beyond the competency of most attacks. The DES can be broken in less than 5 minutes of CPU time at present. Due to the increase in power of computers and stronger algorithms required to face hacker attacks, AES became the solution to that requirement [18]. Finally, it was concluded that AES provides more security in the long term. The original version works on a substitution-permutation network, also known as SP network and requires less memory (RAM) than DES versions.

In their proposal for an efficient AES implementation using Field Programmable Gate Array (FPGA) with enhanced security features, [16] gave the techniques to enhance the encryption quality of AES algorithm and its implementation on FPGA. They did this by using PN Sequence Generator to generate the S-box values in the modified AES algorithm (mAES). Also the initial key required for the encryption/decryption was based on the output of the PN Sequence Generator. The outcome of encryption for mAES algorithm was tested on the Strict Avalanche Criterion for 2048 differences and the mean percentage avalanche effect of 60% was achieved as compared to the traditional AES algorithm. The throughput results and their area were compared with the existing non-pipelined and pipelined designs and a better performance was attained.

There are more attacks being formulated against AES. As CPU speed and competences advance, chances of these attacks are becoming areality. But AES can always increase the number of rounds or move to generating dynamic S-boxes so as to improve the resistance of the standard. In general, the main attack will be against implementation of the standard (when there is a mistake on the programmed standard that can be abused). Properly authenticated and supported codes must be used to protect against this sort of attacks [20].

The comparison of two security criteria based on the theoretical framework of Rogaway-Shrimpton (hiding and puzzle-friendliness with the security of hash function criteria) was investigated in [21]. It was established by [21] that overcoming hiding or puzzle-friendliness is more demanding than that of the traditional hash function criteria. So it is not hard to select a hash function to be used in any blockchain system so as to confirm the establishment of the preimage-resistant or preimage cryptanalysis like SHA256. This also tends to be enough for any blockchain design.

3.3 SHA256

In the implementation of HMAC-SHA256 algorithm for data integrity and message authentication, [22] introduced an algorithm in a hybrid routing protocol for mobile network environment, and the performance of the protocol was analyzed by calculating the throughput, end-to-end delays and packet delivery ration of the network. It was observed after using Network Simulator 2 (NS2) for the simulation that there was an improvement in the packet delivery ration, and the throughput at the cost of more processing time. This made the network more secure by preventing DOS attacks.

To secure all online transactions, [23] proposed a modified SHA256 (MSHA256) security protocol through smart contract based on blockchain mechanism. The main focus on the research was to modify the security protocol that has been designed for practical applications of blockchain with specific reference to trust and privacy. A new transaction procedure was recommended which involves customer and merchant to permit entities to recognize one another and also to enable them to proceed with their transactions security using the mechanism of blockchain.

3.4 Hybrid Cryptosystems

The implementation of a hybrid cryptosystem with symmetric key algorithm AES and a secure hash algorithm SHA256 was presented by [24], where they used the VI LabView toolkit environment. The proposed hybrid cryptosystem used SHA256 bit as a key generation for AES in order to increase the data security to a higher extent. By implementing this hybrid cryptosystem, a higher security in terms of complexity was achieved.

AES is considered as an algorithm that has fast encryption and decryption. To provide very good data security that can be transferred over a network, [25] used AES algorithm to achieve this. In the implementation of the scheme, the files to be encrypted were multimedia files such as images, videos and audios. These files were entered into the application, and then a key that has been encrypted with SHA256 algorithm is applied to secure the contents of the file. Multimedia file encryption applications have therefore been successfully built based on theresults of the experiments in their research.

4. OVERVIEW OF AES and SHA256

a. Advanced Encryption Standard (AES)

Data encryption is one of the most important techniques for securing information. There are two kinds of cryptographic methods namely symmetric and asymmetric cryptosystems. Symmetric cryptography uses a key that is identical to the transmitter as well as the receiver, for encrypting and decrypting the data transferred. Examples of symmetric cryptography include Data Encryption Standard (DES), Triple DES and Advanced Encryption Standard (AES). On the other hand, in asymmetric cryptography, different keys are used for encryption and decryption of transferred data. Rivest-Shamir-Adleman algorithm (RSA), Elliptic Curve Cryptography (ECC) and Digital Signature Algorithm (DSA) are some examples of asymmetric cryptography. Identified by the National Institute of Standards and Technology (NIST) of the USA, the AES algorithm was approved to replace the DES algorithm in 1997 [19].

The AES, which is an example of a symmetric cryptography, was created by Joan Daemen and Vincent Rijmen (Rijndael algorithm), which combined a strong algorithm with a strong key. AES is a widely used symmetric method to secure data where its algorithm has a very fast encryption process. The block cipher can use different blocks with variable key combinations such as 128, 192 or 256 bits to produce a faster and better secure symmetric block ciphers. The Twofish algorithm was another that was considered as an alternative to the Rijndael block cypher. This can use blocks with keys from 128 bits to 256 bits. But the combinations for the Rijndael algorithm provides good performance, ease of implementation, security, and flexibility that makes AES a good selection against the Twofish algorithm [18].

The AES encryption and decryption algorithms are shown in Algorithm 1 below[19]:

Encryption Algorithm

```
s ← in
s ← AddRoundKey(s, w[0, $N_b$-1])
for r=1 to ($N_r$-1) do
   s ← SubBytes(s)
   s ← ShiftRows(s)
   s ← MixColumns(s)
   s ← AddRoundKey(s, w[r $N_b$, (r+1)$N_b$-1])

s ← SubBytes(s)
s ← ShiftRows(s)
s ← AddRoundKey(s, w[$N_rN_b$, ($N_r$+1)$N_b$-1])
out ← s
```

Decryption Algorithm

```
s ← in
s ← AddRoundKey(s, w[$N_rN_b$, ($N_r$+1)$N_b$-1])
for r=($N_r$-1) downto 1 do
   s ← InvShiftRows(s)
   s ← InvSubBytes(s)
   s ← MixColumns(s)
   s ← AddRoundKey(s, w[r $N_b$, (r+1)$N_b$-1])

s ← InvShiftRows(s)
s ← InvSubBytes(s)
s ← AddRoundKey(s, w[0, $N_b$-1])
out ← s
```

Algorithm 1: AES encryption and decryption

b. Secure Hash Function 256 (SHA256)

A Cryptographic Hash Function (CHF) is a mathematical algorithm that takes a random size of data as input and creates a fixed–size output of encrypted text, which is known as a hash value. In[21]authors defined a CHF as a function

$$H: K \times M \rightarrow Y$$

where $K=\{0,1\}^K$, $Y=\{0,1\}^C$ for integers K, c > 0, $M=\{0,1\}^*$ for the set of strings(no length limit). The set K is referred to as key space, and the number c is called the hash length of H.

An example of a CHF is the SHA256 algorithm. It was developed by NISTand usually used in digital certificates and data integrity. In SHA256 algorithm, a message of any arbitrary length less than 264 bits is taken as an input, and after hashing produces an output of 256-bits message digest [22].

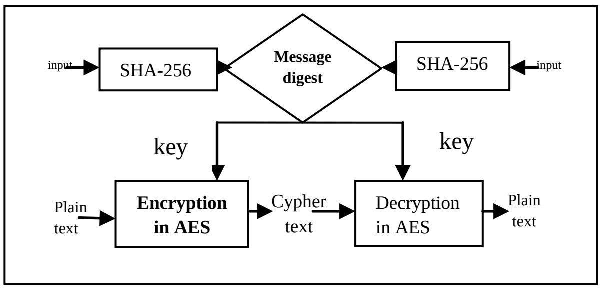

Figure 2: General working of proposed method

To achieve this, [6] stated the steps as follows:

a. The message is first of all filled such that its length is congruent to 448 mod 512. This is known as padding. This involves adding a single 1 bit to the end of the message, and the extra zeros so that the length equals to 448 mod 512.

b. To make the message length exactly a multiple of 512 bits, the result is appended with a 64-bit representation of the message's length.

c. The next step is to parse the padded message into N different 512-bit blocks of messages namely $M^{(1)}$, $M^{(2)}$, $M^{(3)}$,…, $M^{(N)}$. This can be achieved by appending 64-bit block.

d. An initial hash value, $H^{(0)}$ is set with eight 32-bit words. This must be in a hexadecimal form.

e. The message schedule is then prepared and labeled as W_0, W_1, W_2,…, W_{63}. This involves a message schedule of sixty-four 32-bit words. Figure 3 below gives the SHA256 algorithm.

$$W_t = f(x) = \begin{cases} {M_t}^{(t)} & 0 \le t \le 15 \\ \sigma_1^{(256)}(W_{i-2}) + W_{i-7} + \sigma_0^{(256)}(W_{i-15}) + W_{i-16}, & 16 \le t \le 63 \end{cases}$$

where:

$$\sigma_1^{(256)}(W_{i-2}) = \big((W_{i-2})ROTR\ 17\big) \oplus \big((W_{i-2})ROTR\ 19\big) \oplus \big((W_{i-2})SHR\ 10\big)$$

$$\sigma_1^{(256)}(W_{i-15}) = \big((W_{i-15})ROTR\ 7\big) \oplus \big((W_{i-15})ROTR\ 18\big) \oplus ((W_{i-15})SHR\ 3)$$

a. The eight working variables A, B, C, D, E, G, and H are initialized with the (i-1)th hash value.

```
For t = 0 to t = 63:
{
    $T_1 = H + \sum_1^{(256)}(E) + Ch(E,F,G) + K_1^{(256)} + W_1$
    $T_2 = \sum_0^{(256)}(A) + Maj(A,B,C)$
    H = G
    G = F
    F = E
    E = d + $T_1$
    D = C
    C = B
    B = A
    A = $T_1$ + $T_2$
}
```

Where:

$$\Sigma_1^{(256)}(E) = (E\ ROTR\ 6) \oplus (E\ ROTR\ 11) \oplus (E\ ROTR\ 25)$$

$$\Sigma_0^{(256)}(A) = (E\ ROTR\ 2) \oplus (E\ ROTR\ 13) \oplus (E\ ROTR\ 22)$$

$$Ch(E,F,G) = (E\ \wedge \mathrm{F}) \oplus (\sim E\ \wedge \mathrm{G})$$

$$Maj(A,B,C) = (A\ \wedge \mathrm{B}) \oplus (A \wedge \mathrm{C}) \oplus (B \wedge \mathrm{C})$$

b. The resulting hash function, after repeating all the steps a total of N times will yield:

$$H_0^{(N)} \parallel H_1^{(N)} \parallel H_2^{(N)} \parallel H_3^{(N)} \parallel H_4^{(N)} \parallel H_5^{(N)} \parallel H_6^{(N)} \parallel H_7^{(N)}$$

Figure 3: SHA-256 Algorithm

5. PROPOSED SCHEME

AES-128 algorithm (the 8-round version of 128-bit key length AES encryption) was cracked in 2009 with the help of a known-key distinguishing attack.The key should be known to (generated by) the hacker for this to be successful. The key recovery attack on full AES reported by [27] used a biclique technique, which is four times faster than brute force, but didn't provide significant results.This is why AES is still known as the golden standard in cryptography.Attackersalways look for the weakest link to break-in. Such attacks can be precluded using any shadowing technique where an encrypted key is used in AES rather than a plaintext key.This can be done using a multitude of ways like elliptic cryptography, hashing algorithms, etc. This works if the hacker don't know the key generation method.This paper proposesa hybrid cryptosystem with symmetric key AES algorithm and a secure hash algorithm SHA256. In this scheme, data generated by the CPS/IoT sensor-based system (M) will be sent to a central data collection point with the aid of distributed systems. The main theoretical bases deployed in this paper are the combination of two secure routing techniques: a symmetric encryption/decryption model (AES) and a hash function (SHA256).

The data to be encrypted are those generated from CPS/IoT sensor based system as plaintext. These include the date/time the data was sent (T), the unique number of sensor (ID), and the main data that the sensor was designed to collect (D). Applying the two algorithms for AES and SHA-256, an input of any arbitrary length will be given to the SHA256 module.

Table 1. SHA256 hashing to make secure key

Plaintext	Key transform	Ciphertext
Los Angeles Chargers	original	\xa2\x83\x83l\xdfn\x00\x9e\xdb[\xf7\xc7\xaf\x8f\xe5q\xba\x06zB\x0b\xb4f\x96`\x8e\xbcX.Q\xd0\xee
LsnglsChrgrs	vowels, whitespace removed	\x0f\xb3\x85\xbf\x1a\xca^[\xac\x85\x1b\x8f5\x0873\xb4\xd9\x1b\x86\xac\x15\x08\xf5\xd3\xa7j\xd9=\x87\x86\xed

Table 2. SHA256 hashing to recursively secure key

Plaintext	**Key transform**	**Ciphertext**
Buffalo Bills	original	\x1c\xe8\xa0\x93R\x9d/m\xf8\xfc\x0e\x05O\x17\x8b\x97\x17\xa9wXR\x7f@\x13J\xbe~F\x1f\xa9
BfflBlls	vowels, whitespace removed	8&\xd1.T\xea\xbde\xd9\xe6\xa4\x9f\x89\xea\xeeM\x84m\xabk\xd0>\x99\xa4a\x82y-.P\xb9!
BflBls	Dups removed	)\xcd\x8a\xa7&\xeb\x9d`\x80Kt\xce\xd2\xd5\xa3#!\xea4\xa2~\xc1\x08\xe49\xce\xa4\xc9\xea\xadc\x8b
Bf#lBl$s	Dups replaced	\xb5\xc7T\x12`\x9c\xc0/\x18\x96\x01R\x94]\x92\xea\xb8\x1bB\xee\xf1Z\xf3\x8c\x195\xf8\xf5\x87\xca\x80\xbb

A pre-processing of the key is done to make it more difficult to crack. This is done by (i) removing all whitespace (space, tab, etc.) (ii) removing all vowels and (iii)replacing repeated characters by a single one (or by a set of pre-chosen special characters). For example, if the key is “Los Angeles Chargers” removing whitespace and vowels gives “LsnglsChrgrs”. If the key is “Buffalo Bills” removing whitespace and vowels gives “BfflBlls”. An additional step to remove repeating characters results in “BflBls”. On occasion, this may result in repetition of substrings. Consider the key “Tennessee Titans” which after first step becomes “TnnssTtns”, and reduces to “TnsTns” (if character case is not considered in removal of duplicates). This is clearly a repetition of “Tns” and is not considered a good key. Hence the pre-processing step can be made recursive to remove all such repeating substrings to give a strong key. Alternatively replace repeating characters by special ones (second ‘f’ by,say, ‘#’ and second consecutive ‘l’ by ‘$’ to get “Bf#lBl$s” or “Tn@s#T$ns”, etc.). This is more effective to protect classified information as it has higher collision resistance and is hard to brute-force by adversaries.

This will then generate a fixed length (256-bits) of message digest. The message digest generated will be used in the symmetric encryption/decryption procedure as key. A plaintext which is the data generated by the sensor (i.e. T+ID+D), is given to the AES module which will be encrypted using the key generated by the SHA256 module to generate the ciphertext. This ciphertext is then stored at a data-logging system using the blockchain technology. To retrieve the stored ciphertext from the data logging system, the same key that was used to encrypt the plaintext is used to decrypt the ciphertext.

The security in this module is given in terms of its complexity which involves hybrid integration of SHA256 algorithm used along with AES algorithm. The complexity of the proposed architecture is also very high, which guarantees a higher data security. It also ensures the authentication and data integrity of the original data

6. CONCLUSION

In this paper, the application of a symmetric scheme on data generated from a cyber-physical systems/IoT sensor-based system using AES and SHA256 to generate the ciphertext is explored. Data stored at the data-logging center using the blockchain technology will ensure that it is secured and very difficult to attack by adversaries.

The possible future work is to find ways to encrypt multi-media files and also use multimedia keys. A federated learning model in which data are kept locally and the model is kept on the central system, which is updated periodically using parameters of sub-models trained on local data are also under study. This will tremendously decrease network bandwidth requirements as the error information and the learned parameters only are communicated to the central server. It is best suited in time-dependent models when only some of the local data change dynamically over time.

7. ACKNOWLEDGMENTS

We thank the reviewer for helpful comments that has improved the presentation of the paper.

8. REFERENCES

[1] Yaacoub, J.P.A., Salman,O., Noura,H.N.,Kaaniche,N., Chehab,A. and Malli,M. 2020. Cyber-physical systems security: Limitations, issues and future trends, *Microprocess. Microsyst.*, vol. 77, doi: 10.1016/j.micpro.2020.103201.

[2] Farooq,U., Ul Hasan,N., and Baig,I.,2019. Securing Internet of Things (IoT) through an Adaptive Framework, *16th Int. Multi-Conference Syst. Signals Devices, SSD 2019*, pp. 387–392, doi: 10.1109/SSD.2019.8893153.

[3] Parasuraman,K., and Anbarasa Kumar,A.,2020. Cyber Security: A New Approach of Secure Data Through Attentiveness in Cyber Space, in *Lecture Notes on Data Engineering and Communications Technologies*.

[4] Fatima,I., Anjum,A., Malik,S.U.R. and Ahmad,N.,2020. Cyber Physical Systems and IoT: Architectural Practices, Interoperability, and Transformation, *IT Prof.*, vol. 22(3), pp. 46–54, doi: 10.1109/MITP.2019.2912604.

[5] Gauravaram,P.,2007. “Cryptographic Hash Functions : Cryptanalysis , Design and Applications,” *Inf. Secur.*, .

[6] Rachmawati,D.,Tarigan,J.T., and Ginting,A.B.C,2018. A comparative study of Message Digest 5(MD5) and SHA256 algorithm, *J. Phys. Conf. Ser.*, vol. 978, no. 1, doi: 10.1088/1742-6596/978/1/012116.

[7] Krawczyk,H.,1995. New hash functions for message authentication, *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 921, pp. 301–310

[8] Buchanan,W. J.,2017. *Cryptography*.

[9] Bellare,M., Paterson, K.G.and Rogaway,P.,2014. Security of symmetric encryption against mass surveillance, *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8616 LNCS, no. PART 1, pp. 1–19, doi: 10.1007/978-3-662-44371-2_1.

[10] Liu, Y. Peng,Y., Wang,B., Yao,S., and Liu,Z.2017.Review on Cyber-physical Systems, vol. 4, no. 1, pp. 27–40.

[11] Shi, J. Wan, and hehua Y. Hui Suo, A Survey of Cyber-Physical Systems, 2011.

[12] Humayed,A., Lin, J., Li,F. and Luo,B.,2017. Cyber-Physical Systems Security - A Survey, *IEEE Internet Things J.*, vol. 4(6), pp. 1802–1831, doi: 10.1109/JIOT.2017.2703172.

[13] Letichevsky,A.A., Letychevskyi,O.O., Skobelev,V.G. and Volkov,V. A.,2017. Cyber-Physical Systems, *Cybern. Syst. Anal.*, vol. 53, no. 6, pp. 821–834, 2017, doi: 10.1007/s10559-017-9984-9.

[14] Mrabet,H., Belguith,S., Alhomoud,A. and Jemai,A.2020. A survey of IoT security based on a layered architecture of sensing and data analysis, *Sensors (Switzerland)*, vol. 20(13), pp. 1–20, doi: 10.3390/s20133625.

[15] Gubbi,J., Buyya,R., Marusic,S. and Palaniswami,M.2013. Internet of Things (IoT): A vision, architectural elements, and future directions, *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, doi: 10.1016/j.future.2013.01.010.

[16] Greer,C. Burns,M. Wollman,D. and Griffor,E.2019. Cyber-Physical Systems and Internet of Things NIST Special Publication 1900-202 Cyber-Physical Systems and Internet of Things, *NIST Spec. Publ. 1900-202*.

[17] Isakovic,H., Crespo,E.A., and Grosu,R.,2021. An energy sustainable cps/iot ecosystem, vol. 10, pp. 2–3.

[18] Aleisa, N.,2015. A comparison of the 3DES and AES encryption standards, *Int. J. Secur. its Appl.*, vol. 9(7), pp. 241–246, doi: 10.14257/ijsia.2015.9.7.21.

[19] Zodpe, H. and Sapkal, A.,2018. An efficient AES implementation using FPGA with enhanced security features, *J. King Saud Unversity. - Engineering and Sciences*, https://doi.org/10.1016/j.jksues.2018.07.002.

[20] Rahman,A.U. Miah,S.U. and Azad,S.,2014. Advanced encryption standard, *Pract. Cryptogr. Algorithms Implementations Using C++*, no. December, pp. 91–126, 2014, doi: 10.1201/b17707.

[21] Wang,M., Duan,M., and Zhu, J., “Research on the security criteria of hash functions in the blockchain,” *BCC 2018 - Proc. 2nd ACM Work. Blockchains, Cryptocurrencies, Contract. Co-located with ASIA CCS 2018*, pp. 47–55, 2018, doi: 10.1145/3205230.3205238.

[22] Ravilla, D., and Putta,C.S.R.,*2015.* Implementation of HMAC-SHA256 algorithm for hybrid routing protocols in MANETs, *2015 Int. Conf. Electron. Des. Comput. Networks Autom. Verif. EDCAV* , pp. 154–159, doi: 10.1109/EDCAV.2015.7060558.

[23] Perez, M. R. L., Gerardo,B. and Medina,R.,2018. Modified SHA256 for securing online transactions based on blockchain mechanism, *2018 IEEE 10th Int. Conf. Humanoid, Nanotechnology, Inf. Technol. Commun. Control. Environ. Manag. HNICEM 2018*, pp. 0–4, doi: 10.1109/HNICEM.2018.8666341.

[24] latif,L.H., and Erçelebi,E., 2017. Implementation of Hybrid Cryptosystem using AES-256 and SHA-2 256 by LabVIEW, *Ijarcce*, 6(1), pp. 351–357, doi: 10.17148/ijarcce.2017.6169.

[25] Fauziah,N.A.,Rachmawanto, E.H., Setiadi, D.R.I.M. and. Sari, C.A., 2018. Design and implementation of AES and SHA256 cryptography for securing multimedia file over android chat application, *2018 Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2018*, pp. 146–151, doi: 10.1109/ISRITI.2018.8864485.

[26] Rolf Oppliger, 2017. *Contemporary Cryptography*, vol. 110, no. 9.

[27] Bogdanov, A., Khovratovich, D., and Rechberger, C. (2009). Biclique Cryptanalysis of the Full AES, http://research.microsoft.com/en-us/projects/cryptanalysis/aesbc.pdf