

Security enhancement of cyber-physical system using modified encryption AESGNRSA technique

Kundankumar Rameshwar Saraf, P. Malathi

Department of Electronics and Telecommunication Engineering, D. Y. Patil College of Engineering,
Savitribai Phule Pune University, Pune, India

Article Info

Article history:

Received Oct 28, 2023

Revised Nov 16, 2023

Accepted Nov 17, 2023

Keywords:

AES

CPS

Cyber-attacks

Galois counter mode

RSA

ABSTRACT

A cyber-physical system (CPS) is a combination of physical components with computational elements to interact with the physical world. The integration of these two systems has led to an increase in security concerns. Traditional encryption algorithms designed for general-purpose computing environments may not adequately address the distinct challenges of CPS, such as limited processing power, delay, and resource-constrained hardware. Therefore, there is a pressing need to develop an encryption algorithm that is optimized for CPS security without compromising the critical real-time aspects of these systems. This research has designed a modified encryption technique named the advanced encryption standard in galois counter mode with nonce and rivest-shamir-adleman algorithm (AESGNRSA). A smart medical system is designed to monitor the health of remotely located patients. The AESGNRSA algorithm is applied to the three servers of this system. The data of 1.5 lakh patients is fed to this system to verify the effectiveness of the AESGNRSA algorithm. The performance parameters like encryption and decryption time, encryption and decryption throughput, and encrypted file size are calculated for the AESGNRSA algorithm. The comparative analysis proved that AESGNRSA has the highest performance as compared to other algorithms and it can protect CPS against many cyber-attacks.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Kundankumar Rameshwar Saraf

Department of Electronics and Telecommunication Engineering, D. Y. Patil College of Engineering

Savitribai Phule Pune University

Pune, Maharashtra, India

Email: kundansaraf@gmail.com

1. INTRODUCTION

Cyber-physical systems (CPS) are used to manage many public and private businesses such as smart healthcare systems, smart manufacturing systems, transportation management, national security and defense, and secure energy supply systems [1], [2]. CPS has a connection between cyber and the physical world which increases the risk of cyber-attacks [3]. CPS has fulfilled the production requirement in industry 4.0 which leads to improved effectiveness and efficiency of the entire industry [4]. To protect the confidentiality and integrity of IoT devices lightweight cryptographic (LWC) algorithms can be used [5]. However, the limited power sources, memory, capacity, and small physical area of LWC make it unsuitable to use for the security of CPS [6]. This paper explains the need for media access control (MAC) layer security in CPS. It focuses on denial-of-service attacks (DoS), brute force attacks, replay attacks, and man-in-the-middle (MITM) attacks. This paper has developed an advanced encryption standard in galois counter mode with nonce and rivest

shamir adleman algorithm (AESGNRSA) algorithm to protect CPS against major cyber-attacks on the MAC layer.

Rural areas are affected by inefficient medical facilities. Hence, accurate and timely disease diagnosis is missing. It leads to an increase in mortality in patients located in villages. To overcome this issue timely monitoring and diagnosis of the patient's health in rural areas is essential. This leads to the need for a smart health monitoring system that monitors the health of remotely located patients using sensors connected to the beds placed in health care centers [7]. This system can send a notification to a doctor in case of any emergency health issues of patients and in case of any cyber-attack detection on any server of CPS. It can also protect patient data during machine-to-machine communication between different servers and smart health monitoring systems. The AEGNRSA algorithm is developed and implemented to protect CPS data against cyber-attacks.

Problem definition: the integration of cyber and physical components in CPS introduces vulnerabilities that can be exploited by malicious actors, potentially leading to disruptions, safety hazards, and privacy breaches. Traditional encryption algorithms designed for general-purpose computing environments may not adequately address the distinct challenges of CPS, such as limited processing power, delay, and resource-constrained hardware. Therefore, there is a pressing need to develop an encryption algorithm that is optimized for CPS security without compromising the critical real-time aspects of these systems.

Literature survey: many researchers have used hybrid cryptographic algorithms with the amalgamation of both symmetric and asymmetric algorithms. Reza *et al.* [8] use lightweight encryption algorithms (LWCs) to secure the smart grid against cyber-attacks by the ChaCha20 data encryption method. It uses chaos-based key generation and a public key-based authentication scheme. LWCs have limited computing power which reduces the speed of encryption and prone to various cyber-attacks. Also, LWCs lack standardization and support. Hence, the use of standard encryption algorithms like advanced encryption standard (AES), and Rivest, Shamir, and Adleman (RSA) is a better choice for CPS security.

Alsman *et al.* [9] cipher block chaining mode of the AES is used to increase the security and integrity of data and also to mitigate bit-flipping attacks. In the case of CPS security many servers and components are interconnected. The data transmission by AES alone causes a key management attack. Hence, the symmetric algorithm should be used to increase the speed of encryption and the asymmetric algorithm should be used to avoid the key management issue by symmetric algorithm. A combination of symmetric and asymmetric algorithms is a better choice to secure CPS.

Verma *et al.* [10] AES-DES-RSA is used to perform data encryption. This research splits the data into three parts. The first part is encrypted by AES, the second part is encrypted by data encryption standard (DES), and the third part is encrypted by RSA. This process makes the encryption bulky and slow. It can be susceptible to caesar's attack. Hence, a faster version of the hybrid algorithm is required.

Kumar *et al.* [11] paper shows the process which encrypts the image using AES. The AES key is encrypted by the RSA public key. The RSA private key is used to decrypt the AES key at the receiver. This method only applies to medical images. The replay attack and data authentication are not considered in this research.

Harba [12] paper uses AES to encrypt the data, RSA to encrypt the key generated by AES, and hash-based message authentication code (HMAC). HMAC makes this process slow and inefficient. The comparative analysis of the proposed algorithm with similar methods is missing.

Zou *et al.* [13] paper performs data encryption using AES to generate ciphertext1. This ciphertext1 and AES key are again encrypted using the RSA public key to generate ciphertext2. This method is susceptible to replay attacks during file encryption, and data tampering and forgery when the double key is cracked.

Patil and Joshi [14] hybrid technique of RSA and AES is used, to make the system more secure. The RSA algorithm is used to communicate with the receiver through the session key, and the AES algorithm is used to encrypt this session key which makes the key. The use of RSA for data encryption makes the process slow. AES should be used to encrypt the data and RSA should encrypt the AES key.

Pamungkas [15] encrypts large data by AES and the AES key is encrypted by the RSA. It uses Java to secure rest API. Jintcharadze and Iavich [16] show the implementation of hybrid cryptosystems Twofish+RSA, AES+RSA, and AES+ElGamal implemented and compared. The proposed hybrid models can be analyzed by entropy index in the future. Pamungkas [15] and Jintcharadze and Iavich [16] Java-based implementation increases the lag in system response. Patil and Joshi [14] show that the proposed hybrid algorithm AES+RSA is significantly secure.

Siregar [17] the digital file in JPG format is encrypted by AES. The AES key is encrypted by RSA. Secrecy, data integrity, authentication, and non-repudiation achieved. This research is only limited to the encryption of images in JPG format. Other digital files need to be encrypted by this method. This hybrid

cryptosystem [18] based on AES and RSA can effectively enhance the security and efficiency of data transmission. The replay attack consideration is missing.

Analyzing the results [19] shows that the use of RSA, AES, and SHA-3 can protect message privacy among smart objects. It is the best solution, in terms of costs and security. The computing or processing of this algorithm needs to be improved. Liu *et al.* [20] have implemented AES-RSA hybrid encryption for secure email communication using Java language. A comparative analysis of hybrid encryption with other similar existing algorithms is missing.

The impact of MAC layer attacks on CPS: in a DoS attack [21] the attacker sends a huge number of malicious packets to CPS. MAC layer denies service to legitimate users. It disturbs CPS communication and causes delays or failure in critical CPS processes. In a MAC spoofing attack [22] the attackers spoof MAC addresses and mimic themselves as a genuine device. He gains unlawful access to CPS. It can alter data, or launch other cyber-attacks such as MITM. In a jamming attack [23] the attacker sends continuous packets to the MAC layer. It creates congestion in CPS device communication. It disturbs CPS component synchronization and fails the physical system. In a replay attack [24] attackers capture genuine MAC layer packets and later replay these packets to mislead the system. It leads to illegal action and control of CPS by attackers. In an injection attack [25] the attackers manipulate CPS component behavior by injecting malicious packets into the MAC layer. It leads to threats to safety and damage to the equipment. For example, forged sensor reading. In an eavesdropping attack [26] without being detected attackers can passively monitor CPS communication and gather sensitive details. These details help an attacker to gain unlawful CPS access with further minute details of key management attacks [27] the attacker can gain CPS component access by exploiting vulnerabilities in key management protocol. This key can be used to decrypt protected CPS communication that breaches CPS confidentiality and integrity.

Summary of literature findings: The detailed literature survey concludes that the MAC layer attack disturbs the continuity of CPS operation and coordination between CPS devices on the execution layer and control layer. The MAC layer attacks such as DoS, network scanning, and brute force attacks are major disruptions to CPS security. A symmetric algorithm can compromise the keys of encryption during the transmission. An asymmetric algorithm can slow the data transmission. Existing encryption standards have some drawbacks such as latency in communication, low throughput, missing authentication of communication, and high power consumption. A combination of symmetric and asymmetric algorithms (modified encryption) is a better way to secure CPS. A modified encryption standard is needed to have,

- Less processing power, minimum delay, high throughput, and resource-constrained hardware.
- Maintain coordination between the CPS devices during real-time processing of CPS.

Motivation for research, most of the researchers have designed authentication schemes [9], [21], [28], [29] to address the security of machine-to-machine (M2M) communication in CPS against particular attacks. Also, many of the schemes are heavy to implement in the embedded system of CPS which lessens the throughput of the system, increases the end-to-end delay during the communication, and causes poor latency. Hence, there is a need for a security algorithm to enhance the security of CPS against multiple cyber-attacks. It should have high throughput, enough security level, low encryption and decryption time, and less size of encrypted data. With this motivation, this research work has designed a new encryption scheme for the security of M2M communication in CPS.

2. METHOD

This section explains the need for a modified encryption algorithm. The smart health monitoring system. And the AESGNRSA algorithm with its flowchart.

2.1. Need for the modified encryption algorithm

In 2001, the National Institute of Standards and Technology (NIST) started using the AES with the Rijndael algorithm as a federal information processing standard (FIPS). AES proved as most flexible, secure, and fast algorithm [30]. RSA algorithm has the smallest computing power impact that improves the network transmission effect. It maintains link-bearing capacity by improving the resource utilization rate [31].

AES is a symmetric key algorithm. Hence, the sender and receiver need the same key during the encryption and decryption of data respectively. During this key transmission, the attacker can recover the key through an MITM attack on AES. RSA is a relatively slow algorithm. Hence, it can't be used to encrypt user data in many practical applications. Hence, this research uses the RSA algorithm to encrypt the key generated by AES. AES algorithm prone to brute force attack. It also has authentication issues. Hence, this research uses the AES algorithm in galois counter mode (GCM) to increase data authenticity and authentication. The random number in the form of the nonce is added to the AES encrypted cipher text to prevent replay attacks. The security enhancement of CPS depends on various factors. The encryption algorithm used to

encrypt the CPS data should have a small size of cipher text, high encryption and decryption speed, less encryption and decryption time, and an appropriate security level.

2.2. Smart health monitoring system

To implement the AESGNRSA algorithm this research has considered a use case of a smart health monitoring system as shown in Figure 1. In this system, the bed equipped with various sensors is placed in health care centers in rural areas. The temperature sensor, heartbeat sensor, perfusion index (PI) sensor, oxygen level monitoring (SpO2) sensor, and weight measuring sensor are connected to the bed.

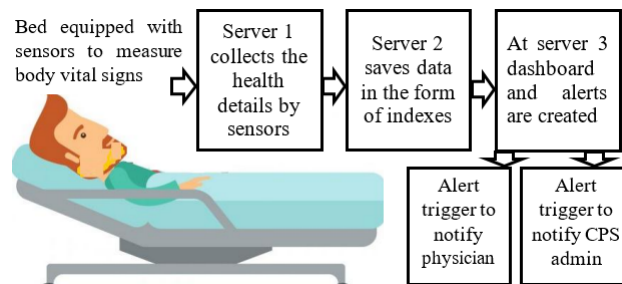


Figure 1. Smart health monitoring system

Server 1 is located in the health care center. It collects the health details of the patient in the form of sensor readings. Server 2 is located at a remote location which saves the data of server 1 in the form of various indexes. Server 3 is used to search the data and create dashboards to monitor the health details of the patient. At server 3 smart health monitoring dashboard is created using splunk enterprise 9.1.0.2. This dashboard has three panels. Panel 1 contains the basic details of the patient including a patient name, gender, age, contact number, e-mail ID, medical history, and present health issues for the patient. Panel 2 contains the physical body parameters of the patient which include height, weight, body mass index, heart rate in beats per minute, body oxygen level in percentage, perfusion index in percentage, body temperature in Fahrenheit, and blood sugar level in mg per dl. The CPS threat detection dashboard is created at server 3. This dashboard has three panels. Panel 1 monitors the DoS attack attempt in the last 1-minute duration, Panel 2 detects the CPS component and port scan in the last 1 hour, and Panel 3 detects brute force attack in the last 24 hours.

2.3. AESGNRSA algorithm

This research has developed an algorithm named AESGNRSA. This algorithm uses AES in GCM. The CPS data is encrypted using the AES key. The AES key is encrypted by the RSA algorithm. The nonce is added to the encrypted AES cipher text. Features of the modified encryption algorithm AESGNRSA are:

- AES-GCM is a block cipher mode of operation that provides high speed of authenticated encryption and integrity. Hence, it can prevent attacks such as brute force attacks, dictionary attacks, password spray, rainbow table attacks, pass-the-hash attacks, pass-the-ticket attacks, silver ticket exploits, golden ticket exploits, credential stuffing, and skeleton keys attacks.
- Nonce is a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in any cyber-attack. Hence, it can prevent replay attacks.

Encryption of AES key by RSA algorithm reduces the risk of symmetric key management during the sharing. Hence, it can prevent MITM, false data injection, and sparse attacks. The Splunk tool is used to remotely monitor DoS attacks (disturbs availability), brute force attacks (disturbs confidentiality), and port scanning attacks (disturbs integrity).

2.4. Flowchart of AESGNRSA algorithm

The flowchart in Figure 2 divides the process of the AESGNRSA algorithm into 5 steps:

- RSA key generation - the RSA public and private keys are generated. A cipher object instance for RSA is created using the public key.
- AES key generation and key encryption - a 128-bit AES key is created and encrypted by RSA public key.
- CPS data encryption by AES - the AES encrypts the CPS data and adds nonce to cipher text.

- Decryption process - the cipher object instance for RSA is created using RSA private key. The AES key is decrypted by the RSA private key.
- Decrypt ciphertext - the CPS data is decrypted by AES. And print the performance parameters.

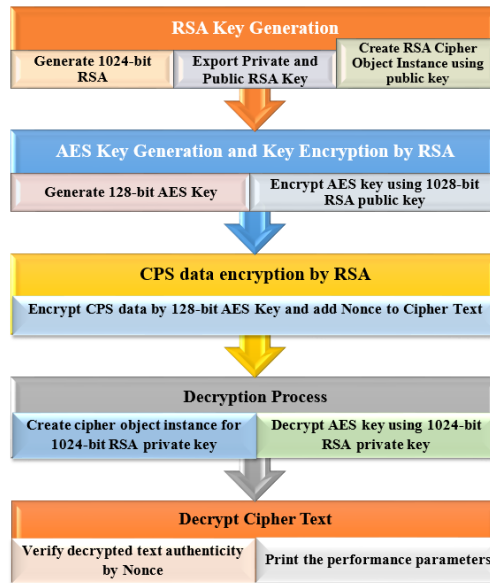


Figure 2. Flowchart of AESGNRSA algorithm

2.5. Modelling of AESGNRSA algorithm with Pseudocode

Key Generation by RSA and AES;

- **RSA Key Generation:** Generate two large prime numbers, p and q. Compute $n = p * q$ and $\phi(n) = (p-1)(q-1)$. Where $\phi(n)$ = Euler’s quotient function. Choose a public exponent e such that $1 < e < \phi(n)$ and e is coprime with $\phi(n)$. Calculate the private exponent d such that $d \equiv e^{-1} \pmod{\phi(n)}$. The public key is (e, n) and the private key is (d, n).
- **AES Key Generation:** Generate a random symmetric key of appropriate length (128 bits).
- **AES Key Exchange:** The public key (e, n) is shared for encryption. The private key (d, n) is kept secret for decryption.
- **AES Encryption:** The sender uses AES to encrypt the data with the randomly generated symmetric key. The symmetric key is encrypted with the recipient's RSA public key (e, n).

Pseudocode:

```

AES_key = GenerateRandomAESKey()
ciphertext = AES_Encrypt(plaintext, AES_key) + nonce
RSA_encrypted_key = RSA_Encrypt(AES_key, RSA_public_key)
  
```

- **AES Decryption:** The receiver uses his RSA private key (d, n) to decrypt the AES key.

The receiver then uses the decrypted AES key to decrypt the ciphertext.

Pseudocode:

```

AES_key = RSA_Decrypt(RSA_encrypted_key, RSA_private_key)
Plaintext = AES_Decrypt(ciphertext, AES_key)
  
```

3. RESULTS AND DISCUSSIONS

This section elaborates software and hardware used in the smart health monitoring system, and the implementation of the AESGNRSA algorithm. Data collected by smart health monitoring system. The encryption-decryption time, encrypted file size, and encryption-decryption throughput are calculated by the AESGNRSA algorithm and compared with the existing research results of other researchers.

3.1. Software and hardware used

The AESGNRSA algorithm is created using Python 3. Dashboards and alerts of smart medical systems are created using Splunk 9.1.0.2. All three CPS servers have 16 GB RAM and a 3 GHz clock speed.

3.2. Data collection method

This system has created and used various .csv files which contain patient data. This data includes the patient's name, gender, age, contact details with email ID, medical history, and present health issues. Table 1 given below shows the number of patients concerning the size of the file.

Table 1. Patient data for various file sizes

File size (KB)	Number of patients	File size (MB)	Number of patients
32	199	1.19	8,329
64	434	3.57	25,289
128	884	7.14	50,468
256	1,739	10.7	75,629
512	3,489	17.8	125,814
1,024	7,004	21.4	151,889
2,048	14,159		
4,096	28,318		

3.3. Encryption time of algorithm

The time required to encrypt the plaintext data using an encryption algorithm is called encryption time. The encryption time (in nanoseconds) should be as small as possible. As shown in Table 2, the AESGNRSA algorithm takes the least time to encrypt the data as compared to other similar encryption algorithms.

Table 2. Encryption time in nanoseconds

Plaintext size (KB)	AESGNRSA	Ref 16				Ref 18	
		AES + RSA	Twofish + RSA	AES + Elgamal	Twofish	RSA + Blowfish	
32	60,600	37,24,59,621	45,44,527	2,28,97,995	14,63,712	90,47,797	
64	97,000	47,76,03,056	89,38,838	2,61,82,346	41,40,075	1,22,03,366	
128	1,65,900	50,19,21,935	1,56,17,402	3,23,77,061	56,25,297	1,35,55,651	
256	4,17,000	52,99,11,194	3,06,01,857	4,75,97,261	1,00,12,910	1,42,40,434	
512	7,76,600	57,03,62,261	4,97,84,217	6,88,21,938	2,00,01,135	2,98,86,045	
1,024	16,87,500	57,10,26,941	11,33,60,689	10,23,85,356	4,21,06,688	4,08,55,251	
2,048	34,71,900	58,82,99,138	22,36,62,075	13,92,74,046	8,19,08,320	4,39,79,084	
4,096	67,32,000	68,61,85,029	40,44,10,673	24,77,89,014	18,31,73,897	6,35,42,269	

3.4. Decryption time of algorithm

The time required to decrypt the plaintext data using a decryption algorithm is called decryption time. The decryption time (in nanoseconds) should be as small as possible. As shown in Table 3, the AESGNRSA algorithm takes the least time to decrypt the data as compared to other similar encryption algorithms.

Table 3. Decryption time in nanoseconds

Plaintext size (KB)	AESGNRSA	Ref 16 Twofish	Ref 18 RSA + Blowfish
32	87,600	17,58,853	18,81,211
64	87,800	32,35,260	21,89,046
128	1,30,400	47,45,870	50,57,937
256	4,12,700	2,17,30,722	93,45,405
512	8,05,000	1,84,26,348	1,81,16,046
1,024	14,46,300	4,42,81,630	2,56,66,278
2,048	27,07,300	12,94,39,314	4,44,15,486
4,096	54,21,600	17,65,83,136	4,44,15,486

3.5. Encrypted file size

The file created after encryption is called an encrypted file or cipher text. The encrypted file should be as small as possible. As shown in Table 4, the encrypted file size (in bytes) of the AESGNRSA algorithm is the smallest as compared to other similar encryption algorithms.

Table 4. Encrypted file size in bytes

Plaintext size (kb)	AESGNRSA	Ref 16 Twofish	Ref 18 RSA+Blowfish	Ref 18 RSA+AES
32	32,179	65,440	59,355	31,744
64	64,725	1,30,848	1,18,428	65,536
128	1,30,942	2,61,696	2,37,417	1,31,072
256	2,61,366	5,23,392	4,77,370	2,62,144
512	5,23,755	10,46,752	9,51,418	5,24,288
1,024	10,48,137	20,96,928	18,98,922	10,48,576
2,048	20,96,902	41,93,856	38,13,804	20,97,152
4,096	41,93,468	83,87,712	76,24,638	41,94,304

3.6. Encryption throughput

The speed of data encryption is called encryption throughput. The encryption throughput should be as large as possible. Table 5 shows the encryption throughput of various encryption algorithms in MB/Sec. The AESGNRSA algorithm has the highest encryption throughput as compared to other similar encryption algorithms.

Table 5. Encryption throughput in megabytes/second

Plaintext size (KB/MB)	AESGNRSA	Ref 13		
		RSA	AES	Hybrid (AES+RSA)
32KB	506	-	-	-
64KB	636	-	-	-
128KB	752	-	-	-
256KB	597	-	-	-
512KB	643	-	-	-
1,024KB	592	-	-	-
2,048KB	575	-	-	-
4,096KB	594	-	-	-
1.19MB	490	15.112	0.158	1.685
3.57MB	679	45.528	0.506	2.072
7.14MB	620	82.409	1.074	2.111
10.7MB	644	132.295	1.419	2.831
17.8MB	641	172.516	2.303	3.495
21.4MB	650	186.969	2.565	3.547

3.7. Decryption throughput

The speed of data decryption is called decryption throughput. The decryption throughput should be as large as possible. Table 6 shows the decryption throughput of various algorithms in MB/Sec. As shown in Table 6, the AESGNRSA algorithm has the highest decryption throughput as compared to other similar encryption algorithms.

Table 6. Decryption throughput in megabytes/second

Plaintext size (KB/MB)	AESGNRSA	Ref 13		
		RSA	AES	Hybrid (AES + RSA)
32KB	350	-	-	-
64KB	703	-	-	-
128KB	957	-	-	-
256KB	603	-	-	-
512KB	620	-	-	-
1024KB	691	-	-	-
2048KB	738	-	-	-
4096KB	737	-	-	-
1.19MB	667	21.595	0.167	18.387
3.57MB	646	77.725	0.488	19.119
7.14MB	695	139.264	0.996	18.425
10.7MB	667	205.924	1.291	20.981
17.8MB	678	260.857	2.654	21.615
21.4MB	640	300.607	2.896	27.676

4. CONCLUSION

In this research, all possible cyber-attacks on CPS have been studied and it is found that MAC layer attacks are most disruptive for CPS security. Hence, this research mainly concentrated on mitigating MAC

layer attacks by the AESGNRSA algorithm. The CPS framework for smart healthcare system is designed. This system monitors the health of remotely located patients using three wireless interconnected servers, a dashboard, and alerts. This research has developed a modified encryption technique named the AESGNRSA algorithm. This algorithm is implemented on a smart health monitoring system and five performance parameters such as encryption time, decryption time, encrypted file size, encryption throughput, and decryption throughput are measured. These parameters are measured using the AESGNRSA algorithm and compared with existing algorithms. The AESGNRSA algorithm has encryption time of 149.30, 24.15, 377.85, 74.99, and 6146.20 times lesser than RSA+Blowfish, Twofish, AES+Elgamal, Twofish+RSA, and AES+RSA algorithms respectively. The AESGNRSA algorithm has a decryption time of 21.47 and 20.08 times less than the RSA+Blowfish and Twofish algorithms respectively. The AESGNRSA algorithm has an encrypted file size that is 0.99 times higher than the AES+RSA algorithm. It is lower than 1.84 and 2.03 times RSA+Blowfish and Twofish algorithm respectively. The AESGNRSA algorithms have encryption throughputs 290.80, 3101.27, and 32.42 times higher than AES+RSA, AES algorithm, and RSA algorithm respectively. The AESGNRSA algorithms have decryption throughputs 36.28, 3994.01, and 30.89 times higher than AES+RSA, AES algorithm, and RSA algorithm respectively. It can be concluded that the AESGNRSA algorithm has the lowest encryption and decryption time, the smallest size of cipher text, and the highest encryption and decryption throughput as compared to other similar algorithms. This system has real-time threat detection capability. Hence, the overall security of CPS has improved with the use of the AESGNRSA algorithm as compared to other existing algorithms. The AESGNRSA algorithm can be used in applications such as smart transportation, smart grid, smart manufacturing, and smart water networks. This algorithm can be further extended to predict the cyber-attacks based on behavioral analysis of CPS. This research has focused on DoS, brute force, and network and port scan detection attacks. The AESGNRSA algorithm needs to be tested against other cyber-attacks.

ACKNOWLEDGMENTS

I express my gratitude to D.Y. Patil College of Engineering and its staff for their support in completing this research.





REFERENCES

- [1] K. R. Saraf, P. Malathi, and K. Shaw, "Security enhancement of contactless tachometer-based cyber physical system," *Machine Learning Approaches for Urban Computing*, 2021, pp. 165–187, doi: 10.1007/978-981-16-0935-0_8.
- [2] K. R. Saraf and P. Malathi, "Cyber physical system of smart three-phase induction motor and its security measures," in *Innovations in Cyber Physical Systems: Select Proceedings of ICICPS 2020*, 2021, pp. 1–10, doi: 10.1007/978-981-16-4149-7_1.
- [3] K. R. Saraf and P. Malathi, "Cyber-physical system-based secure online medication system," in *Handbook of Research on Artificial Intelligence and Soft Computing Techniques in Personalized Healthcare Services*, New York: Apple Academic Press, 2023, pp. 325–348, doi: 10.1201/9781003371250-18.
- [4] S. A. Haque, S. M. Aziz, and M. Rahman, "Review of cyber-physical system in healthcare," *International Journal of Distributed Sensor Networks*, vol. 10, no. 4, p. 217415, Apr. 2014, doi: 10.1155/2014/217415.
- [5] K. R. Saraf and M. P. Jesudason, "Encryption principles and techniques for the internet of things," in *Cryptographic security solutions for the internet of things*, 2019, pp. 42–66, doi: 10.4018/978-1-5225-5742-5.ch002.
- [6] J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber-physical system," *Future Generation Computer Systems*, vol. 108, pp. 1287–1296, Jul. 2020, doi: 10.1016/j.future.2018.04.018.
- [7] K. R. Saraf and P. Malathi, "Intelligent learning analytics in the healthcare sector using machine learning and IoT," *Machine Learning, Deep Learning, Big Data, and Internet of Things for Healthcare*, pp. 37–53, 2022, doi: 10.1201/9781003227595-3.
- [8] S. M. S. Reza, A. Ayob, M. M. Arifeen, N. Amin, M. H. Md Saad, and A. Hussain, "A lightweight security scheme for advanced metering infrastructures in smart grid," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 2, pp. 777–784, Apr. 2020, doi: 10.11591/eei.v9i2.2086.
- [9] Y. S. Alslman, A. Ahmad, and Y. AbuHour, "Enhanced and authenticated cipher block chaining mode," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 4, pp. 2357–2362, Aug. 2023, doi: 10.11591/eei.v12i4.5113.
- [10] V. Verma, P. Kumar, R. K. Verma, and S. Priya, "A novel approach for security in cloud data storage using AES-DES-RSA hybrid cryptography," in *2021 Emerging Trends in Industry 4.0 (ETI 4.0)*, IEEE, May 2021, pp. 1–6, doi: 10.1109/ETI4.051663.2021.9619274.
- [11] S. B. J. Kumar, A. Nair, and R. V. K. Raj, "Hybridization of RSA and AES algorithms for authentication and confidentiality of medical images," in *2017 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, Apr. 2017, pp. 1057–1060, doi: 10.1109/ICCSP.2017.8286536.
- [12] E. S. I. Harba, "Secure data encryption through a combination of AES, RSA, and HMAC," *Engineering, Technology & Applied Science Research*, vol. 7, no. 4, pp. 1781–1785, Aug. 2017, doi: 10.48084/etasr.1272.
- [13] L. Zou, M. Ni, Y. Huang, W. Shi, and X. Li, "Hybrid encryption algorithm based on AES and RSA in file encryption," in *Frontier Computing: Theory, Technologies and Applications (FC 2019) 8*, 2020, pp. 541–551, doi: 10.1007/978-981-15-3250-4_68.
- [14] T. Patil and B. Joshi, "Improved acknowledgement intrusion detection system in MANETs using hybrid cryptographic technique," in *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, IEEE, Oct. 2015, pp. 636–641, doi: 10.1109/ICATccT.2015.7456962.





- [15] T. Pamungkas, "Combining RSA + AES encryption to secure REST endpoint with sensitive data," BATC — BFI Agile Thought Community. Accessed: Apr. 26, 2022. [Online]. Available: <https://medium.com/batc/combining-rsa-aes-encryption-to-secure-rest-endpoint-with-sensitive-data-eb3235b0c0cc>
- [16] E. Jintcharadze and M. Iavich, "Hybrid implementation of twofish, AES, ElGamal and RSA cryptosystems," in *2020 IEEE East-West Design and Test Symposium (EWDTS)*, IEEE, Sep. 2020, pp. 1–5, doi: 10.1109/EWDTS50664.2020.9224901.
- [17] H. Siregar, E. Junaedi, and T. Hayatno, "Implementation of digital signature using AES and RSA Algorithms as a security in disposition system of letter," *IOP Conference Series: Materials Science and Engineering*, vol. 180, p. 012055, Mar. 2017, doi: 10.1088/1757-899X/180/1/012055.
- [18] Guru, Mr Abhishek and A. Ambhaikar, "AES AND RSA-based hybrid algorithms for message encryption & decryption," *Information Technology in Industry*, vol. 9, no. 1, pp. 273–279, Mar. 2021, doi: 10.17762/itii.v9i1.129.
- [19] G. Sánchez-Arias, C. G. García, and B. C. P. G-Bustelo, "Midgar: study of communications security among smart objects using a platform of heterogeneous devices for the internet of things," *Future Generation Computer Systems*, vol. 74, pp. 444–466, Sep. 2017, doi: 10.1016/j.future.2017.01.033.
- [20] Y. Liu, W. Gong, and W. Fan, "Application of AES and RSA hybrid algorithm in e-mail," in *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, IEEE, Jun. 2018, pp. 701–703, doi: 10.1109/ICIS.2018.8466380.
- [21] N. Vicky, "Domain adaptation of deep learning (D) DoS attack detection models in resource-constrained cyber physical systems environments," Auckland University of Technology, 2023, <https://hdl.handle.net/10292/16228>.
- [22] R. Pal and V. Prasanna, "The STREAM mechanism for CPS security the case of the smart grid," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 4, pp. 537–550, Apr. 2017, doi: 10.1109/TCAD.2016.2565201.
- [23] G. Hatzivasilis, I. Papaefstathiou, and C. Manifavas, "SCOTRES: secure routing for IoT and CPS," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2129–2141, Dec. 2017, doi: 10.1109/JIOT.2017.2752801.
- [24] R. A. Abouhogail, "A new secure lightweight authentication protocol for NFC mobile payment," *International Journal of Communication Networks and Information Security*, vol. 11, no. 2, pp. 283–289, 2019, doi: 10.17762/ijcnis.v11i2.4142.
- [25] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: threats and potential solutions," *Computer Networks*, vol. 169, 2020, doi: 10.1016/j.comnet.2019.107094.
- [26] P. Angueira *et al.*, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 2, pp. 810–838, 2022, doi: 10.1109/COMST.2022.3148857.
- [27] M. Abdalzaher, M. Fouda, A. Emran, Z. Fadlullah, and M. Ibrahim, "A survey on key management and authentication approaches in smart metering systems," *Energies*, vol. 16, no. 5, p. 2355, Mar. 2023, doi: 10.3390/en16052355.
- [28] K. R. Saraf and P. Malathi, "Splunk-based threat intelligence of cyber-physical system: a case study with smart healthcare," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 2, pp. 537–549, 2023.
- [29] L. Li, K. Jia, and X. Wang, "Improved meet-in-the-middle attacks on AES-192 and PRINCE.," *IACR Cryptology ePrint Archive*, vol. 2013, p. 573, 2013, [Online]. Available: <http://dblp.uni-trier.de/db/journals/iacr/iacr2013.html#LijW13>
- [30] D. Joan, and V. Rijmen, "Announcing the advanced encryption standard (aes)," Federal Information Processing Standards Publication, 2001, [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf>.
- [31] M. A. Al Sibahee, S. Lu, Z. A. Hussien, M. A. Hussain, K. A.-A. Mutlaq, and Z. A. Abduljabbar, "The best performance evaluation of encryption algorithms to reduce power consumption in WSN," in *2017 International Conference on Computing Intelligence and Information System (CIIS)*, IEEE, Apr. 2017, pp. 308–312, doi: 10.1109/CIIS.2017.50.

BIOGRAPHIES OF AUTHORS



Kundankumar Rameshwar Saraf     is a Ph.D. research scholar (in Cyber Security) at D.Y. Patil College of Engineering, Akurdi, Pune. He is also working as a Technical Lead in Wipro Technologies, Pune. He has a total of 13 years of experience in various domains such as teaching, cyber security training, SOC by Splunk, and Site Reliability Engineer. He has completed his M.E. (2013) and B.E. (2010) in Electronics and Telecommunication Engineering. He has a wide range of global publications which include 11 journal papers, 4 book chapters, 1 Indian copyright, and 2 Indian patents. He is a reviewer for many international journals and books including Springer publication. He is a member of ISTE and IAENG membership. He has been recognized by many awards for presenting papers in National, International, and State level journals. He can be contacted at email: kundansaraf@gmail.com.



Dr. Mrs. P. Malathi     is a recognized Ph.D. guide of Savitribai Phule Pune University. Presently she is working as Principal of D.Y. Patil College of Engineering, Akurdi, Pune. She has a total of 30 years of teaching experience. She has completed a Ph.D. in Electronics and Telecommunication Engineering from the University of Pune. Her publication includes 5 Indian Patents, 4 books, 4 book chapters, and 122 research papers. She is a member of ISTE, IEEE, IETE, IEM, ISC and IAENG. She is a reviewer of many international journals. She has been recognized by the National Mahila Rattan Gold Medal Award and Bharat Vidya Shriromani Award. She can be contacted at email: pjmalathi@dypcoeakurdi.ac.in.