Advanced Encryption Standard Algorithm for Cyber-Physical-Social Computing and Networking

P. Sangeetha[1], M. Manikandan[2], R. Banu Priya[3], M. Jaya Prakash[4]

[1]*PG Student, Department Computer Science and Engineering, Vidhya Vikas College of Engineering and Technology, Tiruchengode, India*

[2]*Professor & HoD, Computer Science and Engineering, Vidhya Vikas College of Engineering and Technology, Tiruchengode, India*

[3]*Assistant Professor, Computer Science and Engineering, Vidhya Vikas College of Engineering and Technology, Tiruchengode, India*

[4]*Associate Professor, Department Master of Computer Application, Vidhya Vikas College of Engineering and Technology, Tiruchengode, India*

Abstract*: With digital communications and computing penetrate into every field of life, the IoT is born. There is no doubt that the IoT is leading innovation in many fields. eventually form Cyber-Physical-Social Computing and Networking (CPSCN) and create great changes of whole society. However, this process is still facing many challenges and information security is one of the most important. The main goal of information risk management is to keep risks at an acceptable level using risk identifications and risk assessments. Over the years, various methods for information security risk assessment have been put forward include the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), the Risk Analysis and Management Methods (CRAMM), and the Expressions of Need and Identifications of Security Objective (EBIOS). The improved neural networks such as Bayesian Network and Wavelet Neural Network (WNN) have been applied to risk assessments and have obtained many achievements. However, improved neural networks also have some disadvantages such as slow convergence speed and easy arrival at the local minima. cyber security or IT security or computer security is the protection of computer systems from hackers(theft) or damage their hardware, software or electronic data, as well as from disruption of the services they provide. Development of Vehicles computerized, cruise controls, anti-lock brake, seat belt tensioner, with engine timings, door locks, airbags and advanced driver-assistance system on more models. Additionally, connected cars may uses Wi-Fi and Bluetooth to communicates with onboard consumer devices and the cell phone networks. Self-driving cars are expected to be even more complex. Therefore, the present article explain the Advanced Encryption Standard algorithm is more valid security for Cyber-Physical-Social Computing and Networking.

***Keywords*: AES, CPSCN, cyber security, Encryption, Decryption.**

1. Introduction

From many generations, the fundamental need of human beings is:

1. To communicate and share information
2. Communicate securely.

These two needs gave origin to the art of coding messages which is known as cryptography.

It is the process of converting the secret messages, information or data into an unreadable form in order to protect it from an unauthorized person, according to some rules. Although, cryptography has been used for thousands of years, it is an adolescent science. It is an ancient way used to encrypt the messages. Encryption is the process in which the plaintext is converted into a ciphertext, this conversion of text is based on algorithms. Encryption can be performed in many ways such as replacing the message with numbers, symbols and pictures. In ancient times, people also use different types of voices to deliver their messages securely to the receiver. The word "cryptography" is extracted from the two Greek words "krypto" which means secret or hidden and "graphein" which means writing. Cryptography is observed with the advent of writing.

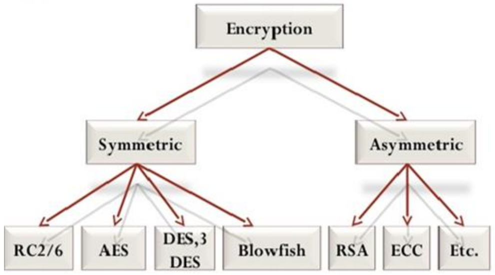

Fig. 1. Cryptography diagram

With digital communications and computing penetrate into every field of life, the IoT is born. There is no doubt that the IoT is leading innovation in many fields. Eventually form

Cyber-Physical-Social Computing and Networking (CPSCN) and create great changes of whole society. However, this process is still facing many challenges and information security is one of the most important. The main goal of information risk management is to keep risks at an acceptable level using risk identification and risk assessment.

Over the years, various methods for information security risk assessment have been put forward include the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), the Risk Analysis and Management Methods (CRAMM), and the Expressions of Need and Identifications of Security Objective (EBIOS). The improved neural networks such as Bayesian Network and Wavelet Neural Network (WNN) have been applied to risk assessments and have obtained many achievements. However, improved neural networks also have some disadvantages such as slow convergence speed and easy arrival at the local minima. we present a BPNN-based risk assessment method optimized by an improved cuckoo search (ICS) algorithm. Then, we put the improved Advanced Encryption Standard algorithm into a risk assessment model for a miniature IoT system.

A. Advanced encryption standard (AES)

AES is the cryptography techniques which uses same secret key, on the Rijndael cipher algorithm. AES is based on substitution and permutation functions and uses complicated ways to produce strong and almost unbreakable key which is our aim in order to transmitting our sensitive data through the network.The first step of AES expand key with the 128 bits length to more than ten key which each of these keys have 128 bits length, the number of produced keys build variant cycle. Input Message parameter will be mixed with these keys. AES just uses AddRoundKey function in the K0 and in the Kn uses SubBytes, Shiftrows and AddRoundKey and in the AES uses in the K2 to Kn-1 all of four functions AddRoundKey, SubBytes, Shiftrows and Add Round Key. Same time message or plain text passes these complicated functions and will be converted to encrypted message or cipher text. AES uses this inverse pattern to produce same message from encrypted message. AES converts message and key to four by four matrix, working by matrix form is more easier than original form. Information security is to protect the information and systems. AES is more secure.

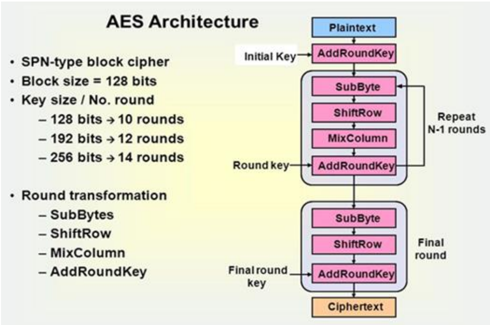

Fig. 2. AES architecture

The Advanced Encryption Standard (AES) is used to protect data against unauthorised access and to encrypt this. This designated AES (Advanced Encryption Standard)-128, AES (Advanced Encryption Standard)-192 or AES (Advanced Encryption Standard)-256 depending on the lengths. This method of encryption of any types of data is considered to be particularly secure and effective. AES is faster in both hardware and software.

2. Existing system

A BP neural network is a supervised learning artificial neural network algorithm, which was proposed in 1986 by Rumelhart, Hinton and Williams. The algorithm has extensive applications in many fields and usually contains three layers. Due to the ability of back-propagating, the BP neural network has excellent adaptability in solving nonlinear problems. The gradient descent method is the most common learning rule of BPNN which adjusted the weights by calculating the least mean squared (LMS) between the actual and the desired outputs. BPNN has been widely used in many fields due to its excellent nonlinear problem solving ability. However, it also has some defects such as slow convergence rate under certain conditions and the tendency to fall into local minimum. To aiming at Cuckoo Search is a new nature inspired Method for solving real valued numerical optimization problems. The method utilize Leavy flights random walk(LFRW) and biased random walk to search for new solutions. The prediction results of BPNN have largest experimental errors, which indicate that BPNN is not fit as risk prediction method. There is a huge variation within the prediction results of CSBPNN, and some of them are not perfect. Part of dimensions to be too aggressive when the large actor is sampled or too insufficient in the case of small factors. Cuckoo Search is varied Scaling Factors.

3. Problem statement

The Internet of things is the network of physical objects, that are embedded with network connectivity, sensors, electronics, software that enables them to collect and exchange data consideration of the security challenges involved.

- The IoT creates opportunities for more direct integration of the physical world into computer-based systems, it also given the opportunities for misuse.
- Particularly, as the Internet of Things spreads widely, cyber-attacks are likely to become an increasingly physical threats.
- Incase front door's lock is connected to the Internet, and may be locked or unlocked from a phone, then a criminal could enter the home at the press of a button from a stolen or hacked phone. People could stand to lose much more than their credit card numbers by IoT-enabled devices.
- Now a day’s Vehicles are increasingly computerized, with cruise control, anti-lock brakes, engine timing,

seat belt tensioners, airbags, door locks and advanced driver-assistance systems on many models and connected cars may use Wi-Fi and Bluetooth to communicate with the cell phone network and onboard consumer devices. Self-driving cars are expected to be even more complex.

- These all systems carry some security risk, and such issues have gained wide attention.

4. Proposed system

In proposed system, an information security program is to protect the information and systems that support the operations and assets of the agency. AES is more secure. The Advanced Encryption Standard (AES) is used in order to protect data from unauthorised access. The cryptographic process key of varying lengths. It is designated on AES-128, AES-192 or AES-256 depending on the length. This encryption method any type of data is considered to be particularly secure and effective. AES is faster in both hardware and software. It is also possible that, this model will allow people to well understand the potential risks in their system and create an incentive for developer to create lower-risk apps that do not contain invasive ad networks and avoid over-requesting permissions. The model is applicable for all types of organizations which conducting information security risk assessment. Different type of Algorithms are widely used throughout all areas of IT (information technology). An Advanced Encryption Standard (AES) algorithm transforms data according to specified actions to protect it. It was intended to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques.

AES can be used for secure communication such as in image encryption, ATM networks and secure storage such as confidential documents, government documents and personal storage devices. In order to improve the performance, AES algorithm can be used in parallel manner to execute operations. AES algorithm will be also modified for its source code bottlenecks and this will also help in the performance of the AES.

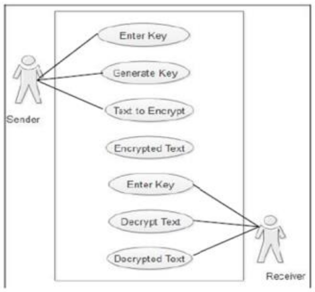

Fig. 3. Use case diagram of proposed AES

The security of the AES will be improved by applying sine, cosine and tangent functions after performing the rounds to make the encrypted data more secure. In the first step we will input key and generate step key using secondary key expansion. This key will help in the encryption and decryption of the data. Below is the UML (Unified Modeling Language) to explain the encryption and decryption process.

In Use Case Diagram, the sender will enter a secret key and then key will be generated. Now the text to be encrypted is entered and as a result the encrypted text will be generated. On the receiver side, the receiver uses the same key to decrypt the text and will get the original text.

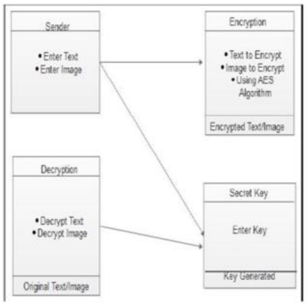

Fig. 4. Class diagram of proposed AES

In class diagram, there are two entities sender and receiver. The sender will send the text or image to encrypt, this encryption is done using AES algorithm. Then a secret key will be generated used in the encryption process. At the receivers end the text or image will be decrypted with the help of the same secret key.

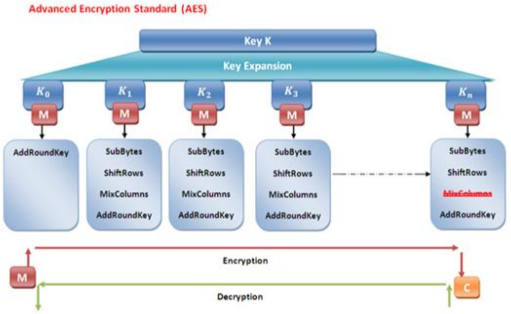

Fig. 5. Key expansion of AES

AES Encryption: AES (Advanced Encryption Standard) Algorithm that browse the source file which is to be encrypted and destination file where encrypted data is copied to it and enter the user defined key which helps to encrypt the desired file and then select the encryption mode zero, CBC and ECB.

AES Decryption: AES (Advanced Encryption Standard) Algorithm that browse the source file which is to be decrypted and destination file where decrypted data is copied to it and enter the user defined key which helps to decrypt the desired file and then select the decryption mode zero, CBC and ECB.

A. Benefits of AES algorithm

- More Security
- Lowest Cost

- Good Memory efficiency
- Simplicity and Flexibility of implementation

5. Conclusion

One of most popular cryptography technique as AES. AES is a symmetric encryption function by using same key in the sender and receiver sides and AES produces strong key which hackers are not able to break it. So AES is a good way to keep data confidential and integrity. It can be easily connected with the network for easily retrieving data and generating results.

References

[1] C. Zhu, L. Shu, V. C. M. Leung, S. Guo, Y. Zhang, and L. T. Yang, “Secure multimedia big data in trust-assisted sensor-cloud for smart city," IEEE Commun. Mag., vol. 55, no. 12, pp. 24-30, Dec. 2017.

[2] Nicholas G. McDonald, "Past and Present Methods of Cryptography and Data Encryption", University of UTAH, Vol 4, No.25, pp. 156-168,2002.

[3] Shasi Mehlrotra seth, Rajan Mishra―Comparative Analysis of Encryption Algorithms for Data Communication‖, IJCST, Vol. 2, Issue 2, June 2011.

[4] A. A. Ganin et al., “Multicriteria decision framework for cyber security risk assessment and management," Risk Anal., Sep. 2017.

[5] P. Mohapatra, S. Chakravarty, and P. K. Dash, ``An improved cuckoo search based extreme learning machine for medical data classification," Swarm Evol. Comput., vol. 24, pp. 25-49, Oct. 2015.

[6] Pitchaiah, Philemon and Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research (IJSER), Vol. 3, No.3, 2012.

[7] Hardjono, "Security in Wireless LANS and MANS," Artech House Publishers 2005.

[8] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[9] W. Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005, pp. 58-309.

[10] A. A. Ganin et al., ``Multicriteria decision framework for cybersecurity risk assessment and management," Risk Anal., Sep. 2017.

[11] L. Atzori, A. Iera, and G. Morabito, ``The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787-2805, Oct. 2010.