Computer Modeling in Engineering & Sciences CMES, vol.122, no.1, pp.323-349, 2020

A Hybrid Encryption Algorithm for Security Enhancement of Wireless Sensor Networks: A Supervisory Approach to Pipelines

Omid Mahdi Ebadati E.[1, *], Farshad Eshghi[2] and Amin Zamani[1]

Abstract: Transmission pipelines are vulnerable to various accidents and acts of vandalism. Therefore, a reliable monitoring system is needed to secure the transmission pipelines. A wireless sensor network is a wireless network consisting of distributed devices distributed at various distances, which monitors the physical and environmental conditions using sensors. Wireless sensor networks have many uses, including the built-in sensor on the outside of the pipeline or installed to support bridge structures, robotics, healthcare, environmental monitoring, etc. Wireless Sensor networks could be used to monitor the temperature, pressure, leak detection and sabotage of transmission lines. Wireless sensor networks are vulnerable to various attacks. Cryptographic algorithms have a good role in information security for wireless sensor networks. Now, various types of cryptographic algorithms provide security in networks, but there are still some problems. In this research, to improve the power of these algorithms, a new hybrid encryption algorithm for monitoring energy transmission lines and increasing the security of wireless sensor networks is proposed. The proposed hybrid encryption algorithm provides the security and timely transmission of data in wireless sensor networks to monitor the transmission pipelines. The proposed algorithm fulfills three principles of cryptography: integrity, confidentiality and authentication. The details of the algorithm and basic concepts are presented in such a way that the algorithm can be operational.

Keywords: Wireless sensor networks, pipeline, cryptography, cryptography algorithm, hybrid cryptography, confidentiality, integration, authentication.

1 Introduction

The pipeline is a way of transferring liquids, gases, or solid products in long distances and often is used to transport natural gas and oil. Pipelines for the transportation of crude and refined petroleum, natural gas, biofuels and other liquids, including sewage and water. Pipelines for drinking water or irrigation of agricultural products that require long-range passage through high-tide areas, are the most appropriate means of transport, according to evaporation, pollution or environmental impacts. Transmission pipelines, including natural

[1] Department of Mathematics and Computer Science, Kharazmi University, Tehran, Iran.

[2] Department of Electrical and Computer Engineering, Kharazmi University, Tehran, Iran.

[*] Corresponding Author: Omid Mahdi Ebadati E. Email: ebadati@khu.ac.ir.

Received: 25 July 2019; Accepted: 11 October 2019.

gas and oil, usually extend from extraction to processing and consumption sites, industrial plants or ports to transport tankers and transport. The pipelines also carry oil products from the refinery to consumption areas. Pipelines in industrial application are also used to continue the production and transportation process. Transmission pipelines are economically feasible, flexible, fully automated, and loading and unloading operations are automatic in them. As a result of reducing costs, this method is very suitable for the transportation of liquid products, for example, its costs are far lower than the cost of transportation by rail.

Pipelines are the most convenient, efficient and cost-effective way of transporting fluids such as oil, petroleum products, natural gas, water or even solids after mixing with liquids. The oil pipeline is usually made of steel or plastic tubes. Oil is transported through pipelines and pump stations along the pipeline. Natural gas and similar fuels, as well as liquid gas (LPG), are transmitted through natural gas pipelines from carbon steel. The possibility of transferring hydrogen, as well as hot water or even water vapor, is possible with the use of a network of insulated pipes. The transfer of toxic substances through pipelines is rarely done because there are many dangers along the pipeline route. Pipelines transporting flammable materials or explosives, such as natural gas or oil, are always accompanied by security considerations; however, there is a possibility of an incident. Pipelines can be targeted at sabotage or even terrorist attacks. In war, pipelines are part of the purpose of military attacks.

Oil and gas transmission lines play an important role in the national economy for transporting energy. Because of the long history of deployment, transmission lines suffer from various defects such as corrosion, cracking, leakage, etc. Disruptions in pipelines may result in human health and interruptions in energy transmission.

Access to sustainable energy is one of the Countries developmental requirements. Therefore, countries suffer expensive costs for energy production and transmission. Any failure or sabotage in the production or transfer of energy can affect the function of affiliated industries. War, internal disputes, legal problems, social inequalities, etc. are underlying causes of vandalism and exhaustion of transmission lines, lack of proper design, human error and etc. are cause of failure. Therefore, centralized monitoring of the energy transmission pipelines is critical. The centralized monitoring of energy facilities in general and the monitoring of energy transmission pipelines in particular have been lacking in intelligence and sustainability over the years. This problem stems from the length of the pipeline infrastructure, land characteristics and other environmental factors. Different technologies and strategies for monitoring pipelines have been developed from physical patrol to satellite monitoring. Some pipeline infrastructure monitoring methods include physical patrols, pipeline inspection gauge, sensor networks, wired sensor network, SCADA, and wireless sensor networks.

A wireless sensor network is a collection of sensor nodes connected to each other by wireless communication channels. Each sensor node is a small device that can collect data from the surrounding area, perform simple calculations and communicate with other nodes or with the main station. Such networks have been developed with the help of recent advances in micro-electromechanical systems and are expected to be widely used in applications such as environmental monitoring, home security, industrial process

monitoring, healthcare programs, and etc.

Security in wireless sensor networks depends on what it protects. Three security goals in wireless sensor networks include confidentiality, integrity and authentication [Yazdinejad, Nayyeri, Ebadati et al. (2017)].

Security can be established in each layer of application, network, data link, and physical layer. Cryptographic algorithms play a significant role in information security systems, and can also meet security goals in wireless sensor networks. Encryption is the process of changing message or information so that only authorized people can read that information. Encryption does not prevent the attack, but the content of the message is protected by the attacker. In an encryption scheme, the information or message set to be transmitted using an encryption algorithm change so that it can only be read by decrypting. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. For a good design encryption scheme, computational resources and much more skills are required. An authorized recipient of the message can easily decrypt the message with a key and an encryption algorithm. Cryptography is a knowledge of hiding information and verification, and includes protocols, algorithms, and secure strategies to prevent unauthorized access to critical information. Encryption provides a mechanism for verifying each component of a communication. Encryption follows the three main goals include message confidentiality, message integrity and Sender authentication.

In message confidentiality, only one authorized recipient must be able to extract the contents of the message from its encrypted form. Confidentiality includes a set of conventions or rules that limit the access to certain types of information, and hid information and stop free access to encrypted information.

In message integrity, the recipient must be able to detect the message that has been tampered with. Data integrity, maintenance, and assurance of the integrity of data throughout its life, and is an essential aspect of the design, implementation and use of any system that stores, processes and retrieves data. Maintaining the accuracy of the data means ensuring that the information is accurate and does not change its original content during transmission. Changing the initial content of the information may be accidental due to sending or deliberate problems.

In sender authentication, the receiver should be able to check the message, the sender's identity, the source, or the send and confirmation path of the sender. Authentication is the correct confirmation of a feature of a single piece of data that is done by an entity. Authentication is a validation process and may involve verification of a person by using his identity documents or by checking his credentials using a digital certificate.

An encryption algorithm is a component for secure electronic data transfer. Operational and mathematical stages develop cryptographic algorithms. Cryptographic algorithms prevent data frauds and unauthorized access to electronic information. Some cryptographic algorithms are faster than others. The designers and developers of the algorithms make the math background more complicated by the algorithms so that the attackers cannot penetrate. The power of an encryption algorithm usually depends on the length of the key. Cryptographic algorithms and functions used in cryptography are divided into symmetric, asymmetric, hashing, key exchange, key derivation and hybrid.

2 Literature review

In Panda [Panda (2014)] paper, two RSA and ECC public key algorithms have been investigated. The ECC algorithm has significant advantages over the RSA algorithm, which reduces the computation time as well as the amount of data transmitted. The RSA algorithm is a method for implementing a public key encryption system whose security depends on the complexity of the large prime numbers factoring. This method is suitable for data encryption and digital signature creation. The ECC algorithm is related to the algebraic structure of elliptic curves and its difficulty in elliptical curve size. The key advantage of this algorithm is the smaller key size, which reduces storage and transmission. For example, an elliptic curve algorithm can provide the same level of security in an RSA based system with smaller modules and keys. For current cryptographic purposes, an elliptic curve is a curved surface that contains points of the equation $y^2=x^3+ax+b$. Compared to the RSA, ECC has a smaller key and uses less memory, which is highly regarded by wireless sensor networks.

ECC cryptography has recently been an important topic in cryptographic research, which provides a higher level of security with a smaller key size than other encryption methods. A new method has been proposed by Singh et al. [Singh and Singh (2015a)] that eliminates the classical methods of mapping characters to offsets in the ECC. ASCII values match pairs of texts, and pairings are used as ECC encryption inputs. This proposed new method reduces the cost of the mapping operation and requires the sharing of the table between the sender and the receiver. The algorithm is designed to be used to encrypt or decrypt any type of text with the values of the ASCII. In this article, some ECC encryption concepts are fully described, and the remainder of the fractional calculation is described in brief with the use of the Euclidean algorithm developed.

Many images are moving in the network daily. Most of these images are confidential and should be transmitted securely. Cryptography plays a significant role in the safe transfer of images. The exponential problem solving a discrete logarithm of an elliptic curve proportional to the size of the ECC key provides a high level of security in comparison with other smaller size key encryption methods, which depends on the correct factoring or discrete logarithmic problem. In another article by Singh et al. [Singh and Singh (2015b)], an ECC algorithm for encryption, decryption, and digital signature of an image has been implemented. In this paper, a real case study was presented and histogram analysis, key size, key sensitivity to change, correlation analysis, entropy analysis, and resistance to some attacks checked out. In this paper, a cryptographic method was provided to match the encrypted photo. The algorithm was presented by grouping the pixels according to ECC parameters. The grouped pixel values are paired together instead of the values mapped to elliptic curve coordinates. This helps to override the use of the mapping table for encryption and decryption. The algorithm produces a cryptographic image with low correlation, even with a picture taken from similar pixels.

Data encryption is required to prevent unwanted access to information by individuals. In Patal et al. [Patel and Panchal (2014)], hybrid methods are investigated by combining two important RSA algorithms and Diffie-Hellman's algorithm. This hybrid cryptographic

algorithm provides more security than the RSA algorithm. RSA is the foundation of many encrypted applications. Great progress is for public key encryption and is also used for digital signing. The algorithm process consists of three steps: key generation, encryption and decryption. The Diffie-Hellman key exchange method allows two entities that have no prior knowledge to share a common key through an unsecured connection channel. Diffie-Hellman has been involved in multi-protocol development, including SSL, SSH, and IPS.

The RSA algorithm is used as one of the most efficient encryption algorithms and provides confidential, information integrity and privacy. In Shankar et al. [Shankar and Akshaya (2014)], the RSA algorithm has been integrated with Round-Robin priority scheduling to enhance security and reduce the effectiveness of infiltration. The minimum overhead, increased throughput and privacy are its benefits. In this method, the user uses the RSA algorithm and generates encrypted messages that are categorized according to priority and then sent. The receiver decrypt messages using the RSA algorithm and according to their priority.

Symmetric and asymmetric hybrid encryption algorithms provide integrated data transfer and concealment at higher speeds and play an important role in virtual private networks. Zhu [Zhu (2011)] article deals with the implementation of a hybrid algorithm. System performance analysis and practical tests show that an AES and ECC algorithm provides higher security than the DES and RSA algorithms, especially in virtual private networks that require secure transport.

Elliptic curve cryptography is an effective cryptography and has its own special advantages such as an efficient key relative to other key public infrastructures. In the article of Shahryar et al. [Shahryar, Fathi and Sekhavat (2017)], the random generator of the elliptic curve defined by the National Institute of Standards and Technology (NIST) is used to generate a sequence of arbitrary numbers based on curves. The generation phase is based on a common key and a generator point of G, which is a generator of a curve to obtain a random sequence. The AES encryption is then applied to these sequences and the keys to the image encryption are obtained. Using AES, along with random allocation, offers a prominent encryption method.

The image encryption is rapidly increasing with the increasing use of the Internet and media. Sharing important images on non-secure channels provides the ability to attack and steal. Encryption techniques are the best ways to protect images against attacks. Hill cipher algorithm is one of the symmetric cryptographic methods, with a simple structure and fast computing, but it has a weak security because the sender and receiver must share a private key on a non-secure channel. In the article of Dawahdeh et al. [Dawahdeh, Yaakob and Razif bin Othman (2018)], a new cryptographic method of elliptical curve encryption and Hill cipher is presented that uses Hill cipher method to use symmetric methods to asymmetric methods and increase security, efficiency and resistance to attacks. A self-inverse key matrix is used to create encryption and decryption keys so there is no need to find the reverse key matrix in the decryption process. A 4×4 hidden key matrix is used as an example in this study.

The Internet in the world today is widely used to access information, which is why there is a need to send secure information. The main goal of Brindha et al. [Brindha, Ramya and Jayantila (2013)] is to examine the encryption methods, to improve some of the current

algorithms, to create a way to increase the security and implementation of information encryption so that it is impossible to read the resources sent to the attackers on the web. AES and ECC are methods used for encryption. In the proposed algorithm, the file containing the text is encrypted using the AES algorithm and its key using the ECC algorithm, and the encrypted text is decrypted on the recipient's side. The AES and ECC algorithms are implemented together to provide hybrid encryption. The text is encrypted using AES. The key is encrypted using ECC. The text and the encrypted key are sent to the recipient. The text and the encrypted key are received. The key is decrypted using ECC. Encrypted text is decrypted using decrypt keys and AES.

The application of the network and the Internet is growing at a high rate, thus increasing the need to protect such applications. Singh et al. [Singh, Panchbhaiya, Pandey et al. (2015)] highlight this problem by providing two cryptographic methods. The first way is to compress data in half, and the second method focuses on producing characters of encrypted text differently for the same text characters than the different events of the character in the text. The combined effect of using symmetric algorithms with the proposed algorithm creates a hybrid encryption scheme that makes it difficult for an attacker to learn from messages transmitted in an unsecured transmission environment. In this paper, encryption and decryption are described in detail in four sections along with the code. In the last section, the key generated is different for each character, which means that a single character in the text may have a different cipher character corresponding to the character position.

Perumal et al. [Perumal and Al Khalidi (2014)] suggest a hybrid cryptographic system using a new public key algorithm and a private key algorithm. A hybrid encryption system combines the convenience of a public key system with the efficiency of a symmetric key. In this article, two secure data encryption methods are provided that are important for confidential. The system uses two different encryption algorithms for the encryption and decryption process; one is public key encryption based on a linear block cipher, and the other is private key encryption based on a symmetric simple algorithm. This encryption algorithm provides more security is better than other existing hybrid algorithms.

A computer network is an interconnected group of independent computing nodes that interact with each other by using a proper definition and a set of agreed rules and conventions known as protocols, and permitting the sharing of resources preferably in a way that can be Predictable and controllable. At the moment, various types of cryptographic algorithms provide high security for information in a controlled network. These algorithms need to specify the data security and authenticity of the user. In order to improve the strength of these security algorithms, a new security protocol for online transactions has been designed using the combination of symmetric and asymmetric encryption methods in Subasree et al. [Subasree and Sakthivel (2010)]. This protocol meets the three basic principles of encryption: integrity, confidentiality, and authentication. These basic principles can be met by using elliptic curve cryptography, Dual RSA and MD5. ECC for encryption, Dual RSA for authentication and MD5 for integrity. This new security protocol uses a combination of symmetric and asymmetric methods for better security and integrity. The text is encrypted using ECC. At the same time, the hash value is calculated using MD5. The resulting hash value is then encrypted with the Dual RSA algorithm. The process of decrypting is the inverse process of encryption.

A set of connected computers using communication channels requires security for the exchange of information. This field of work involves a specialist in network security with the network administrator that prevents and monitors unauthorized access, modifies, and disables the use of the network. To combat this growing problem, security professionals are looking for better protection. Attacks have endangered security; hence, various symmetric and asymmetric encryption algorithms are provided to achieve the appropriate security services such as identity, confidentiality, integrity and availability. These algorithms are designed to provide security and authenticate users. To improve the strength of these security algorithms, Dubai et al. [Dubai, Mahesh and Ghosh (2011)] have developed a new security algorithm using both symmetric and asymmetric encryption methods. This algorithm provides three principles of cryptography: integrity, confidentiality, and identity. This algorithm is derived from the combination of ECDH, ECDSA, DUAL RSA algorithms and MD5 hash algorithms. This new security algorithm has been used for better security and integrity of the combination of symmetric and asymmetric encryption methods.

Wireless sensor networks consist of hundreds or thousands of low-cost, low-power and self-organized nodes that are highly distributed. Wireless sensor networks are growing and require effective security mechanisms, because sensor networks may interact with sensitive data. Cryptographic algorithms have a good role in information security systems. Currently, various types of cryptographic algorithms provide security in wireless sensor networks, but there are still some problems. At present, symmetric and asymmetric encryption methods can provide a level of security with some constraints. In Dhaliwal et al. [Dhaliwal and Soi (2015)], a new hybrid encryption algorithm is proposed to improve the power of these algorithms. The algorithm is designed using a combination of two symmetric and asymmetric encryption methods. The proposed algorithm is a cryptographic method composed of ECC and AES algorithms. RSA and Blowfish are used for authentication and MD5 for integrity. The results show that the proposed encryption algorithm performs better in terms of computation time and encrypted text size.

One of the goals of wireless sensor networks is to transmit trusted information from one node to another in the network. In the paper by Bhave et al. [Bhave and Jajoo (2014)], an enhanced encryption scheme of improved AES and ECC algorithms has been used to increase the security of wireless sensor networks. This paper analyzes the AES algorithm and the S-Box structure and provides an improved AES encryption algorithm. Using the AES algorithm, the message sent by the sender changes to completely new encrypted text so that the attacker cannot guess the recipient's original message. In this article for exploring purposes, plain text is given with 16 bytes and a key is considered and the algorithm is implemented.

Many key management schemes are provided in a wireless sensor network. Sensor nodes are provided with insufficient battery power, low memory, limited computing, and communication constraints. Energy in safe and efficient routing is a major issue for wireless sensor networks. SAERP is an approach in energy-efficient routing that is based on clustering model, which proposed for e-health and real-time communication protocols [Yaeghoobi, Tyagi, Soni et al. (2014)]. In the article by Sharmila et al. [Sharmila and Vijayalakshmi (2015)], the key management scheme consists of a public key encryption

scheme and a symmetric schema. The symmetric key is generated using the genetic algorithm. The initial entry for the genetic algorithm is the key generated by the HECC encryption. The design offers energy efficiency, flexibility against node capture attacks, and key refreshment between cluster heads and cluster nodes. The simulation results show that this hybrid scheme has more robustness, more energy-efficient, and smaller-sized keys.

Some sensors use Bluetooth technology to communicate in wireless sensor networks. In a paper by Ren et al. [Ren and Miao (2010)], a communication encryption algorithm based on DES and RSA is provided to enhance the security of data transmission in Bluetooth communication. Currently, the encryption algorithm used in Bluetooth protects the confidentiality of data during transmission between two or more devices, and a 128-bit symmetric encryption called E0. This encryption is broken down under certain conditions with the complexity of time O (264). In the proposed hybrid algorithm instead of E0 encryption, the DES algorithm is used for data transmission because it has higher efficiency in block encryption and uses the RSA algorithm to decrypt the DES key because it is superior to cryptographic key management. Under the protection of DES and RSA algorithms, the Bluetooth system is safer. It is clear that the whole encryption method is simple and efficient, and in addition, the confidentiality of the algorithm is high. Bluetooth features include wireless, short range and low power.

Rege et al. [Rege, Goenka, Bhutada et al. (2013)], a hybrid encryption algorithm is based on AES and RSA to increase the security of data transfer in Bluetooth communications. At present, the E0 algorithm is used to transfer information between two devices or more via Bluetooth. The combination of the encryption algorithm instead of E0 uses the AES algorithm, which has a great effect on block encryption, and uses the RSA algorithm to encrypt the AES key to exploit the key management benefits. Therefore, the use of AES and RSA algorithms makes it safer to transfer information in Bluetooth. In addition, the hybrid encryption algorithm is a convenient and easy way to encrypt data and enhance confidential.

Security is one of the most important and fundamental issues for transmitting data in wireless sensor networks. Hence, innovative hybrid encryption algorithms for security have been developed. DNA cryptography plays a vital role in the fields of communication and data transmission. In DNA encryption, the biological concept of DNA is used not only to store data and information carriers, but also to perform computations. In the paper by Monika et al. [Monika and Upadhyaya (2015)], computing security is provided using DNA based encryption. This paper presents an innovative algorithm that uses a DNA encryption and SSL protocol to provide a safer channel for the exchange of information in wireless sensor networks.

Encryption plays an important role in securing wireless sensor networks. In Rizk et al. [Rizk and Alkady (2015)], a new algorithm is comprised of symmetric and asymmetric encryption methods with a small security key. This algorithm guarantees three principles of cryptography: integrity, confidentiality and identity. The combination of ECC and AES encryption algorithms is provided. The XOR DUAL RSA algorithm is used to identify and MD5 for integrity. The results show that the hybrid algorithm presented in computational time, cipher text size, and high energy consumption. This algorithm is resistant to a variety of attacks.

With significant progress in cryptographic protocols, it has been seen that not all efficient

protocols were investigated for encrypting image. At present, existing approaches for image encryption still lacks robustness with respect to forward as well as backward secrecy. In Maniyath et al. [Maniyath and Thanikaiselvan (2019)] has been used the potential feature of public key cryptosystem. The proposed system utilizes elliptical curve cryptography for cost effective computation of secret keys required for performing encryption. The study outcome shows that proposed system offers better retention of signal quality as well as lower level of correlation in order to prove better imperceptible features in contrast to existing approaches.

In many applications like confidential video conferencing, medical imaging system, online personal photograph album security is very essential. Also, in industrial process wide usage of images can turn it into a resource and asset. So, it is important to protect confidential images data from unauthorized access. Shakthivel et al. [Sakthivel and Madhubala (2019)] present a secure cloud storage scheme based on hybrid cryptosystem, which consists of Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), and one-way hash function. Here, the data owner exports large volume of encrypted data to a cloud storage provider, the Electronic cryptography is a public key or asymmetric key means that the encryption key and decryption key are different. this paper proposes elliptical curve cryptography-based security mechanism and ant colony optimization based secured key management technique. The proposed system provides better space complexity than existing RSA and CRT, and the ACO improves optimality.

Security in the Wireless Sensor Network plays an important role and can be achieved by cryptographic algorithms. The cryptography is the science and art of transforming messages to make them secure and immune to attacks by authenticating the sender and receiver within the network. The Proposed methodology in the article by Perumal et al. [Perumal and Sundaram (2019)], hybrid cryptographic technique has combined Blowfish algorithm for symmetric and Elliptic Curve Diffie-Hellman algorithm for asymmetric. Blowfish algorithm provides high speed encryption process when compared with the other symmetric algorithms. The Elliptic Curve Diffie Hellman algorithm combines the concept of elliptic curve and Diffie-Hellman key exchange algorithm. Hence, it provides more security compared to other asymmetric algorithm and the key exchange mechanism. Cluster based trust Management approaches are used to identify unauthorized user in WSN. It first identifies the trusted nodes in networks, then send packets through that trusted nodes. Trusted nodes are identified based on trust values to identify the neighboring nodes during verification process for improving the Packet Delivery Ratio and Energy Consumption.

In Taha et al. [Taha, Elminaam and Hosny (2018)], they build a system that encrypts data transferred from the mobile cloud from a mobile phone to a cloud using five hybrid encryption methods. The proposed system demonstrates that the use of hybrid algorithms increases the level of encryption of encrypted mobile data and also reduces the time required for encryption and decryption. Firstly, hybrid cryptography algorithm presents a variety of different encrypting algorithms that allow the user to choose the encrypting method which is suitable with his own type of data. Secondly, the hybrid cryptography algorithm improves the performance of the encryption algorithms, since it encrypts the data in a minimum time and in a secure way. Thirdly, the proposed hybrid cryptography algorithm allows the users to send and receive data in a secure way without facing the

problem of attacking data. Fourthly, the encryption times for encrypting a file with size 1 MB using difference hybrid algorithms come in the following ascending order: using Triple DES and Krishna hybrid algorithm, using AES and Krishna hybrid algorithm, using Triple DES and RSA hybrid algorithm and using Blowfish and Krishna hybrid algorithm. Fifthly, the proposed hybrid cryptography algorithm proves that merging the three encrypting algorithms AES, Blowfish and Krishna to have AES and Blowfish and Krishna hybrid algorithm increases the security level and also saves the encryption time.

Wireless Sensor Networks have rapidly grown in recent years. However, with the rapid growth in the WSNs technology, the threat of deploying the technology without the required security has been a major issue facing a lot of facilities; thus, comes the need for improving the security systems for the WSN. Abdullah et al. [Abdullah, Houssein and Zayed (2018)] proposed a hybrid security protocol for WSN. The proposed hybrid algorithm combines characteristics of the public key cryptography which comes with ease of distributing the key and symmetric cryptography which is easier to calculate and faster. That provides a good and a fast way of securing information transmission. Comparing the proposed hybrid algorithm to several other algorithms has proven that the proposed hybrid algorithm obtains the best results overall.

In Bhat et al. [Bhat and Kapoor (2019)], a hybrid model is proposed which offers excessive security with lessened key maintenance and encryption time using amalgamation of both symmetric and asymmetric cryptographic techniques. In this hybrid model, to achieve the embryonic security services as integrity, confidentiality and authentication by encompassing message digest, symmetric encryption and digital signature, respectively, a digital envelope is also included which comprises all of this to transfer them firmly over the network.

Data or information is the most valuable asset for the modern electronic communication system. To secure data or information has become a challenge in this competitive world. There are many techniques for securing data or information such as cryptography, steganography and etc. In Biswas et al. [Biswas, Gupta and Haque (2019)], hybrid cryptography has been applied using AES and RSA. In this hybrid cryptography, the symmetric key used for message encryption is also encrypted, which ensures a better security. An additional feature of this paper is to create a digital signature by encrypting the hash value of message. At the receiving side this digital signature is used for integrity checking. Then the encrypted message, encrypted symmetric key and encrypted digest are combined together to form a complete message. This complete message again has been secured using the steganography method. Message integrity checking is a special feature of this algorithm.

Cloud Computing is used in many areas to store large amount of data securely. Some of the areas use cloud to store their confidential data. But whichever the area is, security of data would be the prominent entity. Cryptography is the best technique to store and retrieve data efficiently and securely. Using single algorithm will not contribute highly for greater level security of data in cloud. In Abhishek et al. [Abhishek, Ashwij, Harisha et al. (2019)], they have introduced a better security mechanism using symmetric key cryptography algorithms. In this proposed system AES and blowfish algorithms are implemented to provide block wise security to data. Key size of both the algorithms is 128 bits. File will be split into four parts. Each and every part is encrypted using AES and blowfish algorithms

alternatively. All parts are encrypted simultaneously due to multithreading. The same technique is applied in reverse for file decryption. Integrity of data in the file will not be lost after the decryption process.

Cryptography is an art to manipulate a private message, especially for state security. By combining symmetric cryptography and asymmetric cryptography, the security of the hybrid algorithm will increase. Ristiana [Ristiana (2019)] provide the development of combination between one-time pad cryptography and RSA cryptography. The result shows that there are three steps to use this algorithm. First, both of RSA key are generated by the receiver and the receiver give the public key to the sender. Then, the sender encrypts the private message and send it to the receiver. Finally, the receiver decrypts the message. This algorithm will cover the weakness of one-time pad cryptography by RSA cryptography. Therefore, we can say that the security of this algorithm is guaranteed.

Nodes in the wireless sensor networks have limited battery power and deployed to run few days. In general, sensor nodes are placed at very complicated locations; therefore, charging or replacement of nodes battery is very difficult. Hence, it is highly unfavorable to use the complex data security method. The main objective of Prakash et al. [Prakash and Rajput (2018)] is to develop an enhanced algorithm to provide secure data communication as well as to enhance the lifetime of the WSNs. As in symmetric approach the key sharing was a major issue, they have performed the key generation using ECC algorithm which is an asymmetric key algorithm, and using this key, they will encrypt and decrypt data using AES which is a symmetric key algorithm. Hence, they have developed an enhanced algorithm which exploits the advantages of the two algorithms. The proposed algorithm, which reduces complexity as compared with ECC, issued only for key generation and not for data encryption or decryption and it is more secure than AES as it has solved the problem of key sharing in AES.

A complete and secure encryption system must establish three principles of confidentiality, authentication and integrity. An encryption algorithm alone cannot provide all the principles of encryption. A hybrid encryption algorithm, consisting of symmetric and asymmetric encryption algorithms, provides complete security for a cryptographic system. The article by Ebadati et al. [Ebadati, Eshghi and Zamani (2019)] reviewed papers presented in this area over the last few years.

Information security is more important for data communication in physical or network environment. Protected communication is more imperative for data move in the network. In Jain et al. [Jain and Kapoor (2017)], hybrid cryptography is a permutation of Message digest and Symmetric Key cryptography algorithm in the form of Digital Envelope. The message is initially encrypted with AES and the symmetric keys of AES are encrypted with RSA then the hybrid of both AES-RSA is embedded with message digest of data.

The security techniques, today the most widespread, and based on coding algorithms. the encryption operations perform by using digital calculations. Abdullah et al. [Abdullah and Khaleefah (2017)], produce hybrid text encryption algorithm based on chaos and image steganography algorithm based on secret sharing, and chaos. In a novel symmetric algorithm: Firstly, encrypt and decrypt a secret text message. Then, sharing the cipher secret text to multiple shadow based on secret sharing scheme. Finally, embedding the shadow with multi images cover. With numerical simulation results for text encryption, the

proposed algorithm presents high level of security, increase key size and an excellent time for encryption.

3 Proposed method

The purpose of this research is to develop it as an applied research. Initial information on wireless sensor networks, functions and security has been collected, studied and presented. Articles focusing on the operation of wireless sensor networks in the transmission of energy and enhancing the security of data transmission using a combination of encryption algorithms were developed and presented. Familiarity with the latest actions taken in the field of cryptography and diagnostic information in the area of energy transfer. In order to implement the solutions, several articles with the most recent release date were carefully reviewed at the level of implementation details. Throughout the description, details of the implementation of some of the cryptographic algorithms as well as how to combine them together to provide three principles of cryptography including integrity, confidentiality, and authentication were introduced. Some articles in the implementation area have not been fully implemented and only one has provided a hybrid algorithm. In the implementation of some of the algorithms, there were some limitations that arise from the definition of those algorithms. According to the studies, the lack of a hybrid cryptographic algorithm for transmitting diagnostic information in wireless sensor networks was considered to monitor and enhance the security of energy transmission pipelines, in such a way that three principles of cryptography include integrity, confidentiality and authentication Coverage, as well as the possibility of its operational implementation. Each of the examined algorithms fulfilled a part of the security needs, therefore, a comprehensive roadmap for increasing the security of data transfer using past studies is formulated and a general overview of the process of doing the work is determined. The algorithm presented with other algorithms in other articles is compared in terms of efficiency, implementation, security and the three principles of confidentiality, authentication and integrity, and the final result and relative advantages of the proposed algorithm are revealed.

The steps involved in the task of identifying diagnostic information in the energy transfer pipeline, encoding, blocking, confidentiality, authentication, integrity and decryption are briefly outlined below:

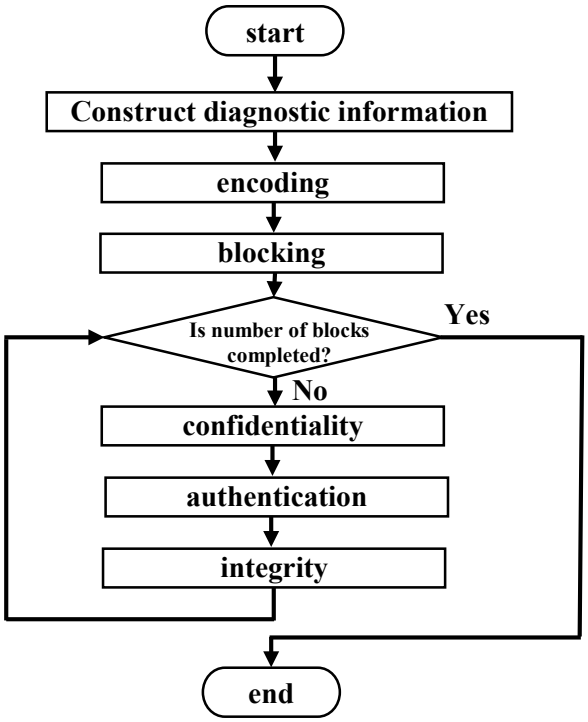

Figure 1: Outline of the proposed algorithm

Diagnostic information includes pipeline information such as temperature, humidity, pressure, etc. This information is used in leak detection and sabotage methods. Some other sensor information includes model, power consumption, battery level and etc. This information is sent to verify the correct operation of the network and security. This information is provided in the format of a numeric string or character before being sent. Some wireless sensors are capable of detecting several parameters of the information string, while others are only capable of detecting only one parameter in a specialized manner. In a monitoring system, a set of wireless sensors work in tandem with each other and sends intelligence fields made from the measured parameters. In sensors capable of sending multiple parameters, and sensors which, in addition to the main task, are responsible for the data transmission and data compilation, as well as the requirement for transmitting sensor status information along with diagnostic information, combining the parameters together is required. The sensor after the measurement produces data and stores it in memory. The information is read and forwarded at the appointed time for sending from memory. To maintain memory information, a specific structure must be developed. Encoding is the process of converting a string of characters, such as letters, numbers and symbols into specific formats for optimal transfer or storage. Decoding the inverse process is encoded and converted into a coded format to the original character sequence. Encoding and decoding are applied in data communications, networking, and data storage. Their main application in radio communication systems (wireless) is very evident. In wireless sensor networks, there is a constraint on the use of energy resources. Most energy is consumed by sensors when transmitting data. Therefore, it is important to select a coding

system that produces the lowest bit-signal in an optimal way. The greater number of sensor connections with the network is to make the packet transmissions less efficient and optimized, the performance of the sensor battery will be more optimal. In telecommunications, a block of bits is encoded and transmitted as a unit in the communication context. A block is a string of records, words, or unit characters for achieving technical and logical goals. The blocks are separated from each other and have a block end signal and one or more information records. Usually, processes are performed on information blocks.

A block transfer, the coordinated sequence of activities between users and the transmission platform for the transfer of a unique block from a specified source to a specified destination. Blocks pass through user interfaces and transmissions. An attempt is made to transfer a block successfully or fail. A successful transfer is a true and non-recurring transfer between the source and the destination. If all blocks for a given data are successfully transferred, all data sent to the destination will be available. The transfer time and the transfer bed quality are effective in the success of the transfer of blocks.

The block size, maximum length of the block and the blocking is the process of placing the data in the blocks. Blocked information is usually read and written in a buffer and several blocks at a time. Blocking reduces data transfer overhead and makes data management easier and faster. The size of most blocked files is not a multiple of the size of the physical block on the hardware, which leads to inefficiencies in the use of storage space. To fix the problem, most of the final block is left blank or filled with specific bits.

The string information generated by the sensors after the encoding should be blocked for transmission in the wireless communication platform. The formula $L(B) = \left\lfloor \frac{L(S)}{n(B)} \right\rfloor + 1$ is used so that L (B) is the length of the block, L (S) is the length of the encoded string and n (B) Are the number of blocks. The length of each block is 256 bits. If n (B) is not an integer, then the sequence of bits 0 is used to complete the final block. The blocks are divided into two equal parts, and for each section of confidentiality, authentication and integrity are established. The reason for dividing blocks into two parts is increasing confidentiality by using two different algorithms. The general scheme of the proposed algorithm is as follows:

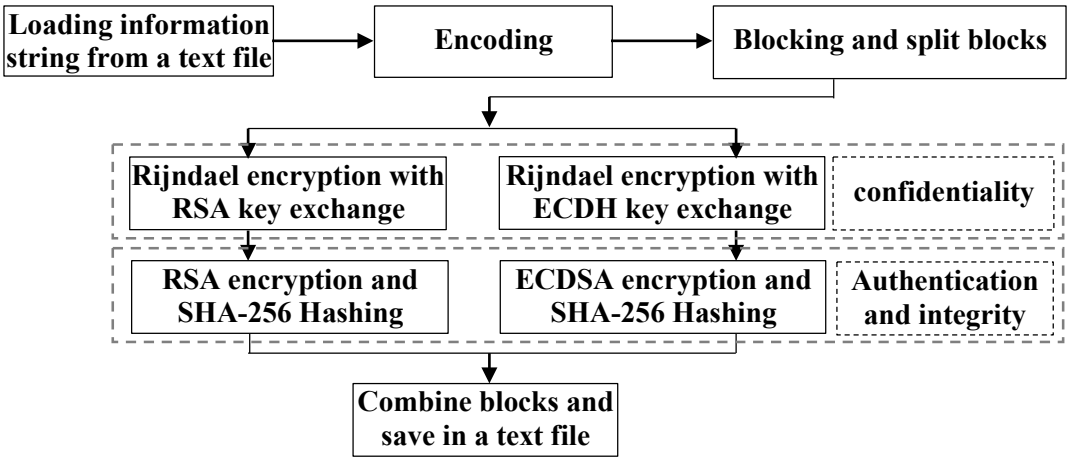

Figure 2: The general scheme of the proposed algorithm

4 Pseudocode

The workflow offers a number of factors that affect implementation, including implementation complexity, implementation with C# programming language, maximum utilization of .NET framework libraries, implementation constraints, comprehensiveness and performance, and several pseudocodes. At the end of the pseudocode integration and the necessary modifications, the final code is prepared so that the syntax and semantic structure of the code is in accordance with the host compiler's instructions and fulfills the intended purpose. The proposed algorithm is implemented using Visual Studio software development environment, C# programming language and .NET library. The algorithm is implemented on a home computer with medium hardware resources. The Pseudocodes are as follows:

Algorithm 1. Loading information string from a text file

```
1. string plaintext = read (string TextFilePath);
```

Algorithm 2. Encoding

```
1.   binary[] encodedText;
2.   for (int i=1; i<= (plaintext.Length)-1; i++)
2.1.      {
2.2.      Assume new node z;
2.3.      Z_left = X = Min(plaintext);
2.4.      Z_right = Y = Min(plaintext);
2.5.      Z_prop = X_prop+Y_prop;
2.6.      Insert Z into encodedText;
2.7.      };
```

Algorithm 3. Blocking and split blocks

```
1.   binary blockedText[] = encodedText;
2.   int padding = (encodedText.Length) mod 256;
3.   if (padding != 0)
```

3.1. {
3.2. binary paddedBits[256-padding]=0;
3.3. Append paddedBits to blockedText;
3.4. };
4. int blockCount = (blockedText.Length)/256;
5. binary blockedText1[(blockCount/2) * 256];
6. binary blockedText2[(blockCount-(blockCount/2)) * 256];
7. Copy blockedText from 0 to blockedText1.Length index into blockedText1;
8. Copy blockedText from blockedText1.Length+1 to blockedText.Length index into blockedText2;

Algorithm 4. Rijndael encryption

1. binary[] resultBlock = inputBlock;
2. for(n=1; n<=14; n++)
2.1. {
2.2. binary[] extendedKey;
2.3. binary block[];
2.4. resultBlock=extendedKey+resultBlock;
2.5. S-Box$_n$(resultBlock);
2.6. Shift$_n$(resultBlock);
2.7. if(n != 14)
2.7.1. {
2.7.2. MixColumn$_n$(resultBlock);
2.7.3. };
2.8. };

Algorithm 5. ECDH

1. int d_A,Q_A,d_B,Q_B; //domain parameters of an elliptic curve
2. int K=(x_K,y_K)=d_A×Q_B;
3. int L=(x_L,y_L)=d_B×Q_A;
4. int keyForRijndael=x_K;

Algorithm 6. RSA

1. int p,q; //p and q are prime numbers
2. int n=p×q;
3. int lmbda(n)=LCM(p-1, q-1);
4. find e where GCD(e, lmbda(n))=1;
5. int d=e^{-1} mod lmbda(n);
6. (n, e) is private Key;
7. (n, d) is public Key;

Algorithm 7. OAEP padding

1. int M; //Message
2. int r; //random k_0 bit

3. int X=M00 ... 0 ⊕ G(r);
4. int Y=r ⊕ H(X);
5. int m=X+Y;

Algorithm 8. ECDSA

1. int e=Hash (m);
2. int k//chosen from 1 to n-1.
3. $(x_1, y_1)=k\times G$; //K and G are domain parameters of an elliptic curve
4. $r=x_1 \bmod n$;
5. if (r=0)

5.1. Goto step 2;

6. int $s=k^{-1} (e+d_A r) \bmod n$;
7. if (s=0)

7.1. Goto step 2;

8. a pair (r, s) is a digital signature;

Algorithm 9. RSA signature

1. int R=hash(m);
2. $R^d \bmod n$ is a digital signature;

The general scheme of the Pseudocode is as follows:

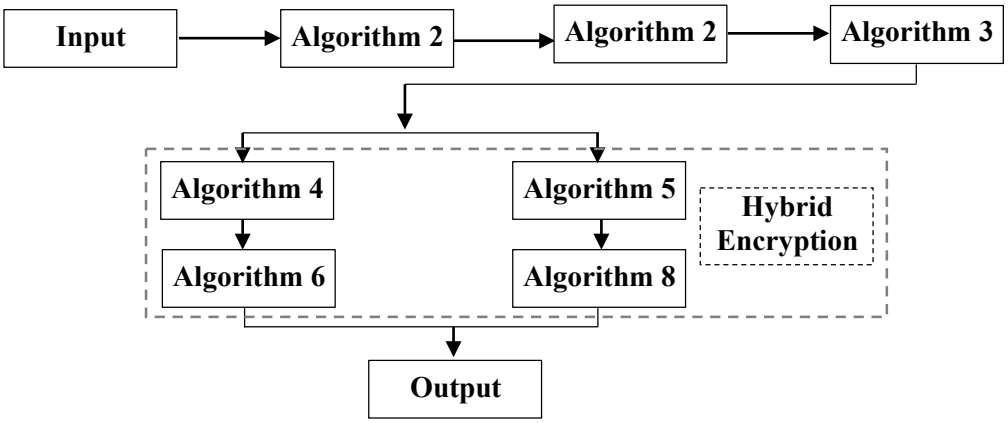

Figure 3: The general scheme of the proposed algorithm

5 Comparison

In the proposed algorithm, the advantages of symmetric and asymmetric encryption algorithms are combined to establish the three principles of confidentiality, authentication and integrity. Correspondingly, the limits of wireless sensor networks are considered in the exchange and transfer of information. The cryptographic process is performed using the Rijndael algorithm with 256-bit blocks. Rijndael algorithm is a high-speed symmetric encryption algorithm and variation in implementation. Based on kerckhoffs's principle, the

security of a cryptographic system depends on maintaining the confidentiality of the encryption key. In the proposed algorithm, the encryption key required by the Rijndael algorithm is provided in two ways. The reason for doing this is to increase the security of the key exchange in the wireless network. If the encryption key is identified for some of the blocks of information, since the key exchange process of the other information blocks is different, it will not be possible for the attacker to recover all information. Due to computational constraints on sensors, two principles of authentication and integration have been attempted in the form of a process so that their digital signatures also provide some kind of integration of the encryption system. Some of the features are tailored to the limitations of the benefits of the proposed algorithm. Some of them are referred to:

1. Using a variable length encoding system
2. Blocking with larger size
3. Using symmetric cryptography
4. Use asymmetric cryptography for key exchange
5. Use of two asymmetric encryption algorithms
6. Combining processes for authentication and integration
7. Using the SHA-256 hash algorithm
8. Implement a hybrid cryptographic system

5.1 Time complexity

The time complexity of an algorithm is the quantity that represents the amount of time consumed to run that algorithm as a function of the input string size. The time complexity of an algorithm is usually expressed by a large O that overlooks the lower-order coefficients and phrases. This display method is an asymptotic description of the complexity of time. For example, if the time needed to run an algorithm for all inputs $n>n_0$ is equal to an^3+bn, the asymptotic time complexity is equal to $O(n^3)$. a, b and n_0 are constant values. The complexity of the time is estimated by counting the number of main operations of the algorithm.

The proposed hybrid encryption algorithm consists of an encoding algorithm, a symmetric encryption algorithm, two asymmetric encryption algorithms for key exchange and two algorithms for authentication and integrity. The time complexity of Huffman's algorithm is O(nlogn). A stack is used to store the weight of each node. The complexity of the time is to determine the lowest weight and add new weight O(logn) and the time complexity of the cycles O(n). Rijndael's algorithm consists of 14 rounds and four distinct operations per round. Operations are all of a mapping type by a predefined table or a linear operation, resulting in a time complexity of O(14n). The time complexity of the elliptic curve encryption algorithm is equal to $O(\sqrt{n})$ and the time complexity of the RSA algorithm is $O(\log n^2)$. The OAEP padding performs actions to replace information blocks by linear operators. As a result, the complexity of the RSA algorithm with OAEP padding is $O(n+\log n^2)$. The SHA-256 hash algorithm also performs several steps to replace information blocks by linear tables and operators, resulting in the O(n) complexity of time. For both authentication and integrity algorithms, the complexity of the elliptic curve encryption time, the RSA, and the SHA-256 hash algorithm are specified, and the

remaining operations are linear and do not affect the complexity of the time, because their grades are in the degree of other operations affecting the algorithm is less. Other operations, such as dividing the information string into two categories, blocking, padding with 0, etc., are all constant, therefore, their complexity is equal to O(k), so that k is the fixed number of the input string function. In general, the complexity of the entire algorithm is equal to O(nlogn). The following table shows the results:

Table 1: Different blocking methods for hypothetical information

Algorithm	Time complexity
Huffman	O(nlogn)
Determine the lowest weight and add new weight	O(logn)
Cycles	O(n)
Rijndael	O(14n)
Elliptic Curve Encryption	O(√n)
RSA	$O(\log n^2)$
RSA with OAEP padding	$O(n+\log n^2)$
SHA-256	O(n)
Dividing, Blocking and Padding	O(k)
Result	O(nlogn)

The proposed algorithm has a good time complexity compared with other proposed algorithms in recent years. While the proposed algorithm is more secure than other hybrid algorithms provided on the communication platform of wireless sensor networks, it fully enforces the three principles of confidentiality, authentication and integrity.

5.2 Memory consumption

The hypothetical information string is as follows:

Internal Temperature: 284.15,External Temperature: 283.15,Environmental Temperature: 282.15¬Absolute Humidity: 15,Relative humidity: 50,Specific humidity: 8¬Internal Pressure: 250,Environmental Pressure: 760¬Environmental Luminosity: 100¬GyroscopeX: 0,GyroscopeY: 0,GyroscopeZ: 0¬AccelerometerX: 0,AccelerometerY: 0,AccelerometerZ: 9.8¬ Longitude: 35.703980,Latitude: 51.426650,Date and Time: 2017-04-01-04-21,Battery Level: 70,Sensor ID: 436647¬¶Motion Detection: 0¬Object Distance: 3-35,2-110,7-50¬Longitude: 35.703981,Latitude: 51.426651,Date and Time: 2017-04-01-04-22,Battery Level: 80,Sensor ID: 436648¬¶Frequency: 2.4,Period: 0.42,Wavelength: 96,Amplitude: 16,Propagation Velocity: 230¬Longitude: 35.703982,Latitude: 51.426652,Date and Time: 2017-04-01-04-23,Battery Level: 70,Sensor ID: 436649¬¶Magnetic Field Strength: 31.869¬Longitude: 35.703983,Latitude: 51.426653,Date and Time: 2017-04-01-04-24,Battery Level: 80,Sensor ID: 436650¬¶•

The hypothetical information string has 946 characters, and an ASCII encoding system needs to store 946 bytes or 7568 bits of space in the physical memory. However, in the proposed algorithm, the final file needs 619 bytes or 4952 bits of space for storage in

physical memory. The proposed algorithm has a variable-length encoding system, and in this string of information, about 35% of the memory consumption is saved.

In the table below, the number of information blocks for transmission in a wireless sensor network is compared in several blocking methods for the hypotheses string:

Table 2: Different blocking methods for hypothetical information

Blocking Method	Block size	Padding bits	Number of Blocks
64-bit	64	48	119
128-bit	128	112	60
256-bit	256	112	30
Proposed method	256	168	20

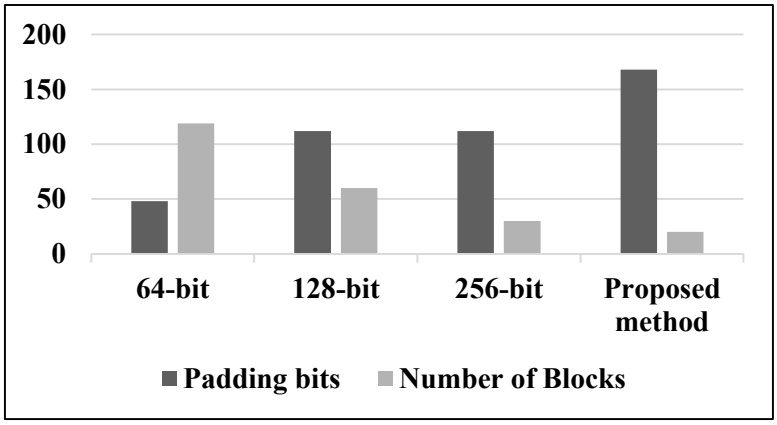

Figure 4: Different blocking method chart for hypothetical information

The number of transition blocks in the proposed algorithm is lower than in other blocking methods. Typically, the DES encryption algorithm contains 64-bit blocks, the AES encryption algorithm has 128-bit blocks, and the Rijndael encryption algorithm has 256-bit blocks. By increasing the size of the blocks, the probability of increasing the number of layers of bits in the final block increases, which only affects the final block, and its number is entirely dependent on the length of the information string. The table above is achieved without regard for integrity and authentication, and it only considers the enclosed blocks of information to be transmitted. The hash algorithms and digital signatures also create additional information blocks to encrypted information blocks and transfer them to the wireless communication platform for integrity and authentication purposes. In the following table, several blocking methods in combination with the hash algorithms and the number of final blocks for transmission of the encrypted information string are specified:

Table 3: Different blocking methods with hash algorithm for hypothetical information

Blocking Method	Hash Algorithm	Number of Final Blocks
64-bit	MD5	238
64-bit	SHA1	417
64-bit	SHA-256	595
128-bit	MD5	90
128-bit	SHA1	135
128-bit	SHA-256	180
256-bit	MD5	38
256-bit	SHA1	49
256-bit	SHA-256	60
Proposed method	SHA-256	40

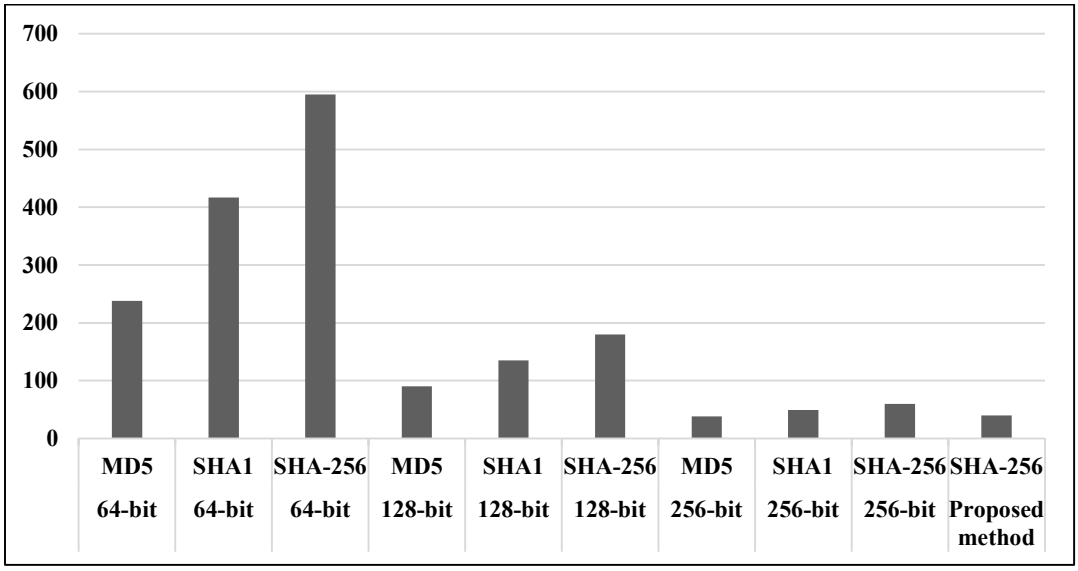

Figure 5: Different blocking method chart with hash algorithm for hypothetical information

Because the length of the final information string in the hybrid method for authentication and integrity is only dependent on the hash algorithm, only the hash algorithms are defined in the table above. The number of blocks in the 256-bit blocking methods with the MD5 and SHA1 hash algorithms is lower than the proposed algorithm. The MD5 algorithm is currently broken and the SHA1 algorithm is broken in certain conditions. As a result, they will not be a good choice in terms of security. The number of rounds in the standard structure of the MD5 hash has been 64 and the number of rounds in the standard structure of the SHA1 algorithm is 80. While the number of rounds in the standard structure of the SHA-256 algorithm is equal to MD5, 64. As a result, the SHA-256 algorithm provides

higher security than the MD5 algorithm with the same complexity of MD5. The following table provides some differences between hash algorithms:

Table 4: Compare hashing algorithms

Hash algorithm	Size of the output blocks	Rounds	Publication year
MD5	128	64	1992
SHA1	160	80	1995
SHA-256	256	64	2001

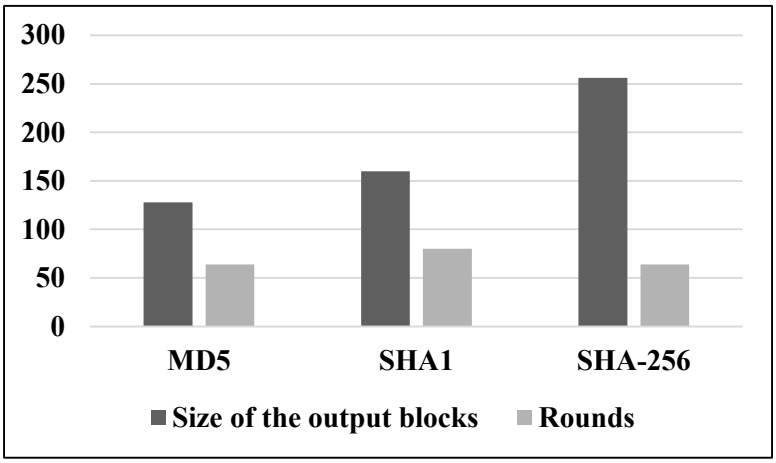

Figure 6: Comparison chart of hash algorithms

The proposed algorithm provides three principles of cryptography: confidentiality, integrity, and authentication with the optimal number of blocks of information.

5.3 Computing time

The proposed algorithm consists of the steps for reading the information file, encoding, blocking, dividing the information blocks into two groups, encrypting the first group of information blocks and generating the corresponding digital signature, and encrypting the second group of information blocks and generating the corresponding digital signature. In ten times the implementation of the algorithm, the measured consumption times are shown in the table below:

Table 5: Results of ten times implementation of the proposed algorithm

Implementation	Reading information	Encoding	Blocking	Split blocks	First encryption	Second encryption	Total

1	0.1607	2.604	0.0651	0.002	1051.8134	228.1939	1282.1839
2	0.1964	2.638	0.1299	0.002	1008.6186	262.3184	1273.903
3	0.2155	2.9789	0.0815	0.002	999.9926	218.898	1222.169
4	0.1867	3.2007	0.1243	0.0023	1233.434	237.5791	1474.527
5	0.2031	2.5375	0.0584	0.002	1189.3881	230.941	1423.13
6	0.2065	2.347	0.0678	0.0016	1121.734	231.514	1355.871
7	0.1897	2.5228	0.0598	0.0016	1108.2271	233.5025	1344.504
8	0.1938	2.0085	0.0972	0.009	1090.7894	232.4102	1325.508
9	0.2008	2.7269	0.0621	0.002	1074.1448	241.9184	1319.055
10	0.2028	2.4984	0.0604	0.001	1114.9746	241.8051	1359.542
Average	0.1956	2.60627	0.08065	0.00255	1099.3117	235.9081	1338.105

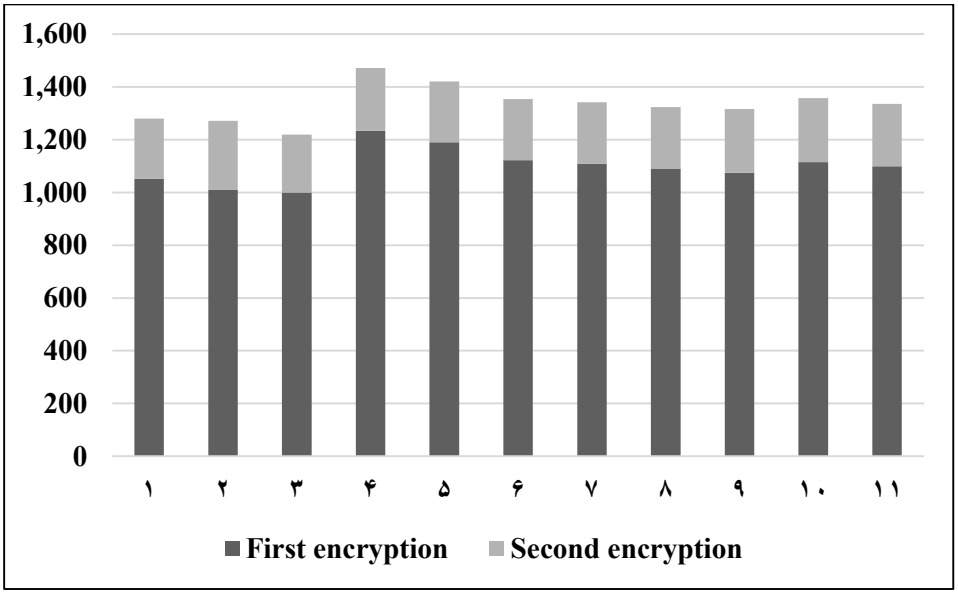

Figure 7: Chart of results of ten times implementation of the proposed algorithm

The unit of measurement for the time consumed in each step is based on milliseconds. The first and second encryption steps take most time to execute the algorithm. As a result, only two of most influential factors are considered in the above diagram. The RSA algorithm uses longer time to encrypt longer strings than ECC algorithm. Naturally, there is a direct relationship between the increased security of data transmission and the time consumed. In the proposed algorithm, there is a balance between the time consumed and the increased security of data transmission, so that the cryptographic key for half the information is rapidly distributed, and half of the information is distributed securely. The distribution of the encryption key in two ways has also helped to increase the security of the proposed algorithm.

6 Conclusion and future work

Energy transmission pipelines considered important in oil and gas industry. Transmission pipelines are economically feasible, flexible, fully automated, and automatic loading and unloading operations are carried out. As a result of reduced costs, this method is very suitable for the transportation of liquid products. Access to sustainable energy is one of the developmental requirements. Therefore, countries suffer a great deal of energy production and transmission. Any failure or sabotage in the production or transfer of energy can jeopardize the function of affiliated industries. War, internal disputes, legal problems, social inequalities, etc. The underlying causes of vandalism and wear out of transmission lines, lack of proper design, human error and etc. are the cause of failure. Therefore, centralized monitoring of the energy transmission pipelines is critical. Energy transmission pipelines are vulnerable to various accidents and acts of vandalism. Therefore, a reliable monitoring system is needed to secure the transmission lines. A comprehensive and optimized solution for reliable data and secure, fast and timely data transmission is the use of wireless sensor networks. Wireless sensor network technology has been gaining great importance over the years, due to the advancement of technologies associated with this technology such as the ability to measure, communicate protocols, processor speeds, embedded systems, and more. These developments gradually affect oil and gas industries in order to automate the processes, system capability and control. The use of sensors is of strategic importance for reasons such as business intelligence, competitive advantage, time-to-market, quality and reliability standards in the industries associated with the transfer of liquids and gases, especially oil and gas. Wireless sensor networks are new technologies that are used for various purposes, including monitoring power transmission pipelines. The structure and operation of wireless sensor networks and sensors were monitored for energy transmission pipelines. Wireless sensor networks are vulnerable to various attacks in different layers. Cryptography is one of the methods for secure transmission of information between sensors in wireless sensor networks. A complete and secure encryption system must establish three principles of confidentiality, authentication and integrity. Confidentiality in sensor networks is the ability to hide messages from an attacker. Integrity is the ability to detect unread or unrecognized messages. Authentication is the reliability of the message's origin. Cryptography is a knowledge of hiding information and verification, and includes protocols, algorithms and secure strategies to prevent unauthorized access to critical information. Encryption provides a mechanism for verifying the components of a connection. An encryption algorithm alone cannot provide all of the principles of encryption. A hybrid encryption algorithm, consisting of symmetric and asymmetric encryption algorithms, provides complete security for a cryptographic system. The papers presented in this area over the past few years and a new secure algorithm are presented that provide three cryptographic principles. The proposed algorithm is presented with regard to the limitations of wireless sensor networks. The proposed algorithm is compared with other algorithms presented in recent years, as well as its power, security, and advantages over other algorithms. The proposed algorithm has optimum time complexity, time and memory usage. The details of the algorithm and basic concepts are presented in such a way that it is possible to implement the algorithm operationally. At the end, suggestions were made for future work.

Many advantages of the proposed algorithm are presented. Computer science is very broad and covers a variety of topics. There are many ideas to improve the performance of hybrid encryption algorithms in securing the transmission of data between sensors in wireless sensor networks. Some of them can be the basis for future research. The use of compression algorithms reduces the amount of memory usage and the number of transition blocks in the communication platform of the wireless sensor network. Compression algorithms have complex operations that use sensor processing resources. Hence, the use of a compression algorithm commensurate with the limits of wireless sensor networks helps to improve the performance of a hybrid encryption system.

Most file systems are blocks that come from host hardware. In many cases, the size of the information string is not a factor of physical hardware blocks. In the proposed algorithm, padding was used to solve this problem. Some new file systems like BtrFS and ZFS do not have such problems or minimize the severity of the problem with methods. The possibility of implementing these file systems on the hardware of the sensors should be investigated. For authentication and integrity in a cryptographic system, methods like HMAC also exist. You should check the performance of these methods on wireless sensor networks. A high security encryption system is also used for wireless sensor networks in other networks. As a result, modifying and improving algorithms helps to provide more security in monitoring systems.

Conflicts of Interest: I hereby declare that there is no conflict of interest related to this manuscript (article) entitled "Fusion of Medical Images in Wavelet Domain: A Hybrid Implementation" with manuscript id: "CMES-8459 Proof".

References

Abdullah, K.; Houssein, E. H.; Zayed, H. H. (2018): New security protocol using hybrid cryptography algorithm for WSN. *1st International Conference on Computer Applications & Information Security*, pp. 1-6.

Abdullah, M. Z.; Khaleefah, Z. J. (2017): Design and implement of a hybrid cryptography textual system. *International Conference on Engineering and Technology*, pp. 1-6.

Abhishek, H. M.; Ashwij, A.; Harisha; Amol (2019): Data security in cloud using hybrid cryptography algorithms. *International Journal for Research in Applied Science and Engineering Technology*, vol. 7, pp. 55-57.

Bhat, S.; Kapoor, V. (2019): Secure and efficient data privacy, authentication and integrity schemes using hybrid cryptography. *International Conference on Advanced Computing Networking and Informatics*, pp. 279-285.

Bhave, A.; Jajoo, S. R. (2014): Secure communication in wireless sensor network using symmetric and asymmetric hybrid encryption scheme. *International Journal of Innovative Science Engineering and Technology*, vol. 1, no. 4, pp. 382-385.

Biswas, C.; Gupta, U. D.; Haque, M. M. (2019): An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography. *International Conference on Electrical, Computer and Communication Engineering*, pp. 1-5.

Brindha, K.; Ramya, G.; Jayantila, R. A. (2013): Secured data transfer in wireless networks using hybrid cryptography. *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 10, pp. 379-381.

Dawahdeh, Z. E.; Yaakob, S. N.; Razif bin Othman, R. (2018): A new image encryption technique combining elliptic curve cryptosystem with hill cipher. *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 349-455.

Dhaliwal, B. S.; Soi, V. (2015): Reprogramming of wireless sensor network securely with new hybrid encryption scheme. *International Journal of Engineering, Technology, Management and Applied Sciences*, vol. 3, no. 4, pp. 258-263.

Dubai, M. J.; Mahesh, T. R.; Ghosh, P. A. (2011): Design of new security algorithm: using hybrid Cryptography architecture. *3rd International Conference of Electronics Computer Technology*, vol. 5, pp. 99-101.

Ebadati E, O. M.; Eshghi, F.; Zamani, A. (2019): Security enhancement of wireless sensor networks: a hybrid efficient encryption algorithm approach. *Journal of Information Systems and Telecommunication*, vol. 23, pp. 180-192.

Jain, A.; Kapoor, V. (2017): Novel hybrid cryptography for confidentiality, integrity, authentication. *International Journal of Computer Applications*, vol. 171, pp. 35-40.

Maniyath, S. R.; Thanikaiselvan, V. (2019): Robust and lightweight image encryption approach using public key cryptosystem. *Computer Science On-line Conference*, pp. 63-73.

Poriye, M.; Upadhyaya, S. (2015): Secu re communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks. *Procedia Computer Science*, vol. 70, pp. 808-813.

Panda, M. (2014): Security in wireless sensor networks using cryptographic techniques. *American Journal of Engineering Research*, vol. 3, no. 1, pp. 50-56.

Patel, G. R.; Panchal, K. (2014): Hybrid encryption algorithm. *International Journal of Engineering Development and Research*, vol. 2, no. 2, pp. 2064-2070.

Perumal, P. K.; Al-Khalidi, S. Q. Y. (2014): Hybrid encryption/decryption technique using new public key and symmetric key algorithm. *International Journal of Information and Computer Security*, vol. 19, no. 2, pp. 1-13.

Perumal, V.; Sundaram, K. M. (2019): Cluster based secured data transmission using hybrid cryptography techniques in wireless sensor network. *International Journal of Computer Sciences and Engineering*, vol. 7, pp. 1271-1276.

Prakash, S.; Rajput, A. (2018): Hybrid cryptography for secure data communication in wireless sensor networks. *Ambient Communications and Computer Systems*, pp. 589-599.

Rege, K.; Goenka, N.; Bhutada, P.; Mane, S. (2013): Bluetooth communication using hybrid encryption algorithm based on AES and RSA. *International Journal of Computer Applications*, vol. 71, no. 22, pp. 10-13.

Ren, W.; Miao, Z. (2010): A hybrid encryption algorithm based on DES and RSA in bluetooth communication. *Second International Conference of Modeling, Simulation and Visualization Methods*, pp. 221-225.

Ristiana, M. G. B (2019): *Hybrid Algorithm of RSA and One-Time Pad Cryptography (Ph.D. Thesis)*, Universitas Pendidikan Indonesia.

Rizk, R.; Alkady, Y. (2015): Two-phase hybrid cryptography algorithm for wireless sensor networks. *Journal of Electrical Systems and Information Technology*, vol. 2, no. 3, pp. 296-313.

Sakthivel, G.; Madhubala, P. (2019): Hybrid elliptic curve cryptography for secured cloud computing. *International Journal of Computer Sciences and Engineering*, vol. 7, pp. 707-719.

Shahryar, T.; Fathi, M. H.; Sekhavat, Y. A. (2017): An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. *Signal Processing*, vol. 141, pp. 217-227.

Shankar, M.; Akshaya, P. (2014): Hybrid cryptographic technique using RSA algorithm and scheduling concepts. *International Journal of Network Security & Its Applications*, vol. 6, no. 6, pp. 39-48.

Sharmila, R.; Vijayalakshmi, V. (2015): Hybrid key management scheme for wireless sensor networks. *International Journal of Security and Its Applications*, vol. 9, no. 11, pp. 125-132.

Singh, L. D.; Singh, K. M. (2015a): Image encryption using elliptic curve cryptography. *Procedia Computer Science*, vol. 54, pp. 472-481.

Singh, L. D.; Singh, K. M. (2015b): Implementation of text encryption using elliptic curve cryptography. *Procedia Computer Science*, vol. 54, pp. 73-82.

Singh, R.; Panchbhaiya, I.; Pandey, A.; Goudar, R. H. (2015): Hybrid encryption scheme (HES): an approach for transmitting secure data over internet. *Procedia Computer Science*, vol. 48, pp. 51-57.

Subasree, S.; Sakthivel, N. K. (2010): Design of a new security protocol using hybrid cryptography algorithms. *International Journal of Research and Reviews*, vol. 2, no. 2, pp. 95-103.

Taha, A. A.; Elminaam, D. S. A.; Hosny, K. M. (2018): An improved security schema for mobile cloud computing using hybrid cryptographic algorithms. *Far East Journal of Electronics and Communications*, vol. 18, no. 4, pp. 521-546.

Yaeghoobi, S. B. K.; Tyagi, S. S.; Soni, M. K.; Ebadati E., O. M. (2014): SAERP: an energy efficiency real-time routing protocol in WSNs. *International Conference on Reliability Optimization and Information Technology*, pp. 249-254.

Yazdinejad, M.; Nayyeri, F.; Ebadati E., O. M.; Afshari, N. (2017): Secure distributed group rekeying scheme for cluster based wireless sensor networks using multilevel encryption. *Internet of Things: Novel Advances and Envisioned Applications*, pp. 127-147.

Zhu, S. H. (2011): Research of hybrid cipher algorithm application to hydraulic information transmission. *International Conference of Electronics, Communications and Control*, pp. 3873-3876.