









## Article

# Improved Secure Encryption with Energy Optimization Using Random Permutation Pseudo Algorithm Based on Internet of Thing in Wireless Sensor Networks

S. Nagaraj <sup>1</sup>, Atul B. Kathole <sup>2</sup>, Leena Arya <sup>3</sup>, Neha Tyagi <sup>4</sup>, S. B. Goyal <sup>5,\*</sup>, Anand Singh Rajawat <sup>6</sup>, Maria Simona Raboaca <sup>7,\*</sup>, Traian Candin Mihaltan <sup>8</sup>, Chaman Verma <sup>9</sup> and George Suci <sup>10,\*</sup>

- <sup>1</sup> Department of CSE, Mallareddy University, Hyderabad 500043, India  
<sup>2</sup> Department of Information Technology, Pimpri Chinchwad College of Engineering, Pune 411044, India  
<sup>3</sup> Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522502, India  
<sup>4</sup> Department of IT, G.L Bajaj Institute of Technology & Management, Knowledge Park 3, Greater Noida 201306, India  
<sup>5</sup> Faculty of Information Technology, City University, Petaling Jaya 46100, Malaysia  
<sup>6</sup> School of Computer Sciences & Engineering, Sandip University, Nashik 422213, India  
<sup>7</sup> ICSI Energy Department, National Research and Development Institute for Cryogenics and Isotopic Technologies, 240050 Ramnicu Valcea, Romania  
<sup>8</sup> Faculty of Building Services, Technical University of Cluj-Napoca, 40033 Cluj-Napoca, Romania  
<sup>9</sup> Faculty of Informatics, University of Eötvös Loránd, 1053 Budapest, Hungary  
<sup>10</sup> R&D Department Beia Consult International, 041386 Bucharest, Romania  
\* Correspondence: sb.goyal@city.edu.my (S.B.G.); simona.raboaca@icsi.ro (M.S.R.); george@beia.ro (G.S.)



**Citation:** Nagaraj, S.; Kathole, A.B.; Arya, L.; Tyagi, N.; Goyal, S.B.; Rajawat, A.S.; Raboaca, M.S.; Mihaltan, T.C.; Verma, C.; Suci, G. Improved Secure Encryption with Energy Optimization Using Random Permutation Pseudo Algorithm Based on Internet of Thing in Wireless Sensor Networks. *Energies* **2023**, *16*, 8. <https://doi.org/10.3390/en16010008>

Academic Editors: R. Maheswar, M. Kathirvelu and K. Mohanasundaram

Received: 19 September 2022

Revised: 13 November 2022

Accepted: 15 December 2022

Published: 20 December 2022



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Abstract:** The use of wireless and Internet of Things (IoT) devices is growing rapidly. Because of this expansion, nowadays, mobile apps are integrated into low-cost, low-power platforms. Low-power, inexpensive sensor nodes are used to facilitate this integration. Given that they self-organize, these systems qualify as IoT-based wireless sensor networks. WSNs have gained tremendous popularity in recent years, but they are also subject to security breaches from multiple entities. WSNs pose various challenges, such as the possibility of numerous attacks, their innate power, and their unfeasibility for use in standard security solutions. In this paper, to overcome these issues, we propose the secure encryption random permutation pseudo algorithm (SERPPA) for achieving network security and energy consumption. SERPPA contains a major entity known as a cluster head responsible for backing up and monitoring the activities of the nodes in the network. The proposed work performance is compared with other work based on secure IoT devices. The calculation metrics taken for consideration are energy, overheads, computation cost, and time consumption. The obtained results show that the proposed SERPPA is very significant in comparison to the existing works, such as GKA (Group Key Agreement) and MPKE (Multipath Key Establishment), in terms of data transfer rate, energy consumption and throughput.

**Keywords:** wireless sensor network (WSN); IoT; security; attacks; cluster mechanism; time consumption

## 1. Introduction

The development of communication and network systems, design advancements, and the implementation of microprocessor devices has resulted in the creation of intelligent systems to monitor and manage complex operations. Wireless Sensor Networks (WSN) as well as IoT devices are examples of communication devices that use the internet infrastructure as well as protocols for managing the world of IoT-linked objects. Technology advancements allow for the progression of various technological and living processes. They have resulted in intelligent robot behaviors, intelligent cities, robotization, and autonomous vehicles [1–4]. Information security plays a vital role in data integrity and privacy, preventing catastrophic consequences, even a general calamity [5–9]. To avoid unexpected behaviors, extra security

mechanisms included within devices and systems are utilized to enhance the security measures incorporated into internet protocols. Furthermore, many these devices, such as surveillance systems, cameras, and sensors, are operated in real-time to ensure that the stated security methods operate without disturbing the overall system functionality. They must be designed so that they are simple to implement in both hardware as well as software and that their use does not disrupt system behaviors and is efficient [10,11].

There are a variety of IoT applications that have become an intrinsic part of our lives. Many of them may be divided into common sectors such as smart home, smart grid, smart healthcare, intelligent transportation, etc. However, due to widespread adoption, various IoT issues have emerged, including a lack of processing capacity, memory resources, different hardware operating characteristics, enormous amounts of data transmission, heterogeneous data, and various kinds of networks [12]. The other significant IoT challenges that must be overcome, especially for low-resource devices and heterogeneous technologies, are data integrity, data confidentiality, and personal privacy [13]. One of the most efficient ways to protect data and communication confidentiality is cryptography. Cryptography can also be used to ensure information integrity and authentication services.

In the IoT era, it is vital to note that most IoT solutions have a “closed design”, making it difficult or complex to add extra security features after the manufacturing process is completed. On the other hand, the suite of cryptographic methods that are executed is narrowing due to IoT devices’ limited software and hardware resources. Hence, there is a need for a proper balance between the desired level of security as well as execution capabilities. Various cryptographic methods that provide roughly the same level of security may consume various amounts of power and resources, so the user must choose the most suitable for their needs, taking into account the restrictions of the IoT application as well as the deployed hardware [14]. The public-key cryptography methods consume considerably more power and resources than symmetric cryptography algorithms due to their long processing times [15]. The implementation of the symmetric method in IoT security solution design is a sensible choice. The work [16] describes a detailed examination as well as comparison of symmetric block-type methods in IoT devices, including LEA, Twofish, RC6, AES, SPECK128 ChaCha20-Poly1305 algorithms. Stream or sequential symmetric key ciphers are often faster than block-type ciphers. Generally, block ciphers require greater memory resources to encrypt/decrypt bigger chunks (blocks) of data, whereas sequential ciphers usually take one or a few bits at a time. They also utilize modest memory requirements and thus are ideal for implementation in constrained contexts. As a subclass of symmetric cryptography algorithms, stream cryptography algorithms are among the most widely used cryptography data protection approaches.

In work [17], the pseudo-random generator generates a series of bits instead of a random sequence of encryption bits. This concept is extracted from Shannon’s one-time pad scheme. The plain-text encryption sequence produced by pseudo-random generator is employed, and its attributes define the security of the protected data. As a result, in stream cryptography methods, the primary goal is to create pseudo-random bit/symbol generators with good cryptographic properties. In the previous fifty years, many concepts have been executed with varying degrees of success.

The RC4 generator, created by Ron Rivest in 1987, is the most popular as well as the most utilized pseudo-random sequence generator. Reverse engineering of the RSA INC program revealed the algorithm description, and Rivest himself confirmed the accuracy of the algorithm description found [18].

The popularity of the RC4 algorithm can be attributed to its simplicity and ease of implementation in software as well as hardware. The cryptanalytic community has taken notice of its tremendous popularity and application. The findings of a rigorous and in-depth investigation of this algorithm revealed several flaws in the method. The empirically observed shortcomings and the actual results of the authors of the article are theoretically proven, which provides a detailed assessment of the weaknesses identified.

The implementation methods in security protocols also contributed to the algorithm's vulnerability; hence its usage in security protocols has been discouraged since 2015.

The idea of the RC4 algorithm and its elegance suggests the possibilities of its commercialization. Our goal is to describe a low-complexity, high-efficiency general method of pseudo-random generator that does not suffer from RC4 flaws and is suited for security solution implementation in computationally restricted microprocessor contexts WSN and IoT. Different mathematical methods are utilized to analyze the probability distribution of the output sequence, information leakage, and correlation properties between the state of the generator as well as output sequence periodicity to prove plausible cryptographic properties of the proposed pseudo-random generator.

WSN raises several research questions, e.g., if it is an effective security management system, has an efficient topology, an efficient WSN architecture, and is an optimized energy-efficient approach. Because of the sensitive data it deals with as well as monitors, security is a rapidly growing study topic in WSN. Effective solutions that ensure security as well as energy efficiency are required. Numerous attacks demand a robust security solution to protect WSN. WSN's energy resource, on the other hand, is often limited. As a result, the various security protocols are not immediately relevant to diverse security challenges. More resources are required for state-of-the-art security solutions. Planetary security and cryptography techniques are primarily used in wired and wireless networks. Still, the most pressing concern is how we might apply these protocols to WSN platforms. Determining the optimal level of application of these protocols for security insurances is a difficult task.

The key motivation for this research is that WSNs monitor various actions, the majority of which are quite sensitive. As a result, we require a comprehensive security mechanism for these operations. We employ a cryptographic approach in the study to safeguard sensitive applications for a variety of applications. However, robust security algorithms require a lot of resources, such as energy, bandwidth, and memory. It is difficult to use any robust cryptographic method in a resource-constrained WSN that limits the capabilities of the resources. The packet delivery and average delay are performed by trust management between sensor nodes with critical management in a dynamic environment. Furthermore, data privacy is effectively secured.

This paper is organized as follows: Section 1 presents the introduction, in Section 2 related works and drawbacks from existing work are discussed, Section 3 presents the proposed mechanism and workflow, Section 4 presents the results and discussion, and finally, Section 5 presents the conclusions.

## 2. Related Work

A complete survey of most qualified research work is provided in this section. The significant problem of these systems is mainly included in that literature. Those systems that have a considerable problem with the suggested scheme are primarily included in that literature. Several major methods for crucial management in WSNs are critically examined. Following a thorough examination, various research shortcomings in the available literature are identified. A novel efficient key agreement mechanism has been presented based on deficiencies identified in the literature review. In the following are some of the most noteworthy schemes and protocols. In WSNs, ref. [19] proposed an elliptic curve cryptography-based group key agreement approach. The proposed protocol offers implicit sensor node verification. The proposed protocol's main advantages are its low communication and computing costs. The fundamental problem with the proposed work is that every node is involved in intricate security processes. The whole calculation cost is massive, affecting the scheme's overall performance. In the WSN situation, ref. [20] presented a unique group key agreement protocol. The suggested technique manages session keys in a very efficient manner. Furthermore, the suggested approach allows for many passive and active attacks within the network while also ensuring forward as well as backward secrecy. Recovering key computation in the given case is complex. As a result, obtaining private key information is challenging for any hacker. However, the primary flaw in this study

is that the clustering algorithm made extensive use of WSN resources. In reference [21] a technique based on round optimization and Group Key Agreement authentication (GKA) was proposed. The suggested protocol validates WSN group key agreement. In addition, the overall number of rounds in the system is kept to a minimum. The cost of processing reduces dramatically, and the complexity of network computing improves as well. The GKA protocol, on the other hand, adds network computing costs.

Similarly, ref. [22] suggested a safe key management approach for WSN. In the suggested method, elliptic curve cryptography was employed for key management, which ensures authentication and secure key management. Furthermore, the suggested technique protects against a variety of security assaults by employing a new technique based on discrete logarithmic issue, which provides increased security. In references [22,23], techniques for managing group session keys between sensor nodes as well as servers were presented. This approach is based on the well-known symmetric key encryption AES. These designs are very costly and security-efficient, according to the extensive reviews of the planned work. The primary difficulty with these systems is that the AES decryption is conducted at base station (BS). As a result, in a given WSN scenario, adequate sensor node authentication is difficult. Virtual and Lu [24–26] suggested techniques based on ECC cryptography as well as the Alike method for IoT platforms. Resistance cryptography is an energy-efficient approach for energy optimization that requires the least amount of energy while providing confidence between sensor nodes. ECC-based cryptography is also a fantastic key management method. The performance of RSA as well as ECC-based algorithms is evaluated in this study. The ECC-based algorithm outperforms the RSA-based approach, according to the output results. However, in the IoT domain, utilizing RSA for the same technique required a variety of network resources. In [27], a key agreement system was suggested. A proposed work session key is established for a defined time between sensor nodes as well as the gateway (GW). The session key is rebuilt for a specific session if there is a change or a fault in the network. Furthermore, the proposed technique provides implicit authentication of WSN nodes. The suggested approach is scalable and protects against network errors. The key challenges with this project, however, are the high communication and computing expenses. Multipath Key Establishment is a technique described by [28] for secure message communication (MPKE). The key value of the suggested research work is the secure and dependable transfer of information. Reed-Solomon codes have been utilized for secure session key agreement, with each round completed utilizing the protocol for Perfectly Secure Message Transmission (PSMT). The main agreement steps are not explicitly explained in this research effort, which is a limitation. As a result, resource-constrained WSNs are ineffective and energy-inefficient.

Some new and attractive research approaches for security and privacy protection have been offered in other relevant works. In this study [29], cryptographic techniques were applied, particularly ECC (Elliptic Curve Cryptography), which has a low processing complexity for cryptographic operations. Furthermore, these schemes consume extremely little energy and have very low communication costs [30–35]. The previous approach contributes about the use of IoT in the different fields to improve the performance [36–38]. This section examines and analyses a complete assessment of related research work [39–41] offered by writers for effective key management in WSN. According to critical analysis of the research work, asymmetric cryptography methods are very appropriate for crucial data communication security. Asymmetric cryptography techniques, on the other hand, can be employed to secure critical operations. Heavy activities are viable as well as necessary for robust security preservation. Symmetric key methods, on the other hand, have been frequently utilized. Symmetric key management techniques, on the other hand, are not very good at defending against a wide range of assaults. The primary problem with public-key cryptography methods is that we cannot use them directly in a WSN with limited resources. Rewards that are given out after state transitions are used to address the convergence problem. The transition mechanism considers different device energy levels and deep learning methods to make the changes in energy consumptions [42–44]. Various schemes

are proposed for perfect secret sharing mechanism in CRT [45]. The suggested model seeks to maximize network lifetime and energy usage [46–49]. We can, however, use them professionally at a dissimilar phase, where complex processes are effectively decreased.

### 3. Contribution of the Proposed Work

1. The proposed protocol aims to enhance performance of communication and network lifetime. It can be achieved by minimizing energy consumption and communication delay.
2. The implementation of secure encryption random permutation pseudo algorithm (SERPPA) for enhancing energy efficient communication.
3. The proposed model contains work cluster member who is responsible for cluster head selection.
4. The cluster head has a significant role, and its activities monitor and backup the nodes' activities in the network.
5. In this work, several existing protocols are described with their advantages and disadvantages. The proposed model is different from the existing models, and the overall result will enhance the data traffic, energy consumption, and throughput rate through stable routing.

Figure 1 shows the proposed architecture diagram; multiple sensor networks are required for data flow among various sources into a single sink. Sensor nodes are subject to limited capacity, memory, and computing resources which need optimal resource utilization. In the network, all sensor nodes use the same variables, and there is a possibility of redundant sensed data. Along with the application specifications, steering methods are designed according to the node's limitations and characteristics. The routing restrictions commonly used are short-latency, adaptive redundancy, QoS performance constraints, severe impact, etc.

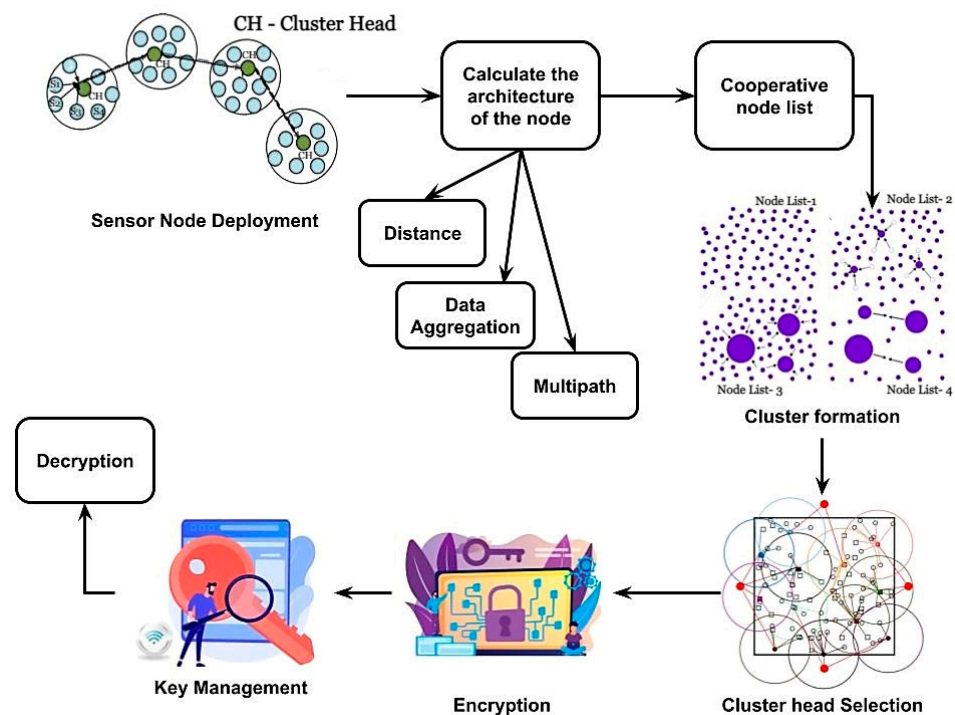


Figure 1. Proposed architecture diagram.

A WSN protocol mainly utilizes one-hop neighborhood information. Implementing two-hop neighborhood information maximizes the configuration complexity, which has a lack of routing decisions results and invalid evasion in WSN. The traffic balance around the network is essential for enhanced network life and transmission time along with tolerable reliability or energy efficiency. Two adaptive routing protocols are proposed to fulfill the implementation demands and challenges, e.g., energy efficiency, timely distribution service, latency, and reliability.

Based on the sensor node, nodes are indexed and connected, respectively. When the nodes are first deployed, they all have the same energy level. "Hello" messages are used to establish a connection between these nodes. The nodes' position, energy level, and distance between them are collected based on request as well as response. We request that all neighboring sensor nodes deliver "hello" messages. A "hello" message is received by each sensor node, which acknowledges it to sync to the other nodes. Each node's initial energy is found before packet transmission begins, and these cluster formations are conducted in various groups. Following the creation of a cluster model, the cluster supervisor's next working procedure begins.

#### *Secure Encryption Random Permutation Pseudo Algorithm (SERPPA)*

The secure encryption random permutation pseudo algorithm (SERPPA) translation cipher mechanism is extracted from the Advanced Encryption Standard (AES). AES is a symmetric-based encryption and block cipher algorithm. The proposed SERPPA can manage the message length of about 128,192,256,512 bits [31]. It ensures an enhanced security level with minimum energy consumption. SERPPA contains four AES operations: byte substitution, mixing columns, shifting rows, and round key. In SERPPA, the key management system is employed for both encryption and decryption on the sensor nodes. The byte substitution comprises key management processes. The sensor nodes collect the meaningful length of 512 bits, and the repeated characters are removed. The fixed key value is assigned and the default character is considered for further process. A special character is filled on the space between the characters. Next, the encryption process begins, and the decryption process is processed through the key management systems represented in Algorithm 1. The architecture of SERPPA is shown in Figure 2.

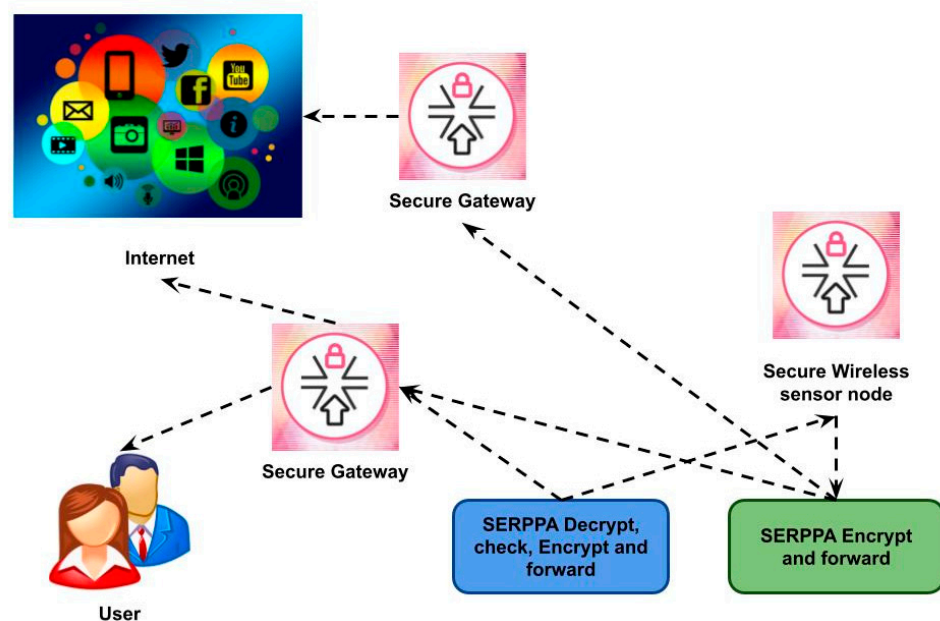


Figure 2. Architecture of SERPPA.

**Algorithm 1: of SERPPA**


---

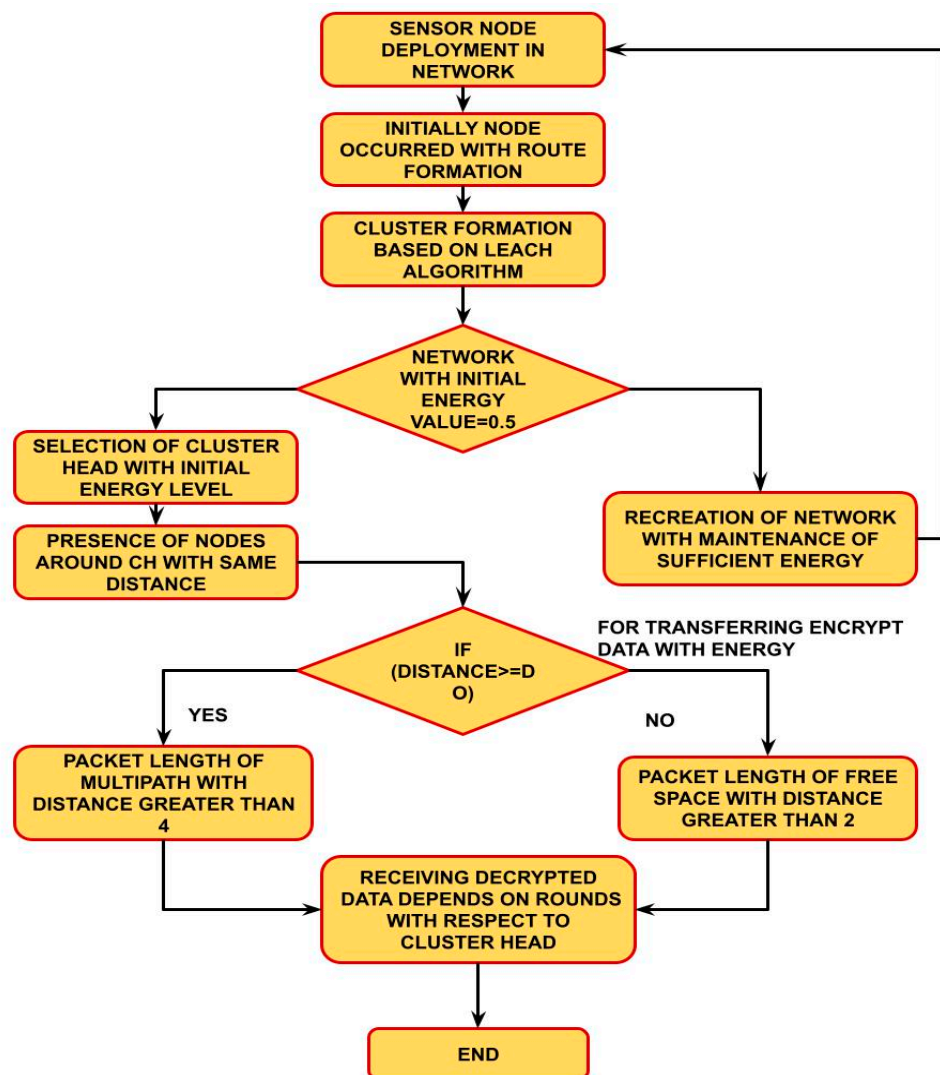
```

Begin
  start the process of getting 512-bitlength inputs
  remove the presence of same character at multiple times
do
  assign the encryption vector values [5,15,22,8,9,11] for the 512 bits
  where "x" is first character
  ex: x = 5 of key length is assigned
  then
    taken key [15,22,8,9,11]
  assign to remaining characters of 512 bits
  if
    presence of space between a letter
    assign a special character (\, #, $, &, *)
  end
do
  encryption
    apply k = [5,15,22,8,9,11] values to first set of 512 input message
  next
    apply k = [11,9,8,22,15,5] to next set of same 512 input message
  Continue . . .
  Stop once the character get over
end
end
end

```

---

Figure 3 shows the data transfer between the sensor nodes in the network. The proposed secure encryption random permutation pseudo algorithm (SERPPA) workflow operates with 512 bits unmeaningful message encryption with limited energy consumption. Initially, the proposed work implementation begins with sensor node deployment. The deployed sensor nodes form a cluster with the cluster head (CH). CH selection is based on the low energy adaptive clustering hierarchy (LEACH) method. The LEACH algorithm works according to the time division multiple access (TDMA) system with the medium access control (MAC) protocol. The proposed system's main function is to achieve minimized energy consumption and enhanced lifetime for the sensor cluster nodes in the networks.



**Figure 3.** Transfer of encrypted data and receiver of decrypted data with energy consumption.

Additionally, CDMA minimizes the interference between the clusters. Initially, 0.5 is the energy level where the network formation begins. The encrypted data transmission is based on distance between nodes, and rounds of CH determine the reception of decrypted data is shown in Algorithm 2.



---

**Algorithm 2: for Secure Encryption Random Permutation Pseudo Algorithm (SERPPA) for Energy Consumption**


---

1. Begin
  2. Step-1 creates the simulation network (1500 × 1500)
  3. {
  4. Set of nodes are deployed randomly;  $S_{n(x,y)}$ ;
  5. Check the node's availability state (idle, active)
  6. {
  7. Send the request "hello" to all neighboring sensor nodes [Hello →  $S_{n(x,y)}$ ];
  8. If received the message and send the acknowledgment nodes states is active →  $S_{n(x,y)}$ ;
  9. Else if
  10. Message not received the sensor node, the node is the idle state [idle →  $S_{n(x,y)}$ ];
  11. Collect the cooperative node list;
  12. }
  13. Ready to form the network [Ready →  $S_{(ex,y)}$ ];
  14. }
  15. Step-2 creates the cluster formation and CH election process-based energy factor.
  16. Create the cluster according to with cooperative node list
  17.  $S_n(d) = \text{distance} \rightarrow \sqrt{(x_{i,x} - x_{j,y})^2 + (y_{i,y} - y_{j,x})^2}$  //  $s_n[i][j]$ ,  $(x_{i,x} - x_{j,y})$  x,i coordinates and, y,j coordinates  $(y_{i,y} - y_{j,x})$  calculate with x and y coordinate distance
  18. Energy factor is patched up with the node cluster for transferring to BS
  19.  $S_n(e)\text{energy} = \left[ \frac{I_{ex} - I_{er}}{R_t} \right]$  // node energy defines  
 $S_{ex} \rightarrow \text{initialenergy}$ ;  $I_{er} \rightarrow \text{ResidualEnergyofanode}$ ;  $R_t \rightarrow \text{Responsetime}$ ;
  20. Packet transfer received Total ratio  $\left[ \frac{\text{packets received by all destination node}}{\text{Total packets send by all source node}} \right]$ ;
  21.  $EDA = \frac{\text{hop}(i)-1}{\text{hop}_{\max}}$   $\text{hop}_{\max}$  is the maximum number of node hops in network, and  $\text{hop}(i)$  is the hop numbers from node i to Sink.
  22.  $ETX = \frac{1}{D_f * D_r}$  where  $D_f$  represents the calculated likelihood that a packet will be received by a neighbour and  $D_r$  is the calculated likelihood that an acknowledgement packet will be successfully received.
  23. Determine optimum distance of a node;
  24. if (distance >= d0)  
nodeArch. Node(chNo). energy =  
 $\text{energy} - (ETX + EDA) * \text{packet length} + Emp * \text{packet length} * (\text{distance}^4)$   
else  
nodeArch. Node(chNo). energy =  
 $\text{energy} - (ETX + EDA) * \text{packet length} + Efs * \text{packet length} * (\text{distance}^2)$   
end  
nodeArch. Node(chNo). energy = nodeArch. Node(chNo). energy - ctrPacketLength \* ERX \*  
round (nodeArch.numNode/clusterModel. NumCluster);
  25. end
  
  - a. ClusterModel. NodeArch = nodeArch;
  26. end
- 

#### 4. Experimental Results

Network simulator NS-2 is taken for the proposed SERPPA execution. The experimental setup consists of a simulation environment in which the network is formed with 120 nodes between 1800 × 1800 m<sup>2</sup>. The nodes in the deployed network are dynamic and independent of each other, and they use the random way mobility model. The link-layer protocol in this configuration adheres to the IEEE 802.11 Mac standard. Network traffic is generated using multicast at constant bit rates. WLAN heterogeneous traffic is used for execution, including IEEE 802 and 802.11b. A TCP or UDP network topology is used to set up the data connection. Two thousand bytes per packet are used for network transmission at 24 Mbps data rates. Table 1 defines the simulation parameters taken for execution.

**Table 1.** Simulation parameters and their values.

Simulation Parameter	Value
Simulator	Network Simulator-2
Number of nodes	100
Simulation time	200 s
Mac Protocol	IEEE 802.11
Simulation area	1800 × 1800 m <sup>2</sup>
Mobility model	accidental waypoint model
Radio range	100 m
Data rate	24 Mbps
Antenna	Omnidirectional antenna
Traffic type	Multicast constant bit ratio
Packet size	512 bytes
Node speed	10–35 m/s

Energy consumption is one of the important factors which determines the efficiency of the algorithms. Figure 4 illustrates the performance in terms of energy consumption with a total number of nodes obtained by each algorithm. The algorithm taken for consideration is the herein proposed SERPPA with existing GKA and MPKE. The X-axis determines the total number of nodes that take part in observation, and the Y-axis defines the total energy consumed. The consumed energy is calculated in terms of joules. At regular intervals, the total number of nodes that take part is gradually increased by ten. Observation of each set of nodes with respect to the algorithms is plotted graphically for analysis. From the herein proposed SERPPA, energy consumption of 10 nodes is 230 joules, 20 nodes is 310 joules, 30 nodes is 500 joules, 40 nodes is 650 joules, 50 nodes is 710 joules, 60 nodes is 800 joules, 70 nodes is 980 joules, 80 nodes is 1200 joules, 90 nodes is 1500 joules, and 100 nodes is 1900 joules. Whereas GKA energy consumption of 10 nodes is 550 joules, 20 nodes is 720 joules, 30 nodes is 810 joules, 40 nodes is 930 joules, 50 nodes is 1100 joules, 60 nodes is 1250 joules, 70 nodes is 1650 joules, 80 nodes is 1800 joules, 90 nodes is 2200 joules, and 100 nodes is 2800 joules. Energy consumed by MPKE for 10 nodes is 650 joules, 20 nodes is 720 joules, 30 nodes is 900 joules, 40 nodes is 1200 joules, 50 nodes is 1630 joules, 60 nodes is 1850 joules, 70 nodes is 2100 joules, 80 nodes is 2500 joules, 90 nodes is 2900 joules, and 100 nodes is 3200 joules. The graphical representation clearly represents that the proposed SERPPA results are more efficient than those of GKA and MPKE.

Network overhead determines the additional information taken while transmitting the packets. More overhead leverages the network performance; hence overhead has a significant impact in the overall network performance. Figure 5 illustrates the performance of overhead with the total number of nodes obtained by each algorithm. The algorithm taken for consideration is proposed SERPPA with existing GKA and MPKE. The X-axis determines the total number of nodes that take part in observation, and the Y-axis defines the total overhead attained by each algorithm. The consumed overhead is calculated in terms of kb. At regular intervals, the total number of nodes that take part is gradually increased by ten. Observation of each set of nodes concerning the algorithms is plotted graphically for analysis. From the proposed SERPPA, the overhead of 10 nodes is 5 kb, 20 nodes is 8 kb, 30 nodes is 12 kb, 40 nodes is 19 kb, 50 nodes is 25 kb, 60 nodes is 30 kb, 70 nodes is 35 kb, 80 nodes is 50 kb, 90 nodes is 65 kb, and 100 nodes is 75 kb. Whereas GKA attained overhead for 10 nodes is 12 kb, 20 nodes is 18 kb, 30 nodes is 21 kb, 40 nodes is 30 kb, 50 nodes is 38 kb, 60 nodes is 50 kb, 70 nodes is 60 kb, 80 nodes is 65 kb, 90 nodes is 70 kb, and 100 nodes is 85 kb. The MPKE attained overhead for 10 nodes is 20 kb, 20 nodes is 28 kb, 30 nodes is 35 kb, 40 nodes is 40 kb, 50 nodes is 45 kb, 60 nodes is 60 kb,

70 nodes is 65 kb, 80 nodes is 70 kb, 90 nodes is 78 kb, and 100 nodes is 90 kb. The graphical representation clearly shows that proposed SERPPA overhead is more efficient than GKA and MPKE.

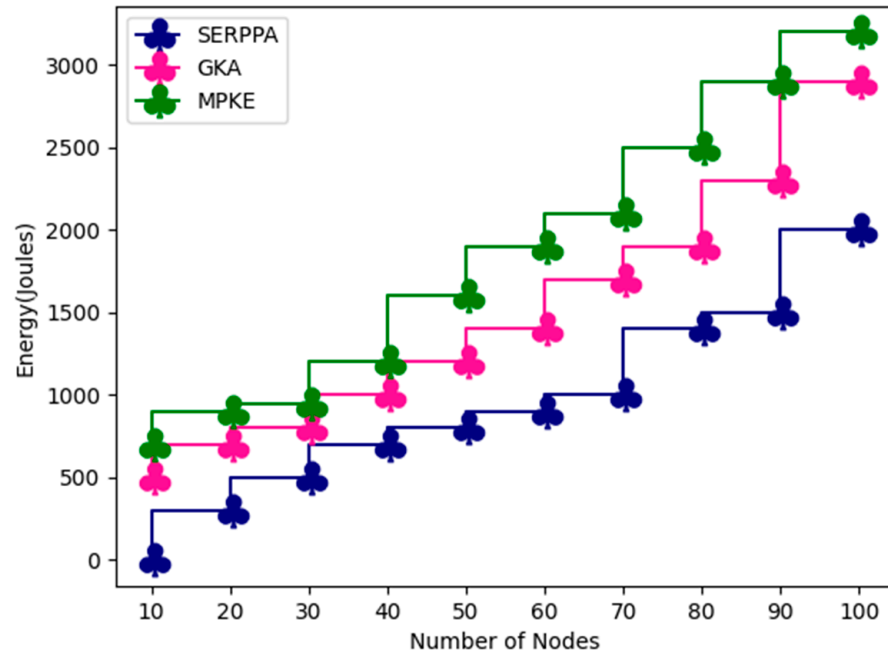


Figure 4. Energy vs. number of nodes.

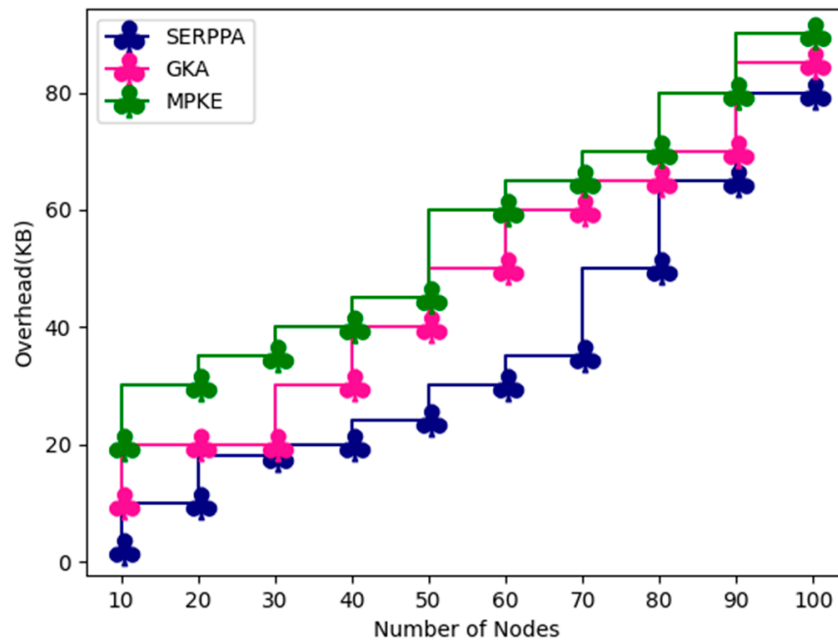
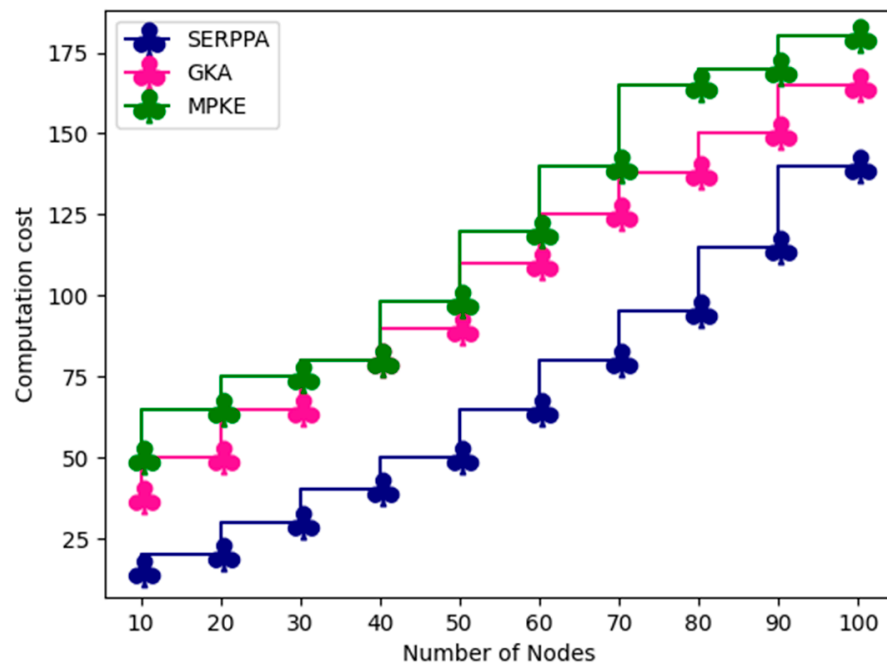


Figure 5. Overhead vs. number of nodes.

The computation cost is the communication cost taken for each transmission by a set of nodes. Figure 6 illustrates the performance of computation cost with a total number of nodes obtained by each algorithm. The algorithm taken for consideration is proposed SERPPA with existing GKA and MPKE. The X-axis determines the total number of nodes that take part in observation, and the Y-axis determines the total computation cost attained by each method. At regular intervals, the total number of nodes that take part is gradually increased by ten. The observation of each set of nodes concerning the algorithms is plotted

graphically for analysis. From the proposed SERPPA, the computation cost of 10 nodes is 15, with 20 nodes is 21, with 30 nodes is 28, with 40 nodes is 40, with 50 nodes is 50, with 60 nodes is 65, with 70 nodes is 80, with 80 nodes is 95, with 90 nodes is 110, and 100 nodes is 140. The computation cost attained by GKA for 10 nodes is 35, with 20 nodes is 50, with 30 nodes is 65, with 40 nodes is 78, with 50 nodes is 90, with 60 nodes is 110, with 70 nodes is 125, with 80 nodes is 138, with 90 nodes is 150, and with 100 nodes is 165. The computation cost attained by MKPE for 10 nodes is 50, with 20 nodes is 65, with 30 nodes is 75, with 40 nodes is 80, with 50 nodes is 95, with 60 nodes is 120, with 70 nodes is 140, with 80 nodes is 165, with 90 nodes is 170, and with 100 nodes is 180. The graphical representation clearly shows that the proposed SERPPA results are very low compared to GKA and MPKE.



**Figure 6.** Computation cost vs. number of nodes.

Quick packet transmission without any data loss is a vital requirement. An algorithm with minimum time and successful transmission determines its efficiency. Figure 7 shows the performance of time consumed with the total number of nodes obtained by each algorithm. The algorithm taken for consideration is proposed SERPPA with existing GKA and MPKE. The X-axis determines the total number of nodes that take part in observation, and the Y-axis defines the total time consumed by each algorithm. The time consumption is calculated in terms of milliseconds (ms). At regular intervals, the total number of nodes that take part is gradually increased by ten. The observation of each set of nodes with respect to the algorithm is plotted graphically for analysis. From which the proposed SERPPA time consumed for 10 nodes is 3 ms, time consumed for 20 nodes is 5 ms, time consumed for 30 nodes is 8 ms, time consumed for 40 nodes is 11 ms, time consumed for 50 nodes is 15 ms, time consumed for 60 nodes is 19 ms, time consumed for 70 nodes is 22 ms, time consumed for 80 nodes is 25 ms, time consumed for 90 nodes is 30 ms and time consumed for 100 nodes is 35 ms. Whereas the time consumption of GKA for 10 nodes is 10 ms, time consumed for 20 nodes is 12 ms, time consumed for 30 nodes is 15 ms, time consumed for 40 nodes is 18 ms, time consumed for 50 nodes is 20 ms, time consumed for 60 nodes is 22 ms, time consumed for 70 nodes is 25 ms, time consumed for 80 nodes is 28 ms, time consumed for 90 nodes is 40 ms and time consumed for 100 nodes is 50 ms. The MKPE time consumption for 10 nodes is 12 ms, time consumed for 20 nodes is 15 ms, time consumed for 30 nodes is 20 ms, time consumed for 40 nodes is 25 ms, time consumed for 50 nodes is

28 ms, time consumed for 60 nodes is 30 ms, time consumed for 70 nodes is 35 ms, time consumed for 80 nodes is 40 ms, time consumed for 90 nodes is 55 ms and time consumed for 100 nodes is 60 ms. The graphical representation clearly shows that the time consumed by the proposed SERPPA is very low in comparison to GKA and MPKE.

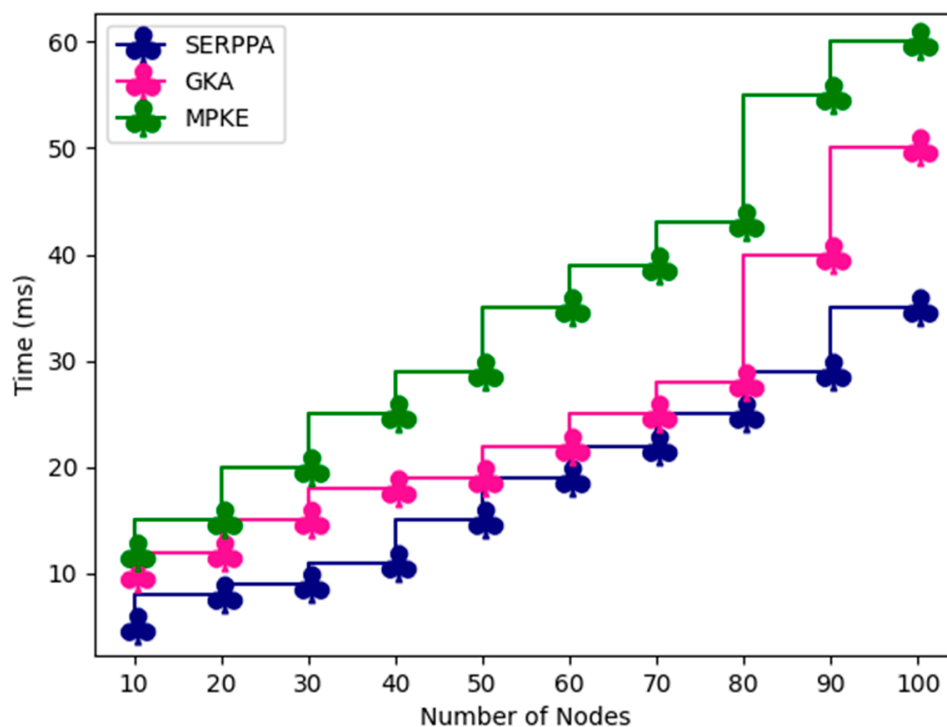


Figure 7. Time consumed vs. number of nodes.

## 5. Conclusions

In this research, we proposed the secure encryption random permutation pseudo algorithm (SERPPA) to secure the data transmitted through WSN. SERPPA is extracted from AES, which is an asymmetric-based encryption and block cipher algorithm. The secure encryption random permutation pseudo algorithm (SERPPA) is a cluster-based mechanism for enhancing energy-efficient communications. The proposed model contains work cluster member, which is responsible for cluster head selection. The cluster head contains the major role, such as monitoring and backing up the activities of the nodes in the network. The performance of the proposed work is determined by a comparison work carried out with GKA and MPKE. The evaluation metrics taken for consideration are energy, overheads, computation cost, and time consumption. Compared to previous methods, data traffic and energy consumption was decreased and throughput rate was increased through stable routing. The experimental results were carried in an NS-2 simulation environment. The proposed system observations are plotted and represented graphically with the result obtained by GKA and MPKE. In all evaluation metrics, the proposed SERPPA results are more efficient than the others. It shows the proposed SERPPA performance is far better than the existing algorithms. Some limitations of the proposed algorithm have not been evaluated across the various algorithms; in future research, it will be evaluated with more different approaches.

**Author Contributions:** Conceptualization, S.N.; supervision, A.B.K. and S.B.G.; writing—original draft, L.A. and N.T.; validation, A.S.R. and S.B.G.; writing—review and editing, A.S.R., S.B.G., M.S.R., T.C.M., C.V., G.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** This paper was partially supported by UEFISCDI Romania and MCI through BEIA projects NGI-UAV-AGRO, SOLID-B5G, T4ME2, DISAVIT, AISTOR, MULTI-AI, ADRIATIC, Hydro3D, EREMI, MUSEION, iPREMAS, IPSUS, U-GARDEN, CREATE, STACK, ENTA and by European Union’s Horizon 2020 research and innovation program under grant agreement No. 883522 (S4ALLCITIES). This work is supported by Ministry of Research, Innovation, Digitization from Romania by the National Plan of R & D, Project PN 19 11, Subprogram 1.1. Institutional performance-Projects to finance excellence in RDI, Contract No. 19PFE/30.12.2021 and a grant of the National Center for Hydrogen and Fuel Cells (CNHPC)—Installations and Special Objectives of National Interest (IOSIN). Ministry of Investments and European Projects: Human Capital Sectoral Operational Program 2014–2020, Contract no. 62461/03.06.2022, SMIS code 153735.

**Data Availability Statement:** Data will be shared for review based on the editorial reviewer’s request.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Rehman, R.A.; Khan, B. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* **2018**, *18*, 2796.
2. Salah, K. *The Era of Internet of Things*, 2nd ed.; Springer: Cham, Switzerland, 2019.
3. Rayes, A.; Samer, S. *Internet of Things from Hype to Reality*, 2nd ed.; Springer: Cham, Switzerland, 2019.
4. Atlam, H.; Walters, R.J.; Wills, G.B. Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues. *Int. J. Intell. Comput. Res.* **2018**, *9*, 928–938. [[CrossRef](#)]
5. Costa, D.G.; Figuerêdo, S.; Oliveira, G. Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions. *Cryptography* **2017**, *1*, 4. [[CrossRef](#)]
6. Kambourakis, G.; Marmol, F.G.; Wang, G. Security and Privacy in Wireless and Mobile Networks. *Future Internet* **2018**, *10*, 18. [[CrossRef](#)]
7. Ziegler, S. *Internet of Things Security and Data Protection*, 2nd ed.; Springer: Cham, Switzerland, 2019.
8. Cheruvu, S.; Kumar, A.; Smith, N.; Wheeler, D.M. *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment*; Apress: Berkeley, CA, USA, 2019.
9. Mahmood, Z. (Ed.) *Security, Privacy and Trust in the IoT Environment*; Springer: Cham, Switzerland, 2019.
10. Banday, M.T. *Cryptographic Security Solutions for the Internet of Things*; IGI Global: Hershey, PA, USA, 2019.
11. Biryukov, A.; Perrin, L. State of the Art in Lightweight Symmetric Cryptography. IACR Cryptology ePrint Archive. 2017. Available online: <https://eprint.iacr.org/2017/511> (accessed on 28 October 2019).
12. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the Internet of Things: Perspectives and challenges. *Wirel. Netw.* **2014**, *20*, 2481–2501. [[CrossRef](#)]
13. Frustaci, M.; Pace, P.; Aloï, G.; Fortino, G. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet Things J.* **2017**, *5*, 2483–2495. [[CrossRef](#)]
14. Hamad, F.; Smalov, L.; James, A. Energy-aware Security in M-Commerce and the Internet of Things. *IETE Tech. Rev.* **2009**, *26*, 357–362. [[CrossRef](#)]
15. Bilal, M.; Kang, S.G. An Authentication Protocol for Future Sensor Networks. *Sensors* **2017**, *17*, 979. [[CrossRef](#)]
16. Saraiva, D.A.F.; Leithardt, V.R.Q.; de Paula, D.; Sales Mendes, A.; González, G.V.; Crocker, P. PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices. *Sensors* **2019**, *19*, 4312. [[CrossRef](#)]
17. Von zur Gathen, J. *CryptoSchool*; Springer: Berlin/Heidelberg, Germany, 2015.
18. Rivest, R.; Schuldt, J. Spritz—A Spongy RC4-Like Stream Cipher and Hash Function. Available online: [https://en.wikipedia.org/wiki/RC4#cite\\_note-Rivest2014-14](https://en.wikipedia.org/wiki/RC4#cite_note-Rivest2014-14) (accessed on 27 October 2014).
19. Tang, H.; Zhu, L.; Zhang, Z. A Novel Authenticated Group Key Agreement Protocol Based on Elliptic Curve Diffie-Hellman. In Proceedings of the 2008 4th International Conference on Wireless Communications, Dalian, China, 12–17 October 2008; pp. 1–4.
20. Zhang, Z.; Jiang, C.; Deng, J. A novel group key agreement protocol for wireless sensor networks. In Proceedings of the 2010 International Conference on Measuring Technology and Mechatronics Automation, Changsha, China, 13–14 March 2010; pp. 230–233.
21. Pramod, N.D.B.; Sharnappa, G.R. Review on fault detection and recovery in WSN. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2015**, *5*.
22. Abi-Char, P.E.; Mhamed, A.; El-Hassan, B. A secure authenticated key agreement protocol based on elliptic curve cryptography. In Proceedings of the 3rd International Symposium on Information Assurance and Security, Manchester, UK, 29–31 August 2007; pp. 89–94.
23. Meingast, M.; Roosta, T.; Sastry, S. Security and privacy issues with health care information technology. In Proceedings of the 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, New York, NY, USA, 30 August–3 September 2006; pp. 5453–5458.
24. Singelée, D.; Latré, B.; Braem, B.; Peeters, M.; De Soete, M.; De Cleyn, P.; Preneel, B.; Moerman, I.; Blondia, C. A secure low-delay protocol for wireless body area networks. *Adhoc. Sens. Wirel. Netw.* **2010**, *9*, 53–72.

25. Ertaul, L.; Lu, W. *ECC Based Treshold Cryptography for Secure Data Forwarding and Secure Key Exchange*; University of Waterloo: Waterloo, ON, Canada, 2005.
26. Ertaul, L.; Chudinov, P.; Morales, B. IoT security: Authenticated lightweight key exchange (ALIKE). In Proceedings of the International Conference on Wireless Networks (ICWN), Rome, Italy, 30 June–4 July 2019; pp. 45–50.
27. Eldefrawy, M.H.; Khan, M.K.; Alghathbar, K. A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography. In Proceedings of the 2010 International Conference on Anti-Counterfeiting, Hoboken, NJ, USA, 22–24 March 2010; pp. 1–6.
28. Wu, J.; Stinson, D.R. Three improved algorithms for multipath key establishment in sensor networks using protocols for secure message transmission. *IEEE Trans. Dependable Secur. Comput.* **2010**, *8*, 929–937.
29. Gope, P.; Das, A.K.; Kumar, N.; Cheng, Y. Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4957–4968. [[CrossRef](#)]
30. He, D.; Ma, M.; Zeadally, S.; Kumar, N.; Liang, K. Certificateless Public Key Authenticated Encryption with Keyword Search for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3618–3627. [[CrossRef](#)]
31. Dua, A.; Kumar, N.; Das, A.K.; Susilo, W. Secure Message Communication Protocol Among Vehicles in Smart City. *IEEE Trans. Veh. Technol.* **2017**, *67*, 4359–4373. [[CrossRef](#)]
32. Tyagi, S.; Kumar, N. A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks. *J. Netw. Comput. Appl.* **2013**, *36*, 623–645. [[CrossRef](#)]
33. He, D.; Zeadally, S.; Kumar, N.; Lee, J.-H. Anonymous Authentication for Wireless Body Area Networks with Provable Security. *IEEE Syst. J.* **2016**, *11*, 2590–2601. [[CrossRef](#)]
34. Yousefpoor, M.S.; Barati, H. Dynamic key management algorithms in wireless sensor networks: A survey. *Comput. Commun.* **2018**, *134*, 52–69. [[CrossRef](#)]
35. Yousefpoor, M.S.; Barati, H. DSKMS: A dynamic smart key management system based on fuzzy logic in wireless Complexity 9 sensor networks. *Wirel. Netw.* **2020**, *26*, 2515–2535. [[CrossRef](#)]
36. Sampathkumar, A.; Tesfayohani, M.; Shandilya, S.K.; Goyal, S.B.; Jamal, S.S.; Shukla, P.K.; Bedi, P.; Albeedan, M. Internet of Medical Things (IoMT) and Reflective Belief Design-Based Big Data Analytics with Convolution Neural Network-Metaheuristic Optimization Procedure (CNN-MOP). *Comput. Intell. Neurosci.* **2022**, *2022*, 2898061. [[CrossRef](#)]
37. Ramanan, M.; Singh, L.; Kumar, A.S.; Suresh, A.; Sampathkumar, A.; Jain, V.; Bacanin, N. Secure blockchain enabled Cyber-Physical health systems using ensemble convolution neural network classification. *Comput. Electr. Eng.* **2022**, *101*, 108058. [[CrossRef](#)]
38. Arumugam, S.; Shandilya, S.K.; Bacanin, N. Federated Learning-Based Privacy Preservation with Blockchain Assistance in IoT 5G Heterogeneous Networks. *J. Web Eng.* **2022**, *21*, 1323–1346. [[CrossRef](#)]
39. Bedi, P.; Goyal, S.B.; Rajawat, A.S.; Shaw, R.N.; Ghosh, A. Application of AI/IoT for Smart Renewable Energy Management in Smart Cities. In *AI and IoT for Smart City Applications; Studies in Computational Intelligence*; Piuri, V., Shaw, R.N., Ghosh, A., Islam, R., Eds.; Springer: Singapore, 2022; Volume 1002. [[CrossRef](#)]
40. Sharma, S.; Rani, M.; Goyal, S. Energy Efficient Data Dissemination with ATIM Window and Dynamic Sink in Wireless Sensor Networks. In Proceedings of the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, Kerala, India, 27–28 October 2009; pp. 559–564. [[CrossRef](#)]
41. Sharma, S.; Goyal, S.B.; Qamar, S. Four-Layer Architecture Model for Energy Conservation in Wireless Sensor Networks. In Proceedings of the 2009 4th International Conference on Embedded and Multimedia Computing, Jeju, Republic of Korea, 10–12 December 2009; pp. 1–3. [[CrossRef](#)]
42. Kaliappan, V.K.; Lalpet Ranganathan, A.B.; Periasamy, S.; Thirumalai, P.; Nguyen, T.A.; Jeon, S.; Min, D.; Choi, E. Energy-Efficient Offloading Based on Efficient Cognitive Energy Management Scheme in Edge Computing Device with Energy Optimization. *Energies* **2022**, *15*, 8273. [[CrossRef](#)]
43. Ibrahim, B.; Rabelo, L.; Gutierrez-Franco, E.; Clavijo-Buritica, N. Machine Learning for Short-Term Load Forecasting in Smart Grids. *Energies* **2022**, *15*, 8079. [[CrossRef](#)]
44. Banuselvasaraswathy, B.; Sampathkumar, A.; Jayarajan, P.; Sheriff, N.; Ashwin, M.; Sivasankaran, V. A Review on Thermal and QoS Aware Routing Protocols for Health Care Applications in WBASN. In Proceedings of the 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 28–30 July 2020; pp. 1472–1477. [[CrossRef](#)]
45. Subrahmanyam, R.; Rukma Rekha, N.; Subba Rao, Y.V. Multipartite Verifiable Secret Sharing Based on CRT. In *Computer Networks and Inventive Communication Technologies; Lecture Notes on Data Engineering and Communications Technologies*; Smys, S., Bestak, R., Palanisamy, R., Kotuliak, I., Eds.; Springer: Singapore, 2022; Volume 75. [[CrossRef](#)]
46. Subramani, N.; Mohan, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. An Efficient Metaheuristic-Based Clustering with Routing Protocol for Underwater Wireless Sensor Networks. *Sensors* **2022**, *22*, 415. [[CrossRef](#)]
47. Bacanin, N.; Arnaut, U.; Zivkovic, M.; Bezdan, T.; Rashid, T.A. Energy Efficient Clustering in Wireless Sensor Networks by Opposition-Based Initialization Bat Algorithm. In *Computer Networks and Inventive Communication Technologies; Lecture Notes on Data Engineering and Communications Technologies*; Smys, S., Bestak, R., Palanisamy, R., Kotuliak, I., Eds.; Springer: Singapore, 2022; Volume 75. [[CrossRef](#)]

48. Lakshmana, K.; Subramani, N.; Alotaibi, Y.; Alghamdi, S.; Khalafand, O.I.; Nanda, A.K. Improved Metaheuristic-Driven Energy-Aware Cluster-Based Routing Scheme for IoT-Assisted Wireless Sensor Networks. *Sustainability* **2022**, *14*, 7712. [[CrossRef](#)]
49. Mehrotra, S.; Sharan, A. Comparative Analysis of K-Means Algorithm and Particle Swarm Optimization for Search Result Clustering. In *Smart Trends in Computing and Communications*; Springer: Singapore, 2020; pp. 109–114. [[CrossRef](#)]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.