Journal of Communication Engineering (JCE)

P- ISSN: 2322-4088 Vol. 11, No. 1, Jan.-Jun. 2022 E- ISSN: 2322-3936

Key Pre-distribution Scheme in Fog Networks with Multi Clouds

M. Tajeri Department of Computer Engineering; Qom Branch; Islamic Azad University; Qom, Iran Email: majid_tajeri@yahoo.com

H. H. S. Javadi* **[Corresponding Author]** Department of Computer Engineering; Shahed University; Tehran, Iran Email: h.s.javadi@shahed.ac.ir

M. Bayat Department of Computer Engineering; Shahed University; Tehran, Iran; Email: mbayat@shahed.ac.ir

M. E. Shiri Department of Mathematics and Computer Science; Amirkabir University of Technology; Tehran, Iran Email: shiri@aut.ac.ir

Received: *16 Feb. 2022* ***Revised:*** *02 May 2022* ***Accepted:*** *15 Jun. 2022*

Abstract: Creating a secure communication channel in hierarchical networks is a very important issue and several algorithms have been proposed for it. Unfortunately, due to limited resources in fog networks, which are a special type of hierarchical networks, it is not possible to use conventional algorithms. In this article, we have presented an algorithm to create a secure communication channel on fog networks, which is based on key pre-distribution and is used for multi-cloud fog networks. In this method, by using the SBIBD, blocks are generated to be assigned to the cloud nodes, and by using the residual design on the SBIBD, classes and blocks are created to be assigned to the fog nodes and end devices. The results show that the proposed method increases scalability and reduces communication, memory and computing overheads. The probability of capturing the network in the proposed method is about 0 and its connectivity is about 1.

Index Terms: Fog Networks, Key Pre-distribution, Multi Clouds, Residual Design, SBIBD.

Citation: M. Tajeri, H. H. S. Javadi, M. Bayat and M. E. Shiri, "Key Pre-distribution Scheme in Fog Networks with Multi Clouds," *Journal of Communication Engineering*, vol. 11, no. 1, pp. 87-110, Jan.-Jun. 2024.

http://dx.doi.org/10.22070/jce.2024.18520.1261

I. INTRODUCTION

An environment for connecting smart devices like mobile phones and laptops to perform tasks is called Internet of Things (IoT). But implementing IoT-based systems faces fundamental challenges such as storage, processing, and limited energy resources. To solve or reduce these challenges, IoT can be integrated with cloud technology and take advantage of the benefits of cloud computing such as high availability and scalability [1]-[2].

If cloud computing extends to the edge, it is called fog computing [3]. Fog allows cloud services be close to IoT devices and reduce latency, network traffic, energy expenditures and storage overhead and support node mobility, node location awareness, and real-time processing, which are not supported by cloud computing [4]. In the cloud data center, there are components such as switches, routers, and gateways that fog devices are connected to [5]. Fog devices can be any computing and storage device developed in different environments and among the millions of end devices that have access to the cloud network. The fog computing architecture has a three-level hierarchical structure consisting of the cloud layer (highest level), the fog layer (middle level), and the end devices (lowest level). In this model, the fog layer and end devices have different processing power, communication amplitude and residual energy and play different roles in network communication [6].

One of the challenges of fog networks is security, which has many complications and challenges. One of security challenges is creating a secure communication channel in the hierarchical structure of this network. Fog networks include devices with relatively limited computing resources, and it is not realistic to implement conventional security solutions on them. The challenge of secure communication in fog networks is similar to hierarchical wireless sensor networks (HWSN). The difference is that the HWSN is well known and several methods have been proposed for it. Also, it is necessary that other conditions such as minimizing overheads of computation, memory and communication and increasing network connectivity, scalability and resiliency are achievable [7]-[8]. Many algorithms have been presented for flat networks, which, in addition to creating a secure communication channel, consider other conditions for better algorithm performance. But such schemes are not directly applicable to hierarchical fog networks. Therefore, due to the increasing popularity of fog networks, the need for an effective key management and distribution plan for use in these networks is felt.

To establish a secure communication channel, key generation and distribution is very important. The key distribution should be in such a way that end devices can connect to the fog nodes directly or through another end devices. Also, in order to reduce communication and computation overheads, cloud nodes should be able to communicate directly with fog nodes in the fog layer.

Table 1. List of used notations

Symbol	Description
p	Prime number
N	Network size
X	Set of objects
B_i	Subset of X is called block
$\ddot{B}$	Finite set of B_i
C_i	Residual Design class
$B\backslash B_i$	Residual Design block
BIBD	Balanced Incomplete Block Design
SBIBD	Symmetric BIBD
RD	Residual Design
KPS	Key Pre-distribution Scheme
KP	Key Pre-distribution
CN	Cluster node
CH	Cluster head
CL	Cloud node
ED	End device
FN	Fog node

One of the solutions is key pre-distribution, where the keys are generated before the establishment of the network and distributed among the nodes in different layers. In this paper, a method for creating a secure communication channel in fog networks is presented, which is based on key pre-distribution scheme (KPS) and is used for multi-clouds fog networks. The proposed method is obtained by combining residual design (RD) and symmetric balanced incomplete block scheme (SBIBD). In this method, we first classify the end devices into different clusters. Then we have used SBIBD to generate blocks and RD to generate classes and RD sets.

Based on the explanations and examples written in Section II.III, the blocks produced by the SBIBD method have at least one key in common with each other, and since these blocks are assigned to cloud nodes, cloud nodes can easily communicate with each other. Also, the classes generated by applying the RD method on SBIBD blocks, have at least one key in common with each other. These classes are assigned to fog nodes, which makes these nodes easily communicate with each other. RD sets are also produced by applying the RD method on SBIBD blocks. These sets either have a common key and communicate with each other directly, or they communicate through a third set with which both of them have a common key. On the other hand, RD classes and sets either directly or through the third class and set have a common key and can communicate,

which causes communication between the fog layer and the end devices layer. At the end, a random key is selected from each class and added to the blocks so that the communication between the cloud layer and the fog layer is also made.

The results show that the proposed method increases scalability, resiliency and connectivity and reduces memory, communication and computation overheads. Also, the proposed method is completely independent of the node mobility model. Table 1 summarizes the notation used in the paper.

In the next section, related works and mathematical concepts will be explained, and in section III, the proposed method will be explained. In section IV, we evaluate the performance of the proposed method based on the parameters of scalability, node mobility, resistance and overheads of memory, communication and computation, and compare the proposed method with similar methods. In section V, a summary of the results obtained after evaluating the proposed method and comparing it with similar methods will be presented and finally, section VI will include conclusions and suggestions for future work.

II. RELATED WORKS

In this section, we first review the recent researches in multi cloud and fog and compare the proposed method in terms of the method used, the parameters checked, and the results obtained with them. The result of this review and comparison can be seen in section II.I. Since the proposed method is based on KPS and RD, in section II.II, we describe KPS schemes and specify that the BIBD scheme used in the proposed method is classified as location-independent schemes. In section II.III, we will describe the mathematical concepts related to BIBD and how to implement the RD on BIBD. At the end, by presenting an example, we explain how to obtain blocks, classes, and RD sets that are used in the proposed method.

II-I. RECENT RESEARCHES IN MULTI CLOUD AND FOG

In [9], to overcome the security issues identified, an improved authentication scheme based on key agreement and management was proposed. The scheme authenticates all the entities in the communication, including the cloud server. The scheme secures against privileged insider attacks, ensures user anonymity, un traceability, and session secrecy. The scheme was verified using rigorous cryptanalysis and its security was proved using the ROR model. Formal verification using scyther also confirmed its security against active and passive attacks. An efficiency analysis was performed by comparing the computation and communication costs with other relevant schemes. Functional analysis proved that the proposed scheme exhibits all the functionalities necessary

for robust authentication in the cloud-fog-device framework. Overall, the new authentication scheme addresses the security concerns of the cloud-fog-device framework, making it a secure and reliable option for real-time applications.

[10] presents an innovative mutual Authentication and Key Agreement protocol that is specifically tailored to meet the security needs of fog computing in the context of the edge–fog–cloud three-tier architecture, enhanced by the incorporation of the 5G network. This study improves security in the edge–fog–cloud context by introducing a stateless authentication mechanism and conducting a comparative analysis of the proposed protocol with well-known alternatives, such as TLS 1.3, 5G-AKA, and various handover protocols. The transmission cost in suggested approach in the authentication phase is approximately 30% lower than other protocols. In addition, the suggested handover protocol only involves two signaling expenses. The computational cost for handover authentication for the edge user is significantly low and is under 10% of the computing costs of other authentication protocols.

[11] proposes an effective two-way authentication between edge devices with key management in fog computing environments (TAKM-FC). The edge nodes are the user's mobile devices and set of smart devices controlled by the fog server. To improve the proposed authentication system, it has made use of techniques like fuzzy extractor and one-way hash with cryptographic primitives. The proposed TAKM-FC scheme is validated mathematically based on the ROR model and then verified using the ProVerif tool. The TAKM-FC scheme has been evaluated using iFogSim to measure the performance parameters like throughput, end-to-end delay, packet loss, energy consumption and network usage. The overhead analysis of the proposed scheme is carried out and shows that the computation cost, communication cost and storage cost are improved compared to existing schemes.

[12] introduces LAAKA, a Lightweight Anonymous Authentication and Key Agreement scheme. Considering the constrained resources of IoT and fog devices, LAAKA utilizes lightweight operations such as hash function and bitwise XOR. Its main objective is to facilitate mutual authentication and establish secure session keys between IoT devices and fog servers, making it useful for various IoT applications. The robustness of LAAKA against various security threats is validates by conducting comprehensive formal security analysis, including Burrows-Abadi-Needham (BAN) logic and Random Oracle Model (ROM), as well as informal analysis. The efficacy of this scheme is further demonstrated through evaluation with the Scyther tool. Compared to other proposed authentication approaches, the results illustrate the superior performance and efficiency of this approach in enhancing the security features, minimizing the computational cost, and optimizing storage utilization.

[13] proposes a BSKM-FC (Blockchain-based Secured Key Management in a Fog Computing Environment) which is a decentralized system in a fog computing environment without using a third party. The BSKM-FC makes use of a one-way hash chain for the generation of private and public key pairs and ECC (Elliptic Curve Cryptography) for secured sharing. Upon successful authentication, the session key generation at both edge devices is based on the key pair provided by the fog server and stored securely in the blockchain. The BSKM-FC system uses private blockchain technology in the fog layer to provide secured storage and management. The work is implemented in the Truffle Blockchain and found that BSKM-FC performs better in terms of overall block preparation time. The security analysis of the proposed scheme is carried out based on the ROR model and also verified using AVISPA for some known attacks. Informal security analysis of the proposed work is performed by considering some of the known attacks where we observe that the proposed scheme overcomes such attacks. Performance overhead analysis is demonstrated using MIRACL considering computation cost, communication cost, and storage cost. The results show that the proposed scheme meets security requirements and performs effectively. The computation overhead, communication overhead, storage overhead, and block preparation time of the proposed scheme were improved, as compared to existing schemes.

[14] proposes an approach based on action-constrained deep reinforcement learning (DRL) to allocate computing resources securely. First, it considers a model of a serverless multi-cloud edge computing network with multiple computing resource nodes that possess various attribute characteristics. Then, designs a security mechanism to guarantee data security. Afterward, it formalizes the network model and objectives and further transforms them into a modeling process known as the Markov decision process. Finally, this study proposes DRL based on action constraints to provide an optimal resource allocation scheduling policy. Simulation results demonstrate that this approach can reduce system costs and improve working performance compared with the comparison schemes.

[15] presents a novel steganographic methodology, Product Cipher-Based Distributed Steganography (PCDS), designed to securely hide data within a multi-cloud environment. This approach, addressing the intricacies of decentralized data concealment, utilizes unaltered cover media as benchmarks for fragmenting and disguising data. The PCDS scheme, by distributing hidden data dynamically across multiple cloud platforms, successfully evades detection through the absence of file modifications or the use of special characters. An in-depth security analysis of this method demonstrates its resilience against unauthorized access; even with complete access to all cloud accounts involved, the extraction of the concealed message remains computationally unfeasible. The utilization of an undisclosed key, alongside a base encoding value and the

inherent computational complexity of the scheme, fortifies its defense against brute-force attacks, significantly elevating its security profile compared to existing methods. This paper contributes substantially to the field of cloud security and steganography by offering an undetectable and innovative approach for data hiding. It effectively counters prevailing vulnerabilities in multi-cloud storage and sets a new precedent for advanced secure data concealment strategies. Contrasting with conventional methods susceptible to brute-force attacks requiring substantially fewer computations, the PCDS framework ensures a higher level of security, providing robust protection for confidential data in cloud environments.

Table 2 shows the summary of recent research presented in the field of multi cloud and fog and its comparison with the proposed method.

II-II. KPS

KPS is divided into two categories: location-independent [16] and location-dependent [17]. If in a scheme, the nodes have no information about their location in the network, we call that scheme location-independent and otherwise, location-dependent. Table 3 shows a comparison of these schemes.

II-II-I. Location-Independent Schemes

In this section, some important location-independent KPS will be introduced.

A. BIBD-BASED HYBRID DESIGN: This scheme is a definite key distribution scheme, meaning that the key chain stored in each node is definitely pre-designed. In [18]-[19], the BIBD scheme is used to construct the key chain, and two schemes, called the symmetric scheme and the symmetric hybrid scheme, are presented. One of the problems with symmetric scheme is its scalability. In this scheme, due to the fact that a complete connection is established, the probability of key sharing is much higher than probabilistic and random schemes, but, the resiliency of this scheme is low.

Due to the mentioned limitations, in [18]-[19] another design called symmetric hybrid design is presented. This scheme is a combination of symmetrical design and its complement. In this way, the good properties of the hybrid schemes and the strength and scalability of the probabilistic schemes are combined to produce better results. Although this hybrid design improves scalability, the probability of key sharing relative to the symmetric design is reduced. In addition, overhead of key storage is large. [20] Provides a solution that requires O ($\sqrt{n}$) of memory but still has limited support for large networks. The difference with this symmetric block design is that it does not guarantee that both desired nodes have a common key with each other, but it does guarantee that both desired nodes can connect to each other through an intermediate node.

B. TRADE-BASED HYBRID DESIGN: [21] Presents a hybrid KPS called Trade-KP. A t-(v, k)-Trade contains the set $T=\{T_1, T_2\}$ in which each of the $T_i(i = 1,2)$ is a set of k member blocks selected from a finite set X so that each set t of members of set X is repeated in the same number of blocks T_1 and T_2. The maximum supported nodes by this scheme is $2p^2$.

C. UNITAL-BASED HYBRID DESIGN: The scheme presented in [22] for a finite set X with v points is as follows:

$$2\text{-}(p^3+1, p^2(p^2-p+1), p^2, p+1, 1) \quad (1)$$

Where has has $p^2(p^2-p+1)$ blocks and $v=p^3+1$. Each block contains p + 1 member and each member contains p^2 blocks.

To map this design to hierarchical networks, from the set of keys with size p^3+1 the number $b=p^2(p^2-p+1)$ of the key chain with size k = p + 1 is selected and assigned them to each node. To raise the probability of that two distinct nodes have a common key, so that the network resiliency remains high, a method called t-UKP and is based on the Unital scheme has been used. In this scheme, a number of separate t blocks are assigned to each node. The value of t is depending on the type of application of this scheme. In the initial method, only one Unital block is assigned to each node.

While in this method, each node is assigned a number of separate t blocks. This means that both nodes will have a common key between zero and t^2. In other words, each node is assigned a number of t(p + 1) separate keys.

In the new method, the network's resiliency increases because the attacker has to capture more common keys to destroy the secure connection. This method also increases the probability of connection between nodes, because each node is assigned a separate number of t-blocks.

II-II-II. Location-Dependent Schemes

In this section, some important location-Dependent KPS will be introduced.

A. Group-Based Design: In this scheme, the nodes are distributed in groups in the environment. The nodes can be thought of as deploying a helicopter to disperse them. When the helicopter lands at a point called the deployment point, the nodes spread in the same area. With this setup, the exact location of each node is still unrecognizable, but it is clear that the nodes spread out at one point will be close together. In this design, the node location distribution model is assumed to be a normal two-dimensional distribution. In this method, nodes that are more likely to be neighbors are assigned more common keys before they are established. Then, the steps of discovering the common key and establishing the route will be done as in the Eschenauer and Gligor scheme [23].

Table 2. Summary the recent research in multi cloud and fog and its comparison with the proposed method

Research	Technique	Performance Parameters	Description	Field
[9]	ROR model	Low Computation and Communication costs	The scheme secures against privileged insider attacks, ensures user anonymity, un traceability, and session secrecy.	Cloud-Fog-Device Framework
[10]	Innovative by the incorporation of the 5G	Low Transmission and Computation costs	This study improves security by introducing a stateless authentication mechanism and conducting a comparative analysis of the proposed protocol with well-known alternatives, such as TLS 1.3, 5G-AKA, and various handover protocols.	Edge-Fog-Cloud Framework
[11]	TAKM-FC scheme based on the ROR model	Low Computation, Communication and Storage cost	The proposed scheme is verified using the ProVerif tool. Then has been evaluated using iFogSim to measure the performance parameters	Authentication between Edge devices in Fog
[12]	LAAKA	High Security Features, Low Computation and Storage cost	The robustness of LAAKA against various security threats is validates by conducting comprehensive formal security analysis, including Burrows-Abadi-Needham (BAN) logic and Random Oracle Model (ROM), as well as informal analysis. The efficacy of this scheme is further demonstrated through evaluation with the Scyther tool.	Secure session between IoT devices and Fog servers
[13]	BSKM-FC	Low Computation, Communication and Storage overheads, and Low Block preparation time	The BSKM-FC system uses private blockchain technology in the fog layer to provide secured storage and management. The work is implemented in the Truffle Blockchain and found that BSKM-FC performs better in terms of overall block preparation time. The security analysis of the proposed scheme is carried out based on the ROR model and also verified using AVISPA for some known attacks.	Fog Computing Environment
[14]	DRL	Low System costs and High Working performance	First, it considers a model of a serverless multi-cloud edge computing network with multiple computing resource nodes that possess various attribute characteristics. Then, designs a security mechanism to guarantee data security	Multi-Cloud Edge Computing
[15]	PCDS	Low Computation overheads and High Resiliency	This approach, addressing the intricacies of decentralized data concealment, utilizes unaltered cover media as benchmarks for fragmenting and disguising data. The PCDS scheme, by distributing hidden data dynamically across multiple cloud platforms, successfully evades detection through the absence of file modifications or the use of special characters.	Multi-Cloud Environment
Proposed Method	Pre-Distribution Scheme Based on SBIBD and RD	High Scalability, Resiliency and Connectivity, Low Communication, Memory and Computing overheads	In this method, by using the SBIBD, blocks are generated to be assigned to the cloud nodes, and by using the residual design on the SBIBD, classes and blocks are created to be assigned to the fog nodes and end devices.	Multi-Cloud Environment

Table 3. Comparison of KPS

Scheme	Communication overhead	Computation overhead	Memory overhead	Resiliency	Scalability	Location
BIBD-Based	O(log N)	O(1)	O()	Low	Low	Independent
Trade-Based	O(p)	O(p)	O(p)	Low	High	Independent
Unital-Based	O(log N)	O()	O()	High	Low	Independent
Group-Based	O(g)	O(g)	O(g)	High	Low	Dependent
Attack Probability-Based	O(p)	O(p)	O(p)	High	Low	Dependent
LKE	O(log N)	O(t)	O(t)	High	Low	Dependent

B. Attack Probability-Based Design: Based on [24], this is a development of a group-based model that also considers the possibility of attacking different groups. Considering the probability of attack, the distribution of keys is done in such a way as to provide more protection to the nodes that are most attacked. In this method, more keys are assigned to these nodes because the logic of this design is that more keys provide more security.

C. Location-aware Key Establishment (LKE) Design: In this scheme, the nodes know their location. Once the network is established, the covered area is divided into sub-areas, in each of which a server node is selected by the voting algorithm. This node randomly forms a two-variable symmetric polynomial of degree t with the first two numbers p and p. The server node sends the public key to all nodes below the region. Each S_i node then sends a random key generated by K_i and its coordinates $(x_i.y_i)$ to the server node after receiving the public key. For all nodes in a subdomain, the server node sends a univariate polynomial containing the coordinate information $(x_i.y_i)$ to the S_i node. Two distinct nodes find a common server node and perform operations on univariate polynomials for find a common key [25].

II-III. MATHEMATICAL CONCEPTS

In this section, the mathematical concepts used in the proposed method are explained.

Definition 1. A Latin square on the q symbol is an instructor matrix p×p so that each symbol appears only once on each level or in each column. The order of this Latin square is p.

Definition 2. Based on Latin squares, Mutually Orthogonal Latin Squares (MOLS) is defined. Suppose $A=(a_{ij})$ and $B=(b_{ij})$ are two Latin squares p×p. These two squares are orthogonal if their placement on top of each other produces a square with distinct elements. Latin squares $A_1, A_2, \ldots, A_n$ are MOLS if they are orthogonal in pairs.

Definition 3. BIBD is to arrange distinct objects (v) in blocks (b) so that each block contains k distinct objects and each object exists exactly in r different blocks, and each two distinct objects

appears exactly in λ blocks. This design is represented as (v, k, λ)-BIBD or (v, b, r, k, λ)-BIBD where $\lambda \times (v-1) = r \times (k-1)$ and $b \times k = v \times r$.

For example, consider the set S={1,2,3,4,5,6,7,8,9}. The scheme (9, 12, 4, 3, 1) is a BIBD on the set S, because 1×(9-1)= 4×(3-1) and 12×3=9×4 on this scheme is applies. (9, 12, 4, 3, 1)-BIBD means that 9 objects are placed in 12 blocks so that each block has 3 distinct objects and each object exists in exactly 4 different blocks. Also, each pair of distinct objects appears in exactly one block. The blocks of this scheme on the set S will be as follows:

B_1={1,2,3} , B_2={4,5,6} , B_3={7,8,9} , B_4={1,4,7} , B_5={1,5,9} , B_6={1,6,8}

B_7={2,4,9} , B_8={2,5,8} , B_9={2,7,6} , B_{10}={3,4,8} , B_{11}={3,5,7} , B_{12}={3,6,9}

Definition 4. If in the BIBD, b = v and therefore r = k, the design is called SBIBD and is displayed as (v, k, λ)-SBIBD. For each prime number p≥2, a $(p^2+p+1, p+1, 1)$-SBIBD there exists.

For example, consider the set X = {1, 2, 3, 4, 5, 6, 7}. The scheme (7, 7, 3, 3, 1) is a BIBD on the set X, because 1 × (7-1) = 3 × (3-1) and 7 × 3 = 7 × 3 on this scheme is applies. According to this scheme, v = 7, b = 7, r = 3, k = 3 and λ = 1. Therefore, the proposed BIBD can be presented as (7, 3, 1)-SBIBD. The blocks of this scheme on the set X will be as follows:

B_1={1.2.3} , B_2={1.4.5} , B_3={1.6.7} , B_4={2.4.6} , B_5={2.5.7} , B_6={3.4.7} , B_7={3.5.6}

Definition 5. A Projective plane consists of a set of lines, points, and the relationship between them (point and line intersection) where exactly one line passes through both distinct points, the intersection of both arbitrary lines is exactly one point, p+1 lines pass through each point, and each line contains p+1 points. Therefore, a Projective plane is a SBIBD ($(p^2+p+1, p+1, 1)$-SBIBD).

Definition 6. Suppose (X,B□) is a (v, k, λ)-SBIBD where $X=\{x_1,x_2,\ldots,x_v\}$ is set of objects and $B□=\{B_1, B_2,\ldots,B_v\}$ is finite set of subsets of X. Then for each $1 \le i \le v$, $B_1\backslash B_i, B_2\backslash B_i, \ldots, B_{i-1}\backslash B_i, B_{i+1}\backslash B_i, \ldots, B_v\backslash B_i$ are blocks of one (v-k, v-1, k, k-λ, λ)-BIBD from the set of points $X\backslash B_i$ which $k \ge \lambda + 2$.

Therefore, $Res(X,B□,B_i)=\{X\backslash B_i, \{B\backslash B_i : B \in B□, B \neq B_i\}\}$ is called the RD of BIBD. In other words, the RD is created by deleting all points that are not in B_i and then deleting. The RD is a BIBD and the size of the blocks is larger than one and one unit smaller than the number of points.

For example, in **Definition** 4, the set X with its blocks $(B_1,B_2,B_3,B_4,B_5,B_6,B_7)$ was explained. The RD sets $(B_i\backslash B_j)$ and classes $(C_1,C_2,C_3,C_4,C_5,C_6,C_7)$ are obtained from $X\backslash B_1$, $X\backslash B_2$, $X\backslash B_3$, $X\backslash B_4$, $X\backslash B_5$, $X\backslash B_6$, $X\backslash B_7$ as follows:

$C_1=X\backslash B_1$={4.5.6.7} ,

$B_2\backslash B_1$={4.5} , $B_3\backslash B_1$={6.7} , $B_4\backslash B_1$={4.6} , $B_5\backslash B_1$={5.7} , $B_6\backslash B_1$={4.7} , $B_7\backslash B_1$={5.6}

$C_2=X\backslash B_2$={2.3.6.7}

$B_1\backslash B_2$={2.3} , $B_3\backslash B_2$={6.7} , $B_4\backslash B_2$={2.6} , $B_5\backslash B_2$={2.7} , $B_6\backslash B_2$={3.7} , $B_7\backslash B_2$={3.6}

$C_3 = X \backslash B_3 = \{2.3.4.5\}$

$B_1 \backslash B_3 = \{2.3\}$, $B_2 \backslash B_3 = \{4.5\}$, $B_4 \backslash B_3 = \{2.4\}$, $B_5 \backslash B_3 = \{2.5\}$, $B_6 \backslash B_3 = \{3.4\}$, $B_7 \backslash B_3 = \{3.5\}$

$C_4 = X \backslash B_4 = \{1.3.5.7\}$

$B_1 \backslash B_4 = \{1.3\}$, $B_2 \backslash B_4 = \{1.5\}$, $B_3 \backslash B_4 = \{1.7\}$, $B_5 \backslash B_4 = \{5.7\}$, $B_6 \backslash B_4 = \{3.7\}$, $B_7 \backslash B_4 = \{3.5\}$

$C_5 = X \backslash B_5 = \{1.3.4.6\}$

$B_1 \backslash B_5 = \{1.3\}$, $B_2 \backslash B_5 = \{1.4\}$, $B_3 \backslash B_5 = \{1.6\}$, $B_4 \backslash B_5 = \{4.6\}$, $B_6 \backslash B_5 = \{3.4\}$, $B_7 \backslash B_5 = \{3.6\}$

$C_6 = X \backslash B_6 = \{1.2.5.6\}$

$B_1 \backslash B_6 = \{1.2\}$, $B_2 \backslash B_6 = \{1.5\}$, $B_3 \backslash B_6 = \{1.6\}$, $B_4 \backslash B_6 = \{2.6\}$, $B_5 \backslash B_6 = \{2.5\}$, $B_7 \backslash B_6 = \{5.6\}$

$C_7 = X \backslash B_7 = \{1.2.4.7\}$

$B_1 \backslash B_7 = \{1.2\}$, $B_2 \backslash B_7 = \{1.4\}$, $B_3 \backslash B_7 = \{1.7\}$, $B_4 \backslash B_7 = \{2.4\}$, $B_5 \backslash B_7 = \{2.7\}$, $B_6 \backslash B_7 = \{4.7\}$

III. PROPOSED METHOD

In this section, the proposed KPS in multi-clouds fog networks will be explained, which includes the network model, how to build a RD and convert from RD to KPS.

III-I. NETWORK MODEL

The hierarchical fog network in the proposed scheme has EDs in the lowest layer, FNs in the middle layer, and CLs in the highest layer. We categorize EDs into different clusters and consider them as CNs and FNs as CHs.

In the proposed scheme, first, based on the SBIBD, blocks are made and assign to the CLs. Therefore, CLs communicate with each other directly or through other CLs.

Then, the RD is applied to the blocks created in the previous step to generate classes and RD sets and map classes to FNs as CHs and RD sets to EDs as CNs. Therefore, the CNs have a common key with all nodes except the nodes whose elements have been removed from the cluster, so each node can choose any CH as its CH.

To increase connectivity and reduce communication and computation overheads, it is necessary for CLs to be able to communicate with each FN directly. Therefore, each CL randomly selects a key from each key chain of FNs and adds it to its key chain.

To increase capture resistance, each cluster's key space is separated after distribution. In this way, after the distribution, the CH randomly generates a number that is unique in each cluster and sends it to the nodes encrypted with the common key of each node and the CH. This random number is then added to the end of each key in CNs and CHs.

After KP, the EDs search for their neighbors that have common key with them and send a list of own key identifiers to each other. To do this, each ED distributes its key identifiers through

a distribution network to find other devices in its cluster. CNs that do not have a common key, discover the key through headers. In this way, CNs share their key identifiers through CHs to create a common path.

According to the above, the proposed method can be divided into three phases as follows:

Phase 1, KP Phase: In this phase, a key repository will be created using a secure base station or distribution center and a number of p^2+p+1 blocks will be generated by SBIBD that we assign them to the CLs.

Then, using the proposed RD, the key chains will be generated as $(p^2+p+1)^2$, of which (p^2+p+1) will be assigned to the FNs as CHs and $(p^2+p+1)(p^2+p)$ will be assigned to EDs as CNs.

After that, each CL randomly selects a key from each key chain of headers and adds it to its key chain.

Phase 2, Common Key Discovery Phase: In this phase, the EDs search for their neighbors who have a common key with them and send each other a list of their key identifiers. To do this, each ED distributes its key identifiers through a distribution network to find other devices in its cluster.

Phase 3, Path Creation Phase: In this phase, CNs that do not have a common key, discover the key through the CHs. In this way, CNs share their key identifiers through CHs to create a common path.

Algorithm 1 shows the proposed method's algorithm.

III-II. HOW TO BUILD A RD

The main core of the offered scheme is using the RD to produce the primary keys in the pre-distribution phase. To make this design, we use finite image planes with order p which, as described in section II, is a special type of SBIBD. To build this design, we consider several features:

A: The set of points in the proposed method make (v.b.r.k.λ)-BIBD=$(p^2,p^2+p,p+1,p,1)$.

B: Suppose in the symmetric design the size of the key ring is k= p+1 and the size of the key space is equal to $v=p^2+p+1$, then the maximum size of network that supports by proposed RD is $(p^2+p+1)^2$. Because each class forms a RD $(p^2,p^2+p,p+1,p,1)$-BIBD and p^2+p+1 is the number of classes, can support $(p^2+p+1)(p^2+p)$ CNs. Each class can also be assigned to CHs. So $(p^2+p+1)(p^2+p)+(p^2+p+1)$ node that equal to $(p^2+p+1)^2$ can be covered.

III-III. CONVERT FROM RD TO KEY DISTRIBUTION

Before the nodes are distributed, they are loaded by the key chain that generated by the BS. The key chains are generated based on Res(X, $\overline{B}$, B_i). Each B_j^i in Res(X, $\overline{B}$, B_i) is used to assign the key

chain $K_{i,j}$ to CN_j^i that $1 \leq i \leq p^2 + p$. Each C_i is stored as a key chain in CH_i. At this stage, we need to have a mapping of the RD to the KPS to assign the key chains extracted from the key repository to the nodes. Table 4 shows this mapping [26].

IV. ANALYSIS OF THE PROPOSED METHOD

IV-I. SIMULATION

According to [27]-[28], in order to simulate a network, in the node location, two values must be specified: one is the number of nodes (n) and the other is the radio range of each node.

The radio range of nodes is denoted by a circle with r (radius) which is $0 < r < 1$. In this case, by connecting each node to another node on its radio board, a graph is obtained. Since in calculations, the location of the nodes and the radio range are in order to find the nodes that are in the vicinity of a node, in the resulting graph, the degree of each node can be considered instead of its location. The relationship between the degree of each node (d) and the radio range r is calculated from the below equation [28]:

$$\mathbf{d} = (\mathbf{n} - \mathbf{1})(\boldsymbol{\pi}\mathbf{r}^{\mathbf{2}} - \frac{\mathbf{8}}{\mathbf{3}}\mathbf{r}^{\mathbf{3}} + \frac{\mathbf{1}}{\mathbf{2}}\mathbf{r}^{\mathbf{4}}) \quad (2)$$

Therefore, in simulation, it is necessary to specify only the n and the average of d. The equivalent of a network is then considered a random graph with n and d.

In [29] it is stated that in order for the resulting random graph to be connected with probability c, the mean degrees of the vertices of the random graph must be in accordance with below equation:

$$d = \frac{n-1}{n}(\ln(n) + \ln(-\ln(c))) \quad (3)$$

In the above relation, the value of c is assumed to be 0.9 in order to obtain the most likely connected random graph.

IV-II. PERFORMANCE EVALUATION

In this section, examination the parameters of scalability, connectivity, resiliency, node mobility model and overheads of memory, communications and computations is done.

IV-II-I. Memory Overhead

Memory overhead can be examined from two parameters: one is the number of keys in the key ring of each node and the amount of support for the maximum node with a same number of keys and the other is the memory consumption of each node.

Due to the use of the RD for KPS, the number of keys will depend on the order of the scheme

Algorithm 1 Proposed method's algorithm

Input: N

The largest p is found where $p^2 + p + 1 < N$;

Generate the first $(p^2 + p + 1. p + 1.1) - SBIBD$ with the $X = \{K_1. K_2. \ldots . K_v\}$;

Generate blocks $\ddot{B} = \{B_1. B_2. \ldots . B_b\}$ from X and assign them to CLs;

Applying the RD as $Res(X. \ddot{B}. B_i)$ on $\ddot{B}$ and generate key chain as $(p^2 + p + 1)^2$;

Assign $(p^2 + p + 1)$ key chain to CHs and $(p^2 + p + 1)(p^2 + p)$ to CNs;

Select randomly a key from each CH key chain and add it to CLs key chain;

If two CNs have common key:

- True: CNs are neighbors
- False: Share key IDs by CHs and find common path between them;

Table 4. Map from RD to KPS

RD	KPS
Point Set (|S|)	Key Pool (KP)
Size of Object Set (|S| = p^2 +p+1)	Size of Key Pool
Blocks	Key Ring
Number of Blocks ((p^2+p+1)(p^2+p)))	Key Rings Number
Block Size (k=p)	Key Ring Size

Table 5. The proposed scheme comparison with similar schemes for keys in the key ring of each end node

Scheme	Keys in the key ring of each end node
[19]	p+1
[21]	p
[22]	p+1
[30]	p
Proposed Method	p

Table 6. The proposed scheme comparison with similar schemes in terms of the maximum number of supported CNs

Scheme	Maximum number of supported CNs
[19]	p^2+p+1
[21]	$2p^2$
[22]	p^2 (p^2-p+1)
[30]	p^2
Proposed Method	(p^2+p+1)(p^2+p)

used. For example, if a RD scheme with order p is used, each CN will be loaded with a separate p key. Table 5 and Table 6 show the proposed scheme comparison with other hybrid designs. Since the ratio of CHs and CLs to CNs in the proposed design is equal to $\frac{1}{p^2+p}$ and very low, they are not considered in this comparison [26]. From Table 5 and Table 6 can understand that compared to similar methods, proposed scheme supports a larger network with fewer keys in key ring per node. Fig. 1 shows the details of this comparison.

Using $(p^2+p+1,p+1,1)$-SBIBD and RD, p^2+p+1 cluster where each cluster is a $(p^2,p^2+p,p+1,p,1)$-BIBD can produced which the number of CHs is p^2+p+1 and the number of CNs is $(p^2+p+1)(p^2+p)$. In the KPS based on the RD, each CH with a key chain of length p^2+p to communicate with its own nodes plus a key chain of the BIBD scheme to communicate with other BIBDs that is approximately equal to $\sqrt{p^2+p+1}\big)$ is loaded. As a result, the amount of memory required to load each CH can be calculated from the following equation:

$$\left((p^2+p)+\sqrt{p^2+p+1}\right)\times S^k \quad (4)$$

By the way, the key chain length of each CN in the RD is equal to p, so the amount of memory required for each CN is equal to $p\times S^k$, where S^k is equal to the key size in symmetric cryptography [26].

KP has many advantages over public key protocols in a hierarchical network, one of which is the amount of memory consumed by nodes [29]-[31]. In [32]-[33], two public key-based schemes for hierarchical networks are presented, which we compare the proposed method in the amount of memory consumed by each node with them. For comparison, suppose the total network size is $(p^2+p+1)^2$ with p^2+p+1 clusters and each cluster having p^2+p CNs. If A^k is the key size in general encryption and d_m is the maximum degree of neighborhood, Tables 7 and 8 show a comparison of the offered design with those designs.

IV-II-II. Communications Overhead

In the proposed scheme, the maximum path length between two nodes depends on the key chain length, which is p + 1. Therefore, the average communication overhead is of order O(p).

IV-II-III. Computations Overhead

In KPS, base stations have the highest computational overhead, but this overhead does not interfere with the overall process of the method. In the proposed method, each node requires a time equal to p + 1 for computations. As a result, the average computational overhead is of order O(p).

IV-II-IV. Connectivity

If we consider the global connectivity equal to the probability of finding a common key between two distinct nodes and call it Pc, we must first calculate the local connectivity (Pc_j), which is equal

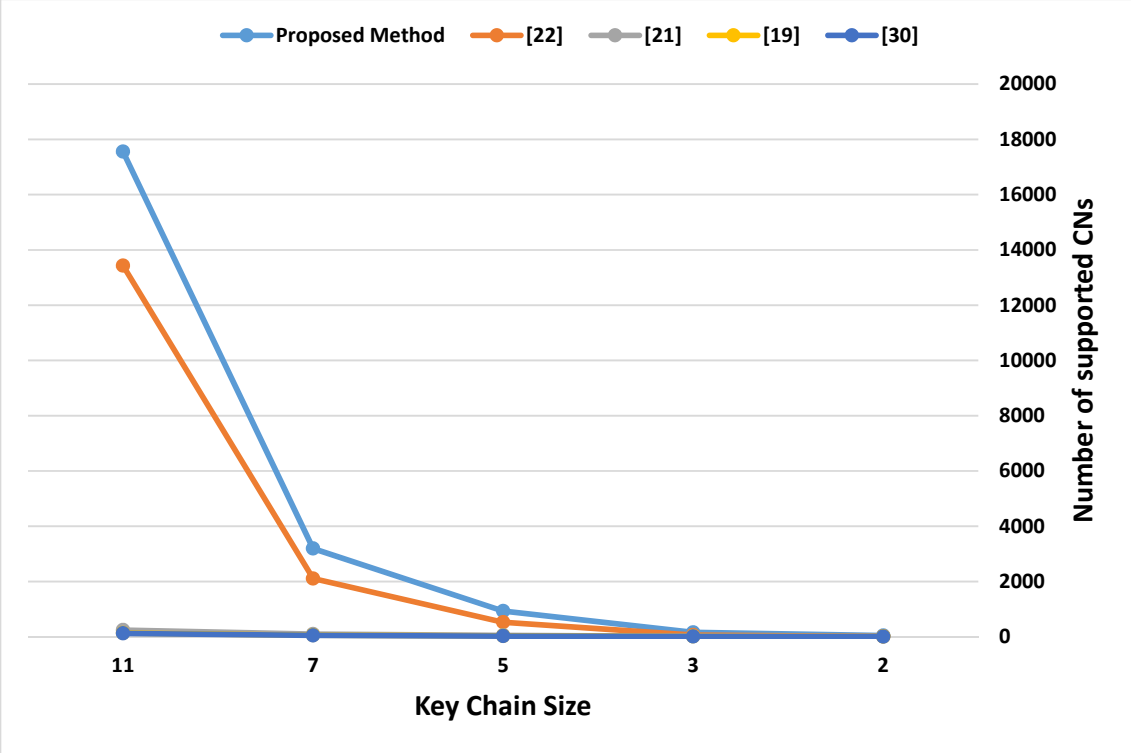

Fig. 1. The proposed scheme comparison with similar schemes in terms of network size

to the connectivity of each cluster. Then the Pc is calculated with calculating the weighted average of Pc_j obtained in the whole network. As described in section II, the use of BIBD falls into the category of location-independent KPS, so a node mobility model is not required for the proposed connectivity calculation scheme.

If use RD for KPS, from the p^2+p key chain that are possible in each cluster, each key appears in p+1 of them. If we consider two nodes CN_i^j and CN_z^j in cluster j that are selected randomly, CN_i^j is already with a key chain with a separate key p and CN_z^j is already with a separate key p once loaded, each key is located at CN_i^j in p of the key chain (p + 1-1 = p) through p^2+p-1 of the existing key chain. Also, since $\lambda = 1$, each key pair appears exactly in the same key chain. So we find that key chains that contain two separate keys from the CN_i^j key chain are completely separate. Therefore, each node shares a key with a number of other nodes (((r-1) × k) = p × p) among the available nodes (p^2+p-1). As a result, Pc_j is equal to $\frac{p^2}{p^2+p+1}$ and with assume that n_j is the number of CNs in cluster j, which according to the RD is equal to p^2+p, the Pc can be calculated from the following equation [26]:

$$Pc = \frac{\sum_{i=1}^{c} n_j \times Pc_j}{N} = \frac{\sum_{i=1}^{c} n_j \times Pc_j}{(p^2+p+1)(p^2+p)} = \frac{(p^2+p+1)(p^2+p)(p^2)}{(p^2+p+1)(p^2+p)(p^2+p-1)} = \frac{p^2}{p^2+p-1} \quad (5)$$

Fig. 2 shows the proposed scheme probability of communication in one step. As can be seen

Table 7. The proposed scheme comparison with similar schemes in terms of memory required by each CH

Scheme	Memory required by each CH
[32]	$(2p^2+2p+2)\times A^k$
[33]	$(p^4+2p^3+2p^2+p+2)\times A^k$
Proposed Method	$((p^2+p)+\sqrt{p^2+p+1})\times S^k$

Table 8. The proposed scheme comparison with similar schemes in terms of memory required by each CN

Scheme	Memory required by each CN
[32]	$(p^2+p+2)\times A^k$
[33]	$(p^2+p+3)\times A^k+(d_m\times S^k)$
Proposed Method	$p\times S^k$

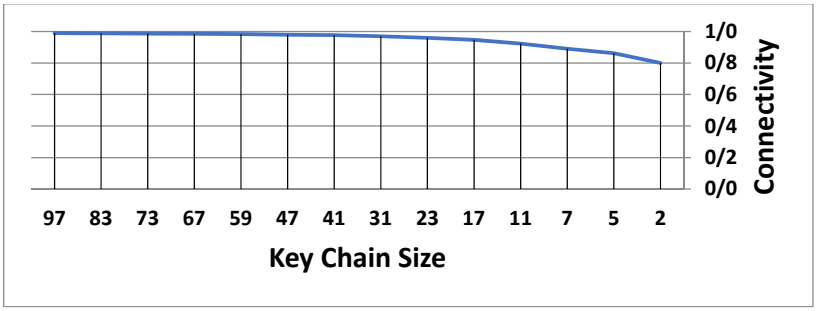

Fig. 2. The proposed scheme probability of communication in one step

in Fig. 2, the probability of communication in one step in the proposed method is very high and is close to 1.

IV-II-V. Network Resiliency

Because the keys are distributed to the nodes before the network distribution, so the pre-distribution phase in the proposed method is secure. Therefore, the attacker has no information about the key store and key chain of each node. Also, assuming an attack in the shared key discovery phase, there will still be no problem for the network, because at this phase, the nodes only exchange key identifiers, and the attacker will not have access to the keys stored in the nodes. Even if the attacker knows the key ID, but does not know the key ID mapping method, he will not be able to recognize the exchanged messages [34]. Therefore, the network is safe from attack until the method of identifying the ID is revealed.

It is explained in [35] that the physical attack is the first step in other network attacks, which compromises the node connections throughout the network by accessing the security keys stored in the nodes. Therefore, in this article, network resistance based on this type of attack has been investigated. For this purpose, we check what effect on other nodes if x nodes ($x\leq(p^2+p+1)^2$) are

captured. Also, if x nodes are captured in a cluster, what is the probability that the attacker can decrypt the communication between two hypothetical nodes "a" and "b" in that cluster? We call this probability $P(L \mid N_x)$ and are looking to find it. Relations 6, 7 and 8 are the proof and finding this probability.

In the first step we need to find the probability that a secure connection (l) is secured with k (l_k). Since in each cluster, each key is found in p+1 CNs, this probability is calculated from the following relation:

$$P(l_k|l) = \frac{\binom{p+1}{2}}{\binom{(p^2+p+1)(p^2+p)}{2}} \quad (6)$$

The next parameter to be calculated is if x nodes in the network are attacked (N_x), with what probability the block contains the k (B_k) will also be attacked. This probability is obtained from the following relation:

$$P(B_k|N_x) = 1 - \frac{\binom{(p^2+p+1)(p^2+p)-(p+1)}{x}}{\binom{(p^2+p+1)(p^2+p)}{x}} \quad (7)$$

The last parameter required is the probability that a secure connection secured by k (C_k) will also be attacked if x nodes are attacked. This probability is obtained from the following relation:

$$P(C_k|N_x) = P(l_k|l)P(B_k|N_x) \quad (8)$$

At the end, $P(L \mid N_x)$ is obtained from below relation [26]:

$$P(L|N_x) = \sum_{k=1}^{p^2+p+1} P(C_k|N_x) \quad (9)$$

On [19]-[21], the probability of conquest for the BIBD-based hybrid method and the Trade-based hybrid method are explained. Fig. 3 shows the probability of conquering the offered method and similar methods for keys of lengths 11, 19, 29 and 53 in the case where 10 nodes have been attacked, and Fig. 4 shows this probability for the case where 100 nodes have been captured.

IV-II-VI. Scalability

It is explained in [26] that in the block schemes used for KP, if more nodes can be supported with a shorter key chain length, the design is more scalable. In other words, network scalability is measured based on the number of blocks produced, each block corresponding to a key chain. In pre-distribution based on RD rank p, the number of nodes that can be supported by the design is the same as the number of generated key chains. Since according to RD, each cluster forms a $(p^2,p^2+p,p+1,p,1)$-BIBD and the number of clusters is equal to p^2+p+1 and there are p^2+p nodes in each cluster, so the sum of nodes in a cluster is equal to $(p^2+p+1)(p^2+p)$. This number should be added to the number of clusters. As a result, the total number of supported nodes in the proposed method is equal to $(p^2+p+1)^2$. Fig. 5 shows the proposed scheme comparison with similar schemes in terms of scalability.

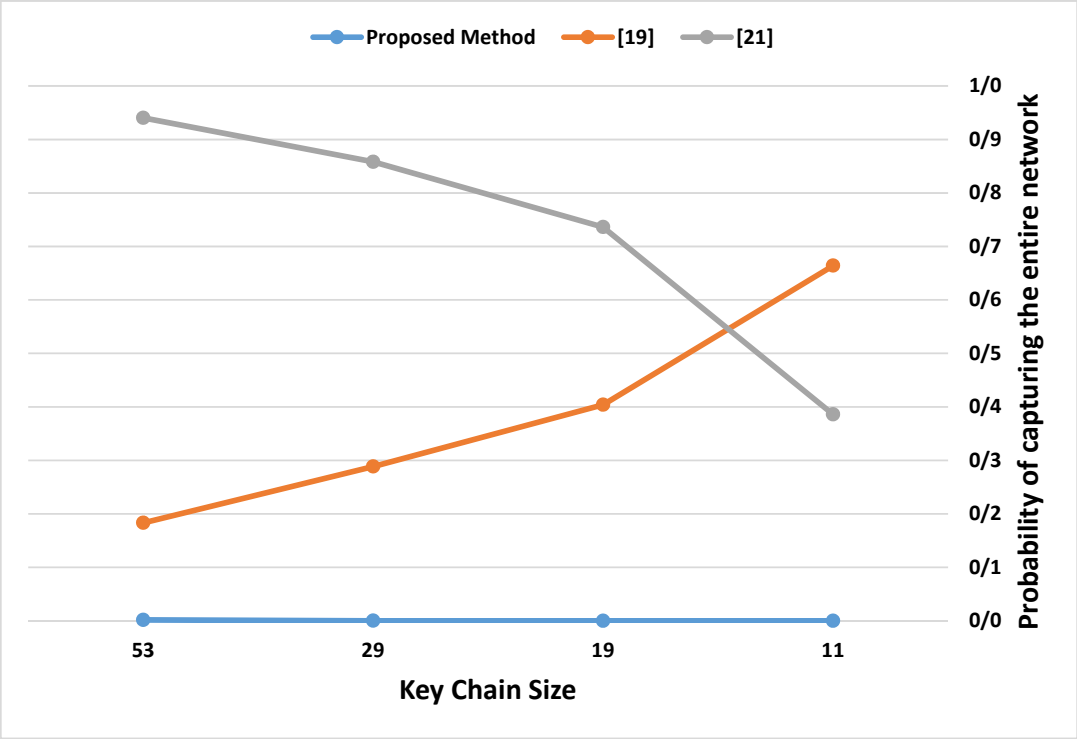

Fig. 3. The proposed scheme comparison with similar schemes in terms of the probability of capturing the entire network for the capture of 10 nodes

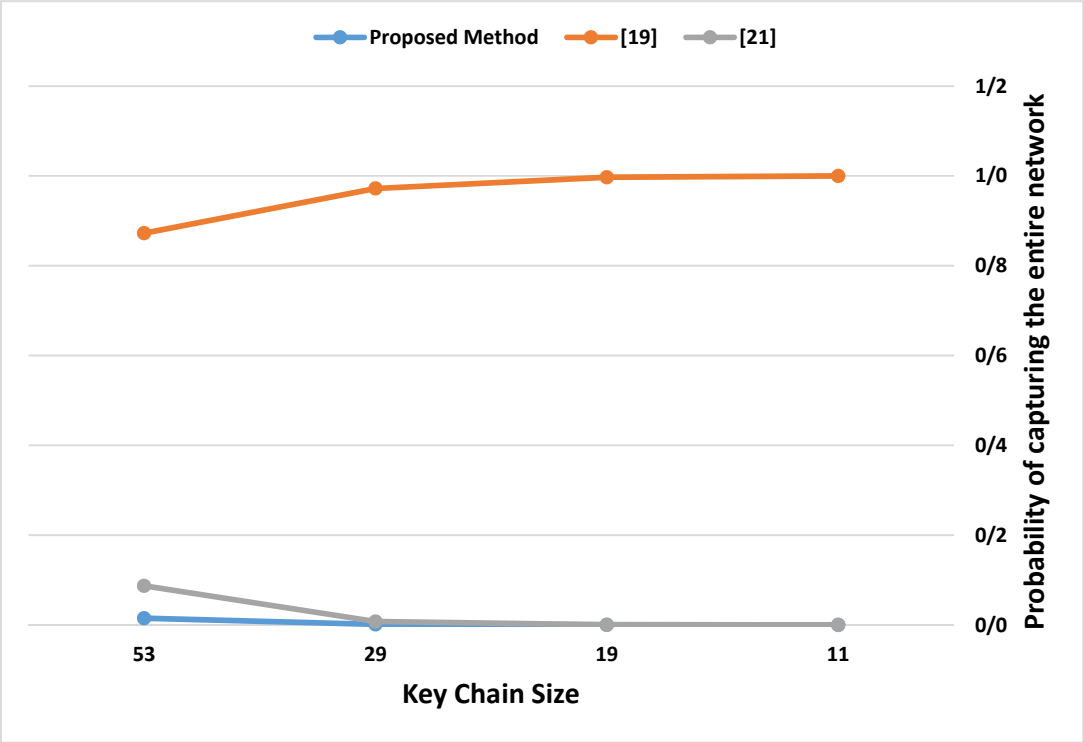

Fig. 4. The proposed scheme comparison with similar schemes in terms of the probability of capturing the entire network for 100 nodes

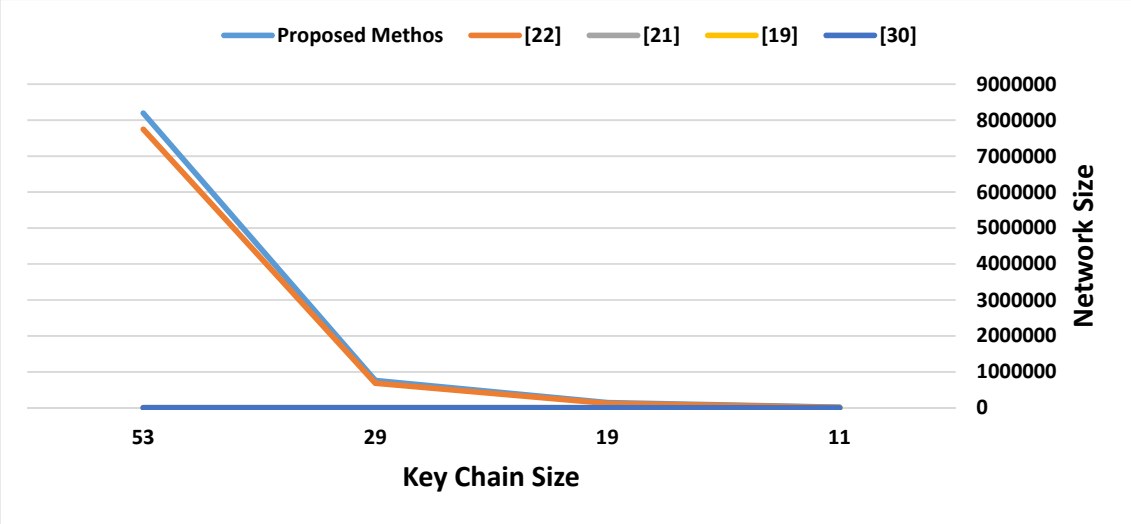

Fig. 5. The proposed scheme comparison with similar schemes in terms of scalability

IV-II-VII. Node Mobility

In [36], node mobility models and their effective parameters are described. In this article, it is explained that the node mobility model is independent from the encryption algorithm and depends on the routing algorithms and network topology. Also, the proposed method is based on SBIBD, which, as explained in section II, is a location-independent KPS method. As a result, the proposed method is completely independent of the node mobility model in the network, and node movement does not affect its performance.

V. DISCUSSION

In section IV, we evaluated the proposed method and compared it with other similar methods, which we summarize in this section. The communication and computation overheads of the proposed method are of the order of O(p), which is an acceptable value compared to the data in Table 3. According to Tables 7 and 8, the memory overhead of the proposed method is much lower than other methods. For example, the memory required for each CN in the [32] is 6 times and in the [33] is 8 times the proposed method and the memory required for each CH in the [32] is almost 2 times and in the [33] is 25 times the proposed method. Based on Fig.2, the network connectivity of the proposed method is above 0.8 and close to the BIBD design, which is a fully connected KPS. Based on Fig.3 and Fig.4, the probability of capturing the entire network in proposed method is about 0, while it is much higher in [19]-[21]. According to Table 6 and Fig.5, compared to [19]-[21]-[22]-[30], the scalability of the proposed method is higher and the proposed method supports more nodes with a shorter key chain. In the proposed method, for a network with size N, the size of the key chain is $\sqrt[4]{N}$

. Also, based on [36] and description of section II, the proposed method is completely independent of the node mobility model.

VI. CONCLUSION AND FUTURE WORK

In this paper, a KPS in fog networks is presented that used for multi-cloud fog networks. In this method, by using the SBIBD, blocks are generated to be assigned to the cloud nodes, and by using the residual design on the SBIBD, classes and blocks are created to be assigned to the fog nodes and end devices. We found that the proposed design with minimizing overheads of memory, communication and computation, increases scalability, connectivity and resiliency. Also, in this article, we showed that the proposed method is completely independent of the node mobility model and the movement of nodes in the network has no effect on its performance.

In proposed method, we checked physical attack model, so in future research, can review other attack models and provide a solution to further protect the CHs.

REFERENCES

[1] P. Asghari, A.M. Rahmani, and H.H.S. Javadi, "Privacy-aware cloud service composition based on QoS optimization in Internet of Things," Journal of Ambient Intelligence and Humanized Computing, vol. 13, no. 11, pp. 5295-5320, Jan. 2020.

[2] P. Asghari, A.M. Rahmani, and H. Haj Seyyed Javadi, "A medical monitoring scheme and health-medical service composition model in cloud-based IoT platform," *Trans. Emerging Telecommunications Technologies*, vol. 30, no. 6, p.e 3637, May 2019.

[3] M. Faraji Mehmandar, S. Jabbehdari, and H. Haj Seyyed Javadi, "A dynamic fog service provisioning approach for IoT applications," *International Journal of Communication Systems*, vol. 33, no. 14, p.e 4541, July 2020.

[4] M. Ghobaei-Arani, A. Souri, and A.A. Rahmanian, "Resource management approaches in fog computing: a comprehensive review," *Journal of Grid Computing*, vol. 18, no. 1, pp. 1-42, Sept. 2019.

[5] M. Etemadi, M. Ghobaei-Arani, and A. Shahidinejad, "Resource provisioning for IoT services in the fog computing environment: An autonomic approach," *Computer Communications*, vol. 161, no. 1, pp. 109-131, Sept. 2020.

[6] M. Iorga, L. Feldman, R. Barton, M.J. Martin, N.S. Goren, and C. Mahmoudi, "Fog computing conceptual model," *National Institute of Standards and Technology, no. NIST Special Publication (SP),* pp. 325-500, March 2018.

[7] A. Morshed Aski, H. Haj Seyyed Javadi and G.H. Shirdel, "A Full Connectable and High Scalable Key Pre-distribution Scheme Based on Combinatorial Designs for Resource-Constrained Devices in IoT Network," *Wireless Personal Communications,* vol. 114, no. 3, pp. 2079-2103, May 2020.

[8] N. Masaeli, H.H.S. Javadi and S.H. Erfani, "Key pre-distribution scheme based on transversal design in large mobile fog networks with multi-clouds," *Journal of Information Security and Applications*, vol. 54, no. 1, pp. 1-12, Oct. 2020.

[9] M. Hegde, R.R. Rao and R. Bhat, "Design of an efficient and secure authentication scheme for cloud-fog-device framework using key agreement and management," *IEEE Access*, vol. 12, no. 1, pp. 78173-78192, May 2024.

[10] J. Zhang, A. Ouda and R. Abu-Rukba, "Authentication and Key Agreement Protocol in Hybrid Edge–Fog–Cloud Computing Enhanced by 5G Networks," *Future Internet*, vol. 16, no. 6, pp.209-249, June 2024.

[11] N.C. Gowda, S.S. Manvi, A.B. Malakreddy and R. Buyya, "TAKM-FC: Two-way Authentication with efficient Key Management in Fog Computing Environments," *The Journal of Supercomputing*, vol. 80, no. 5, pp. 6855-6890, March 2024.

[12] H. Ali and I. Ahmed, "LAAKA: Lightweight Anonymous Authentication and Key Agreement Scheme for Secure Fog-Driven IoT Systems," *Computers & Security,* vol. 140, no. 1, pp.103770-103791, May 2024.

[13] N.C. Gowda, S.S. Manvi, B. Malakreddy and P. Lorenz, "BSKM-FC: Blockchain-based secured key management in a fog computing environment," *Future generation computer systems*, vol. 142, no, 1, pp.276-291, May 2023.

[14] H. Zhang, J. Wang, H. Zhang, and C. Bu, "Security computing resource allocation based on deep reinforcement learning in serverless multi-cloud edge computing," *Future Generation Computer Systems*, vol. 151, no. 1, pp. 152-161, Feb. 2024.

[15] S. S. Hashmi, A. A. Khan Mohammad, A. M. Abdul, C. Atheeq and M. K. Nizamuddin, "Enhancing Data Security in Multi-Cloud Environments: A Product Cipher-Based Distributed Steganography Approach," *International Journal of Safety & Security Engineering,* vol. 14, no. 1, pp. 47-62, Feb. 2024.

[16] W.K. Nicholson, "Introduction to abstract algebra," John Wiley & Sons, March 2012.

[17] A. Pattanayak and B. Majhi, "Key Predistribution Schemes in Distributed Wireless Sensor Network using Combinatorial Designs Revisited," *Cryptology ePrint Archive*, vol. 1, no. 1, p. 131, Jan. 2009.

[18] S.A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," *Rensselaer Polytechnic Institute,* vol. 1, no. 1, pp. 05-07, March 2005.

[19] S.A. Camtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Trans. Networking*, vol. 15, no. 2, pp. 346-358, April 2007.

[20] J. Lee and D.R. Stinson, "On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs," *ACM Trans. Information and System Security (TISSEC),* vol. 11, no. 2, pp. 1-35, May 2008.

[21] S. Ruj, A. Nayak and I. Stojmenovic, "Pairwise and triple key distribution in wireless sensor networks with applications," *IEEE Trans. Computers*, vol. 62, no. 11, pp. 2224-2237, Nov. 2013.

[22] W. Bechkit, Y. Challal, A. Bouabdallah and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks," *IEEE Trans. Wireless Communications*, vol. 12, no. 2, pp. 948-959, Feb. 2013.

[23] W. Du, J. Deng, Y.S. Han, S. Chen and P.K. Varshney. "A key management scheme for wireless sensor networks using deployment knowledge," *IEEE INFOCOM 2004*, vol. 1, no. 1, pp. 586-597, March 2004.

[24] S.P. Chan, "A key management scheme in distributed sensor networks using attack probabilities," *IEEE GLOBECOM* 2005, vol. 2, no. 1, pp. 1007-1011, Nov. 2005.

[25] F. Liu and X. Cheng, "LKE: a self-configuring scheme for location-aware key establishment in wireless sensor networks*," IEEE Trans. Wireless Communications*, vol. 7, no. 1, pp. 224-232, Jan. 2008.

[26] V. Modiri, H.H.S. Javadi and M. Anzani, "A novel scalable key pre-distribution scheme for wireless sensor networks based on residual design," *Wireless Personal Communications*, vol. 96, no. 2, pp. 2821-2841, Sept. 2017.

[27] R. Di Pietro, L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, "Redoubtable sensor networks," *ACM Trans. Information and System Security (TISSEC)*, vol. 11, no. 3, pp. 1-22, March 2008.

[28] T.M. Vu, C. Williamson and R. Safavi-Naini, "Simulation modeling of secure wireless sensor networks," *Fourth International ICST Conference on Performance Evaluation Methodologies and Tools*, vol. 1, no. 1, pp. 1-10, May 2010.

[29] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks," *9th ACM Conference on Computer and Communications Security,* vol. 1, no. 1, pp. 41-47, Nov. 2002.

[30] M. Javanbakht, H. Erfani, H.H.S. Javadi and P. Daneshjoo, "Key predistribution scheme for clustered hierarchical wireless sensor networks based on combinatorial designs," *Security and Communication Networks*, vol. 7, no. 11, pp. 2003-2014, Nov. 2014.

[31] J. Lopez, R. Roman and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks," *Foundations of Security Analysis and Design V,* vol. 1, no. 1, pp. 289-338, Sept. 2007.

[32] R. Riaz, A. Naureen, A. Akram, A.H. Akbar, K.H. Kim and H.F. Ahmed, "A unified security framework with three key management schemes for wireless sensor networks," *Computer Communications*, vol. 31, no. 18, pp. 4269-4280, Dec. 2008.

[33] R. Azarderskhsh and A. Reyhani-Masoleh, "Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, no. 1, pp. 1-12, Dec. 2011.

[34] R.R. Brooks, S.S. Iyengar and R. Brooks, "Distributed sensor networks," Chapman & Hall/CRC, December 2004.

[35] M. Conti, R. Di Pietro, L.V. Mancini and A. Mei, "Emergent properties: detection of the node-capture attack in mobile wireless sensor networks," *First ACM conference on Wireless network security*, vol. 1, no. 1, pp. 214-219, March 2008.

[36] M. Karyakarte, A. Tavildar and R. Khanna, "Effect of Mobility Models on Performance of Mobile Wireless Sensor Networks," *International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC*), vol. 3, no. 1, pp. 137-148, March 2013.