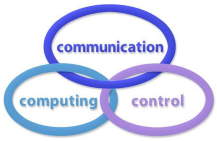
INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Online ISSN 1841-9844, ISSN-L 1841-9836, Volume: 17, Issue: 6, Month: December, Year: 2022
Article Number: 4363, https://doi.org/10.15837/ijccc.2022.6.4363



CCC Publications

Bi-Level Minimal Resource Protected Key Generation Framework For Fog Computing Applications

Arul Sindhia.P, Bharathi.R

Arul Sindhia.P
University College of Engineering Nagercoil, 629004, India
Corresponding author: arulsindhiaphd@gmail.com

Bharathi.R
University College of Engineering Nagercoil, 629004, India.
BharathiBharathi1993@hotmail.com

Abstract

Fog computing is a viewpoint that expands on the Cloud stage concept by placing processing assets at the organization's edges. It might be described as a cloud-like platform with comparable data, computation, storage, and applications. They are unique in that they are decentralized in nature. Data protection and route analysis of time-sensitive data are made easier using fog computing. This minimizes the volume and distance of data sent to the cloud, lowering the risk of security and privacy breaches in IoT applications. When it comes to security and privacy, fog computing confronts several issues. The constraints of fog computing resources are the root of these difficulties. The fog system, in fact, may raise new security and privacy concerns. To address these challenges, cryptography is used in conjunction with key management techniques to provide safe data transfer. A Minimal Resource Viterbi based Bi-level Secured Key Generation (MRV-BSKG) technique for a secured fog-based system is proposed to compromise the security level and computational complexity. The BSKG technique, which combines Lagrange's Key Generation (LKG) and the Location-Based Key (LBK) generation approaches, can safeguard secrecy and integrity. In comparison to the previous techniques, the new MRV, BSKG, delivers security with improved outcomes.

Keywords: Minimal Resource Viterbi based Bi-level Secured Key Generation (MRV-BSKG), Fog Computing, Lagrange's Key, Location-Based Key, Shortest path.

1 Introduction

Fog computing is in great demand in most real-time applications [1], including industrial automation systems, smart grid systems, smart cities, smart buildings, health care systems, surveillance and monitoring, traffic control systems, smart agriculture, and smart factories, among others. The Fog System platform is divided into three layers: the end user layer, the fog layer, and the cloud layer [2]. Fog System serves as a link between IoT devices and cloud computing. The fog computer gadget may send many types of new information. Cloud computing and fog computing have similar working

principles. Nonetheless, with cloud computing, the cloud can handle massive volumes of data utilizing virtual cloud resources which can be recovered from the cloud when necessary. The probability of network traffic due to a huge quantity of data transfer presents a key barrier in cloud computing [3]. The data transfer between the smart devices and the cloud requires adequate time and appropriate bandwidth. However, maintaining these standards during data transfer in cloud computing is difficult. There are additional issues with latency, location awareness, and mobility [4]. The Internet of Things (IoT) is becoming an inextricable aspect of the Internet's expanding privacy inside its bounds. However, IoT-based gadgets and tools face security and privacy risks, particularly because nodes are primarily meant to collect data about users' behaviours, keys, and surroundings, resulting in profitable, targeted invasions. CISCO has launched Fog Computing, an improved version of cloud computing, to address these concerns. Fog nodes are employed at the network's edge and act as a link between smart devices and the cloud. Smart population of devices are linked to fog edges rather than having direct touch with the cloud. The solution is ideal for any latency sensing applications without smart devices that can quickly obtain data thanks to fog computing. As a result, an approximation approach that provides scaled graphics processing with substantial acceleration is required. A vector-based machine learning algorithms is used [21] to approximate the shortest path distance in a large image. The main focus of the fog system is security, which can be achieved using fog forecasts and several key management schemes [5].It should be considered that the design of security methods has no impact on the system's performance. Fog-based system design with less security leads to fraudulent activities such as hacking of information about the users. Encryption technology will also be used to improve the security of fog-based systems.But the ineffective key management technique affects the communication between the user and the cloud [6]. So there is a demand for a highly secured Fog based system to make it suitable for time-sensitive applications. In this paper, fog based system with Bi-level Secured Key Generation (BSKG) method is proposed that combines Lagrange's Key Generation (LKG) and Location-Based Key (LBK) generation. During the data transmission from source to fog nodes, LKG is done using a source encoder, and in every fog node, LBK is done using a channel encoder. The generated key is a combination of alphabetical letters and numerical characters leading tohigh-level security. On the receiver side, the generated key is decrypted using the LBK method in the channel decoder and again decrypted using the LKG method in the source decoder and then stored in the cloud. Here, the information is secured in multiple levels by encoding at source and each node based on its position. This approach provides a common security mode and provide secured data as compared to other algorithms like attribute based encryption or machine learning model. The rest of the paper is as follows. Existing works relating to techniques for fog computing and key management are described in Section 2.The fog-based smart grid system model is presented in Section 3.Section 4 describes the structure of the proposed fog-based system for the main generation of two-level protection. Section 5 describes the functions of the proposed smart grid system, and Section 6 concludes the work.

2 Related work

Cloud computing and fog computing services provide the same data processing, from consumers to these collectors, which are then stored in the cloud [7, 8].Cloud computing is a three-level structure, while fog computing is a tri-level structure.This tri-level structure supports real time applications due to its better services in terms of Quality of Service (QoS), latency, geographical distribution and network traffic [9].To reduce the latency in fog computing, shortest path algorithms such as Dijikshtra, Thorup's algorithm, Pulse Coupled Neural Network (PCNN), Time Delay Neural Network (TDNN), etc. are discussed by Huang et al. which determines the minimum distance between the source and destination with the neural network. The main thing not to pay attention to in fog estimates is security and privacy issues. Only after the fog nodes collect sensitive information about the user will we send it to the cloud server.So, there may be a possibility for security threats [10].Key management techniques and cryptography algorithms can improve securities to fog nodes and cloud servers. Mate Horwath [11] has proposed Attribute-Based Encryption (ABE) that uses Linear Secret Sharing Scheme (LSSS),which supports multiple users. It is an identity-based user revocation that reduces the cloud's

computational overhead by increasing the computational overhead in both encryption and decryption. The modified structure of Ciphertext Policy ABE (CP-ABE) is presented in [12] that effectively exchanges the hierarchy files in the cloud to reduce the time required for decryption. Simultaneously, the user can get all files by using a single key, which reduces the overall system's cost. Peng Zhang et al. proposed a CP-ABE scheme to reduce the cloud's burden by transferring some computation processes to fog nodes [13]. In this structure, the number of attributes is independent of the encryption and decryption process. Key Management Scheme for Communication Layer (KMS-CL)method exploits an access control approach to improve the security during file transmission in fog nodes. It increases the computational complexity due to the outsourced encryption process. To provide better security and privacy services, privacy-preserving data aggregation methods are presented in [14-16]. In [11-13], ABE based mechanisms only were used for securing the data. The data can be hacked if the user information is leaked or hacked by third party. But, in [14 -16], this problem is overcome by using encryption mechanism; but its information is processed through third party and it also risk of information leakage. Lightweight Privacy Data Preserving Aggregation (LDPA) was proposed by Rongxing Lu et al. [17], primarily for IoT applications. To provide great security and privacy, it employs the Chinese Remainder Theorem (CRT) with Parlier encryption. The notion of shared keys is a flaw in this strategy since it cannot guarantee collision resistance. For traditional systems, different processing and machine learning modules are used in the physiological data processing cloud [23].The machine learning model [22 -23] based processing is best for only particular model and achieves best security in that model alone. Tian Wang et al. [18] have presented a trajectory privacy preservation method that uses Dummy Rotation (DR) algorithm to provide location-based services. By using this approach, privacy preservation is achieved, but it doesn't focus the integrity. Zhi Li et al. presented a novel Hyper-graph-based Key Management (HKM) scheme that focused on confidentiality and integrity [19]. It has a key generation center for generating secret keys, fog server for processing the data, cloud for data storage and users. The scheme secures the storage data in both forward and backward directions. Bashar Alohali et al. [20]have presented the key management scheme in the Smart Grid (KM-CL-SG) communication layer. Since the security and privacy issues threaten modern technology, various researches focus on achieving high security.

3 Implementation of the Proposed System

The major problems presented in the cloud-based system are data overloading and latency that lead to user data hacking. This can be overcome by fog-based organizations that play a key role in the construction of smart cities and smart transportation. The system model of the proposed fog-based system is shown in Figure 1. The application layer, network layer, and perception layer are the three

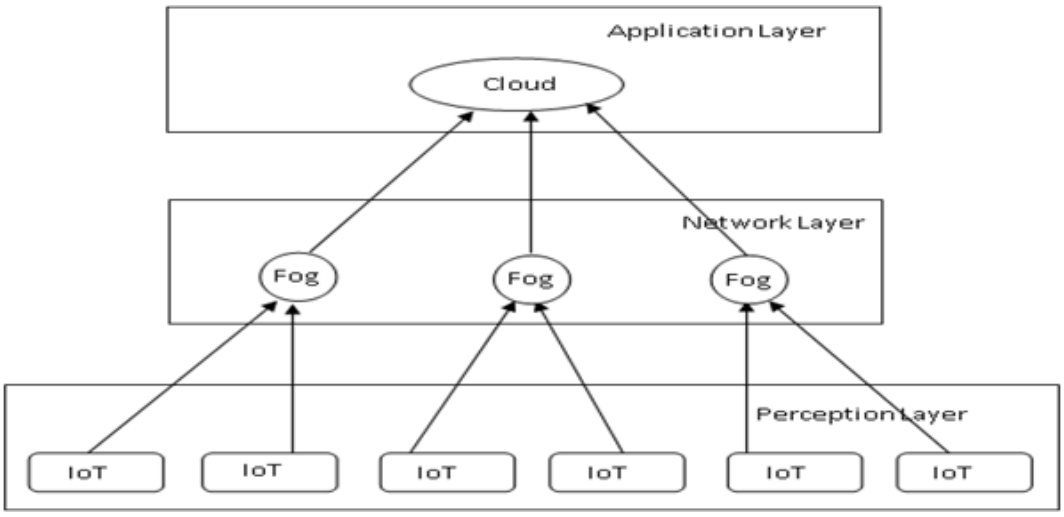


Figure 1: The system model of Fog based System

levels that make up FOG system. The perception layer at the bottom of the design is where the IoT

devices are positioned. Because every IoT node senses and collects the users' information for further processing, it's also known as an end-user layer. The network layer, which sits in the middle of the architecture, serves as a link between the perception and application levels. For processing and sending data to the upper layer, it incorporates fog nodes and network components such as routers, gateways, switches, and so on. The data are saved in the cloud at the top layer, which is an application layer.

3.1 Proposed Fog based System

Due to the growth in population and technology, the Fog-based system is necessary to communicate between the cloud server and customers. The block diagram of the proposed fog-based system is shown in Figure 2.

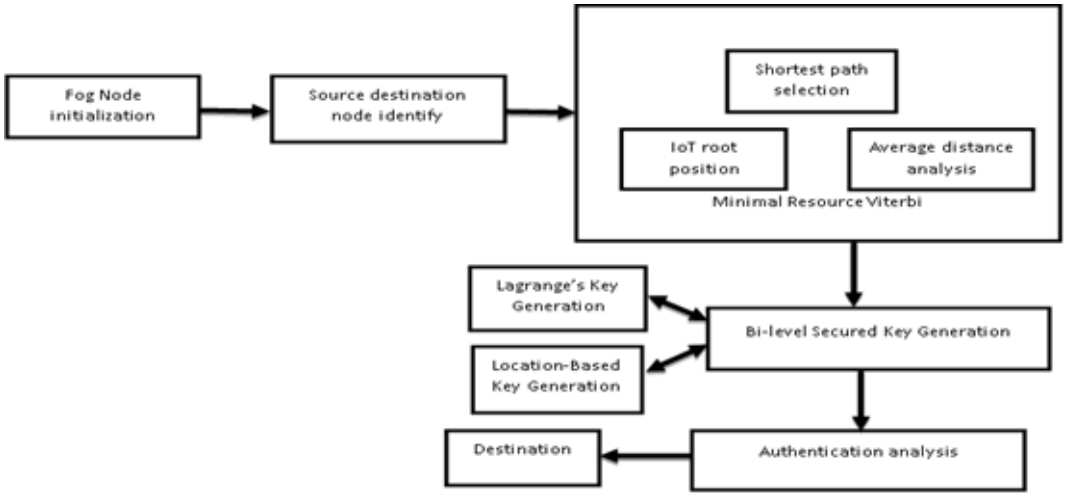


Figure 2: Proposed System Diagram

While Fog Node offers services used in different locations, cloud computing tipping offers its own cache and subsequent requests locally. Act as the central controller of global service delivery and distributed fog nodes. In addition, the cloud image receives the necessary information from the fog population sensor on the end user device, which can now communicate with the IoT sensors central information database, and then use the fog terminal to communicate. It not only provides information about the devices, but it also provides the user's private information. So there is a possibility for hacking or spoofing the user information. The proposed hybrid Bi-level can mitigate its secured key generation scheme, which combines Lagrange's Key Generation (LKG) and Location-Based Key (LBK) generation.

The encryption procedure for safeguarding information about and from users is conducted out during data transfer from end-users to fog nodes using Lagrange's key generation technique. The fog node stores the encrypted data created. In order to offer two-level security, LBK is created in every fog node and combined with the encrypted data. Using MRV cloud nodes and fog nodes, reduce short path secretion between users. The data is decrypted again on the cloud server using the encryption logger key, and the data is eventually saved in the cloud, as shown in Figure 3.

Algorithm Step 1: Create n number of nodes $n_1, n_2, n_3, ...n_n$
Step 2: Assign the position of nodes and set the distance between nodes
for (i=0; i<n ;i++) (tmp =distance between node i and i+1..... (1))
Step 3: Selection of source node (S_i) and destination node (D_i)
Step 4: Data transmission from Si to fog node (f_i)
Step 5: Attacker determination by sending hello message to neighbor nodes
Step 6: Computation of shortest path using MRV by ignoring the attacker nodes
Step 7: BSKG key encryption LKG & LBK, LKG can be generated using equation 5, and LBK can be generated based on the location of fog nodes
Step 8: Data transmission from f_n to D_n

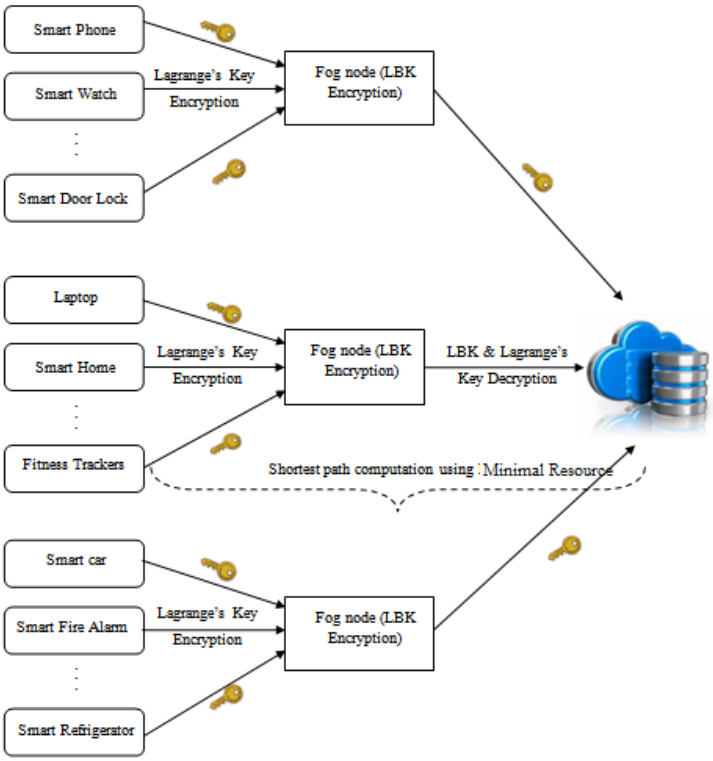


Figure 3: Architecture Diagram of Data transmission with security

Step 9: BSKG key decryption LBK & LKG
Step 10: Detection of the mobile station for specific users
Step 11: Data reception in the D_n or cloud

3.2 Bi-level Secured Key Generation (BSKG)

The major concern in most modern applications is high-level security. By focusing on this, BSKG is introduced, which is a combination of LKG and LBK key generation methods. It can generate keys in terms of alphanumeric, which is a combination of alphabets and numbers. This effective key generation method is applied when transmitted from the source to the fog node.

3.2.1 Lagrange's Key Generation (LKG))

The data transmission from source to fog node generates a secret key based on Lagrange's equation to secure the customer data. If the systemyis represented as a function of x and it is defined in terms of the parameter α, then

$$y = x + \alpha\psi + (y) \tag{1}$$

Where α denotes Lagrange's parameter, and $\psi + (y)$ denotes the holomorphic function defined as a complex differentiable function.
The following Lagrange's expansion can compute the Lagrange's key of the system y
Lagrange's key generation approach uses the interpolation methods for performing both encryption and decryption processes.Itapplies the interpolation to generate the polynomial for the data sensed from the smart devices. The polynomial functions are generated between the smart devices and fog nodes, and the data are represented as (x0, y0), (x1, y1),. . . . . (xn,yn). It resulted in the nth degree polynomial by utilizing n+1 data. The following equation can represent Lagrange's polynomial with the interpolation method.

$$f(y) = f(x) + \alpha/1!\,\psi(x)f`(x) + \alpha^2/2!\,\partial/\partial x[\psi(x)]^2 f`(x) + - - - - - - + \alpha^{n+1}[\psi(x)]^{n+1} f`(x) \tag{2}$$

Algorithm

Step 1: Create n number of nodes

Step 2: Assign the position of nodes and set the distance between nodes

$for\ (i = 0;\ i < n;\ i++)$

{

$tmp\ =\ distance\ between\ node\ i\ and\ i + 1$

}

Step 3: Selection of source node (S_i) and destination node (D_i)

Step 4: Data transmission from S_i to fog node (f_i)

Step 5: Attacker determination by sending hello message to neighbor nodes

Step 6: Computation of shortest path using MRV by ignoring the attacker nodes

Step 7: BSKG key encryption {LKG & LBK}, LKG can be generated using equation 5, and LBK can be generated based on the location of fog nodes

Step 8: Data transmission from f_n to D_n

Step 9: BSKG key decryption {LBK & LKG}

Step 10: Detection of the mobile station for specific users

Step 11: Data reception in the D_n or cloud

Where n denotes the degree of polynomial and can be represented as follows

$$p_n(x) = \sum_{j=0}^{n} L_j(x) f(x_j) \tag{3}$$

The simplified form of (5) can be expressed as follows.

$$L_j(x) = x - x_0/x_j - x_0.x - x_1/x_j - x_1.....x - x_{j-1}/x_j - x_{j-1}.....x - x_n/x_j - x_n \tag{4}$$

If the value of the x is known, then only the data is hacked. Still, it is difficult to predict the value because it was chosen randomly ensures the security and confidentiality of the customer data.

3.2.2 Location-based Key Generation (LBK)

To attain secure and safe communication in fog computing, it should be ensured that secured data is shared between fog nodes and the cloud. LBK key generation is applied in every fog node after performing the encryption using Lagrange's expansion. This can provide bi-level security for the customer data protection. The key generated from LBK is an alphanumeric code that differs in every fog node to achieve high-level security.It uses a novel key updating process depending on the grid's location information to avoid data corruption and hacking.

$$L_j(x) = \prod_{i=0}^{n}, J = 0, 1.....n : i \not\equiv j \tag{5}$$

The working principle of the LBK key generation method is shown in Figure 4. This figure shows securing of data against the attackers while the adversary tries to hack the data. It provides high-level security by generating the key based on the location. It differs from the cryptographic key by its alphanumeric key generation. In cryptography keys, the keys are generated as 32-bit binary keys. In contrast, in LBK, the key is a combination of alphabets and numerals, which leads to high security over other key management techniques.It is termed geo encryption because it is location-dependent,

and it enables the routes for transmission from the source node to the destination node. If any attacker is found in any of the nodes, the data is transferred through some other nodes. Since the data are location authenticated, it can be transferred with high security.
To calculate each neighbor node location authenticated based average distance analysis

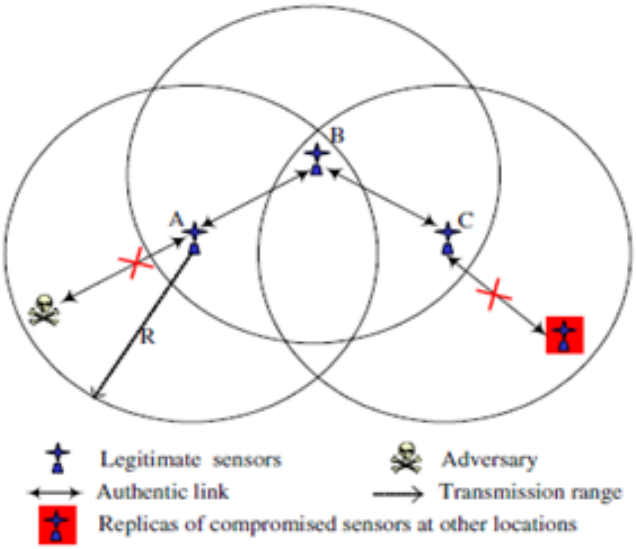


Figure 4: Location-Based Key Generation

Every fog node in the network generates a distinct key, and it is in the form of alphabets. After performing LBK, the resultant key is alphanumeric. The key obtained from the LKG approach is added in every fog node, increasing the security of the data transmission. The LPK system attempts to locate the source / target by directly measuring the radio signal traveling between the transmitter and the receiver. The relationship between the limit difference between the recipients and the LKG is provided

$$L_j = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \tag{6}$$

$$R_{m,n} = s * d_{m,n} = R_m - R_n \tag{7}$$

Where
s- Signal propagation speed
m,n – between neighbor node
R- Allocation of signal
These LBK, LKG systems use time, phase, or frequency measurement values to estimate the direction or range of the first signal propagation path, and then use solutions that provide calculations based on the distance of the data node measured by the generated key.

3.3 Minimal Resource Viterbi

In the proposed Fog-based Smart Grid system, information exchange with high speed is desirable. This can be realized by finding the short path fog tip and fog tip cloud computing among users.MRV is used to compute the shortest path effectively by exploiting dynamic programming approaches [21]. Instead of differential equations, minimizers are used in every neuron of this network. It uses adders and minimizers for shortest path computation leading to low computational complexity. This reduces the number of computations in each neuron and reduces the number of repetitions.This network initiates the operation by activating the source neuron,which results in an auto wave, and then it travels through all nodes of the network; finally, the best path is stored in the output.
Algorithm Steps Consider a graph G(N, V) with N nodes and V edges. Each node is assigned a time window W_T $[l_i, u_i]$ with upper(ui) and lower (l_i) threshold values. SPi is the shortest path from

s to i, and TT_i is the traversal time of the path to reach node i.
Step 1: Initialize the network, set the upper threshold and lower threshold in the threshold window

$$T_S^L = 0 : T_U^S = \varepsilon : T_i^L = l_i; Ti^U = u_i + \varepsilon \tag{8}$$

Step 2: Source neuron is activated by setting the input of the neuron within the threshold so that the auto wave is generated and propagates to neighborhood neurons
Step3: Communication Range: To use the communication range of the behind the formula:

$$E = (u, v)\epsilon V^2 | u \neq v \tag{9}$$

Step4: Since the length of the shortest path from node n_i
Step5: An available distance of node n_i and required the minimum distance of node m_i
Step6: Critical sensing point of the n_i . If source node denote as and the nearest neighbor node denote $n_n n_i < m_i$
Step 7: Competition of all minimum distance paths to the node happens, and this takes place simultaneously in all neurons

$$C_i(t) = j, j\epsilon BS(i) and TT_j(t) + d_{ij}[TT_j(t)]\epsilon[Ti^L + TiU] \tag{10}$$

Step 8: Compute traversal time at the output of the neuron,

$$TTi^U(t+1) = minTT_i(t+1), TTi^U(t) \tag{11}$$

Compute the shortest path from $N_s$to N_i Where l = winning node
Step 9: Update the upper threshold of the node
Step 10: Repeat the autosave travel and competition (step3 to step6) until the network converges.

When the MRV is used for the first time, the node will be removed, but the retained path information will pass through the node just like all the previously mentioned paths; Therefore, when the next search is made to proceed to this node, the stored path information will be used, and the map can be easily used to find the shortest path at the fastest time to avoid recounting.

4 Results and Discussions

This chapter discusses the comparison of Minimal Resource Viterbi based Bi-level Secured Key Generation (MRV-BSKG) and previous security;Bi-level Secured Key Generation provides authenticate for the data when source node send the data and it is transmitted through the neighbouring node in communication. The Minimal Resource Viterbichooses a different path if the neighbouring terminal changes its position. So these two proposed methods are compared in this section.The previous methods Attribute-Based Encryption (ABE), Ciphertext Policy-ABE (CP-ABE), Lightweight privacy data Preserving Aggregation (LDPA), Hyper-graph based Key Management (HKM) and Key Management Scheme for Communication Layer (KMS-CL). The proposed Fog-based system's performances are analyzed in terms of packet drop, packet delivery ratio, throughput, and security.The parameters used for simulation are tabulated in Table 1.

4.1 Packet Delivery Ratio (PDR)

It is defined as the ratio of the total number of packets received by the receiver atthe destination to the total number of packets sent by the sender from the source.

$$PDR = P_D/P_s \tag{12}$$

Using the above equation 11, the PDR for the proposed scheme is compared with the existing approaches. Due to the highly secure key management mechanism and MRV approach, the proposed fog-based system achieves a high PDR. Every path's journey is saved in the hidden layers of MRV,

Table 1: Simulation Parameters

Simulation Parameters	Value
Number of nodes	50
Routing Protocol	Dynamic Source Routing (DSR)
Queue type	Priority Queue
Packet size	300 bytes
MAC type	802.11
Antenna	Omni-directional antenna
Initial energy	100J
Idle node energy	0.001J/s
Power required for transmission	1.35J
Power required for reception	1.7J
Power consumed by sleep nodes	0.001J
Distance between Source and Destination	669.9Km
Energy consumed by the highest antenna	1.5 J/s
Propagation model	Two-way ground

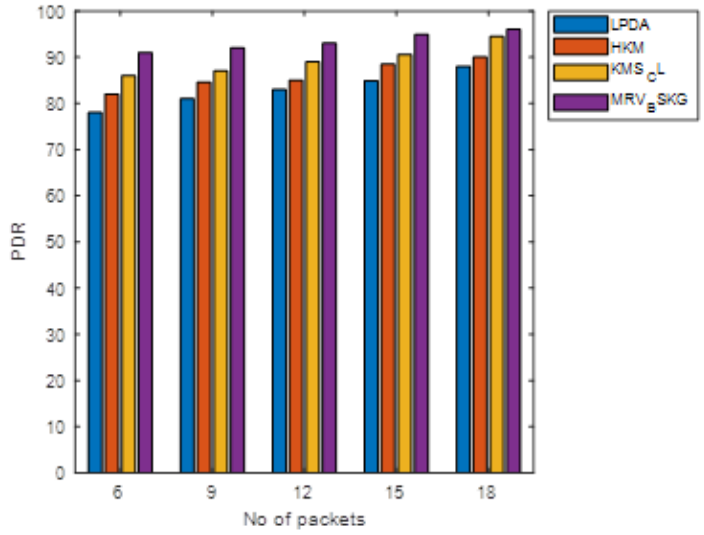


Figure 5: PDR comparison of the proposed system with existing techniques

and the attackers between the source and destination are discovered. To avoid packet loss, it stores the attacker's location in memory after it has been discovered.

The proposed fog-based method produces improved PDR outcomes in the vast majority of instances. However, if an attacker is present, the packet delivery ratio is lowered. However, it outperforms other key management systems currently in use. Figure 5 shows the PDR of the proposed fog-based system in comparison to existing approaches. The suggested MRV-BSKG has a packet delivery ratio of 96 percent when compared to other current approaches such as LDPA (88 percent), HKM (90 percent), and KMS-CL (94.45 percent).

4.2 Packet Drop

Packet drop mainly occurs in the wireless network during data transmission and network congestion. It exhibits the reliability of the communication process in wireless networks. It is defined as the number of packets sent from the source PS to the number of packets dropped (PND) during transmission.

$$PDD = \frac{P_{ND}}{P_S} \qquad (12)$$

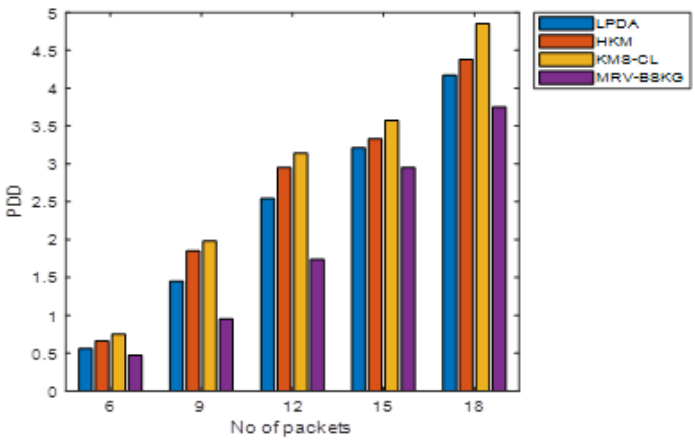


Figure 6: Comparison of packet loss

The proposed MRV method's packet loss is compared to current approaches. The findings are shown in Figure 6 above. The efficiency of the proposed MRV-BSKG approach is determined by altering the number of nodes and assessing the time associated with packet loss. The findings reveal that the proposed MRV-BSKG approach detects packet drops in 3.75 seconds owing to attackers and mobile stations, which is better than other methods currently in use. KMS-CL is 4.85 with ms, LPDA is 4.17 with sec, HKM is 4.38 with sec, and LPDA is 4.17 with sec.

4.3 Throughput

It is defined as the amount of information sent from source to destination within a specific amount of time. The following equation can compute the throughput of the wireless network. PR indicates the packet received and PSindicate the packet size received in a time (T) sec.

$$Throughput(bps) = P_R * PS/T \qquad (13)$$

The comparison graph demonstrates that the suggested method outperforms other current strategies in terms of throughput. At 20ms, the suggested Fog-based system enhances the throughput comparison given in figure 7; this demonstrates that the proposed technique has a higher throughput ratio than previous approaches.

$$TT_j(t+1) = TT_j(t) = TT_j$$
$$SP_i(t+1) = SP_i(t) = SP_i$$

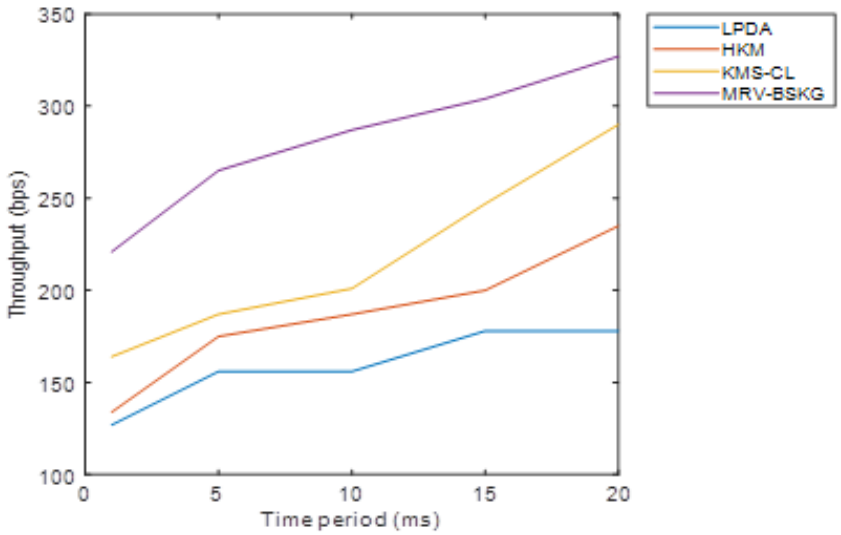


Figure 7: Throughput comparison of proposed Fog based system with other existing techniques

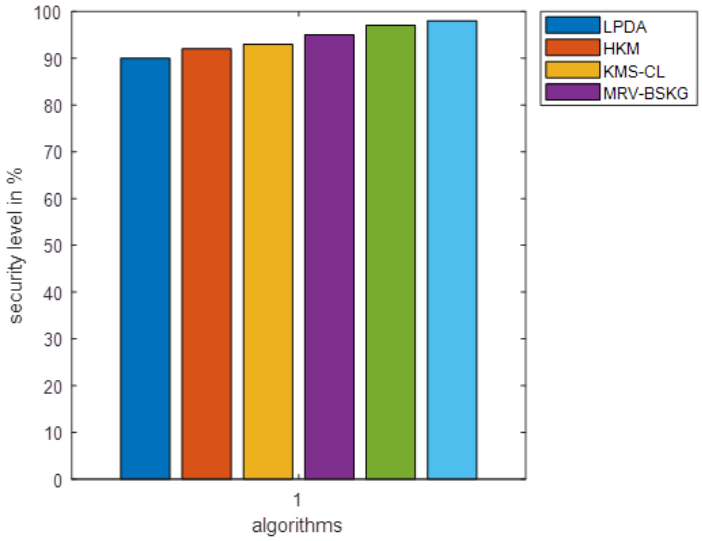


Figure 8: Security Level Analysis

Figure 7 depicts the throughput curve of the proposed Fog-based system using the MRV-BSKG key management approach. This graph indicates that as time passes, the system's throughput grows. The suggested Fog-based system's throughput is compared to existing key management systems.

4.4 Computation Time

The time required for computing the shortest path between the source and destination in the proposed Fog based system is shown in Figure 8.

Figure 8shows that the MRV reduces the latency by 23.14%, 48.82% and 43.79% compared with conventional shortest path computation algorithms such as LPDA, HKM.

4.5 Security Analysis

Fog-based system's major concern is network security because there are some adversaries to hack the data during data transmission from source to destination. To mitigate these security and privacy issues highly secured BSKG key generation-based fog system is designed that can provide 98% secured

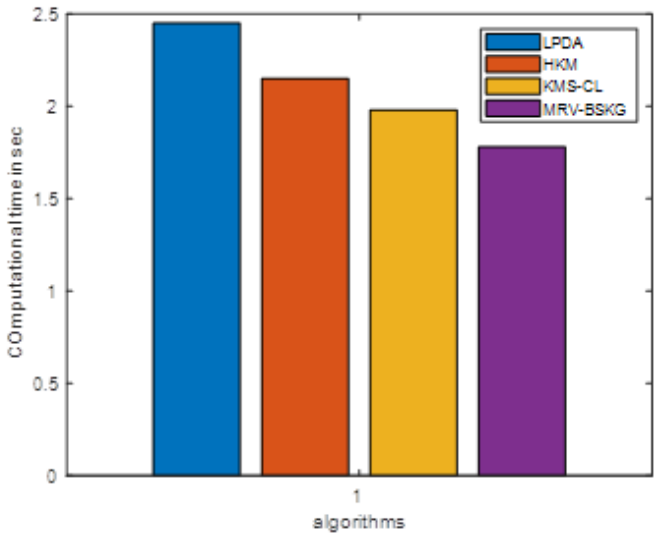


Figure 9: The computation time of shortest path algorithms

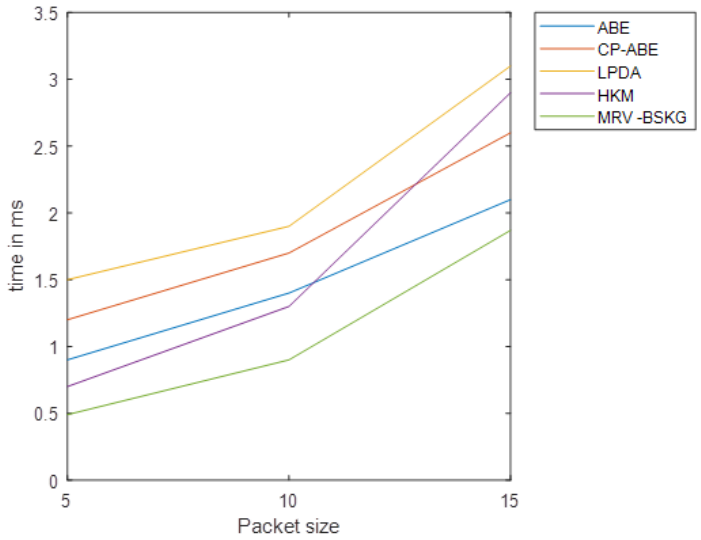


Figure 10: Data Decryption Time

data. Figure9 shows the results; it is observed that the proposed BSKG based security level is 98% increases the security by when compared with the existing key management techniques such as ABE is 90%, CP-ABE is 92%, and LDPA is 93

4.6 Analysis of Error Rate

It can be seen that the Key Bit Error Rate increases as the data size increases due to the decreased subspace distance between potential precedes. The above figure 10 shows that the analysis of error rate compared with proposed MRV-BSKG is 36% and the previous ABE is 67%, CP-ABE is 63%, LDPA is 55%, HKM is 49%, KMS-CL is 41%.

4.7 Analysis of Encryption Time

Analysis of encryption time that indicates the speed of encryption. The experiments for comparing the performance of the different previous security algorithm and proposed algorithm.

Figure 11 shows that encryption time for uploading the data and then it indicates how long it took to convert the original data. The proposed MRV-BSKG is 1.87 with ms and the existing methods

ABE with 2.9 ms, CP-ABE with 3.1 ms, LDPA with 2.6 ms, and HKM with 2.4 ms.

4.8 Decryption Time

The proposed MRV-BSKG algorithm providing a separate key to each user requesting the authentication of necessary data posted by the data owner.

Indicates how long it took to convert the encrypted data and retrieve the original data. The proposed MRV-BSKG algorithm it should be used once to decrypt the required information. The above figure 12 shows the comparison of the proposed and previous methods. Hence the proposed MRV-BSKG to give better decryption time

5 Conclusion

Fog- Cloud Computing is considered a good partner; it is an extended cloud service by end users .The fundamental here is to interface and change the safety efforts and apply them as per the necessities of the Fog platform. The secured key management efforts have gone through testing, and utilizing them can guarantee that any Fog computing fulfills vital mechanical security norms. Various security issues may arise in the design and implementation of the technology. In this paper, the Fog-based system is proposed with a hybrid BSKG method formed by combining two key generation approaches, LKG and LBK. This method achieved high-level security against node capture attacks. The LKG method is used for both encryption and decryption, and LBK is used to generate key in fog nodes. The generated key is difficult to express because of its high dispersion nature. Analysis shows that the proposed method achieves all security requirements like location privacy,anonymity,data integrity. Future work may lead to the development of knowledge-based supplementary and aided systems, which can provide decision support services to developers in designing a safe and efficient fog infrastructure.

Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Conflict of interest

The authors declare no conflict of interest.

Ethics Approval and Consent to Participate

No participation of humans takes place in this implementation process

Human and Animal Rights

No violation of Human and Animal Rights is involved.

Funding

No funding is involved in this work.

Authorship contributions

There is no authorship contribution.

Acknowledgement

There is no acknowledgement involved in this work

References

[1] Haina Zheng, KeXiong, Pingyi Fan, ZhangduiZhong and Khaled Ben Letaief, 2019.“Fog-Assisted Multi-User SWIPT Networks: Local Computing or Offloading”, IEEE Internet of Things Journal, pp. 5246-5264.

[2] Andrea Tassi, IoannisMavromatis, Robert Piechockiy and Andrew Nix, 2019.“Agile Data Offloading over Novel Fog Computing Infrastructure for CAVs”, Networking and Internet Architecture.

[3] Mahesh U. Shankarwar and Ambika V. Pawar, 2016.“Security and Privacy in Cloud Computing: A Survey”, Springer.

[4] MadjidMerabti, Bashar Alohali and KashifKifayat,2015. “A New Key Management Scheme Based on Smart Grid Requirements”, Advances in Information Science and Computer Engineering, pp. 436-444.

[5] W. Wang and Z. Lu, 2013 “Cyber security in the smart grid: Survey and challenges,” Computer Networks, vol. 57, no. 5, pp. 1344–1371.

[6] M. Benmalek and Y. Challal, 2016 “MK-AMI: Efficient multi-group key management scheme for secure communications in AMI systems,” in Proc. of IEEE Wireless Communications and Networking Conference (IEEE WCNC), pp. 1–6.

[7] K. K. R. Choo, O. F. Rana, and M. Rajarajan. 2017“Cloud Security Engineering:Theory, Practice and Future Research.” IEEE Transactions on CloudComputing, 5(3):372–374.

[8] .O. A. Osanaiye, S. Chen, Z. Yan, R. Lu, K. K. R. Choo, and M. E.Dlodlo. 2017 From “Cloud to Fog Computing: A Review and a ConceptualLive VM Migration Framework”. IEEE Access, 5(1):8284–8300.

[9] AshkanYousefpour et al, 2017 “All one needs to know about fog computing and related edge computing paradigms: A complete survey”, Elsevier, Journal of Systems Architecture, Vol. 89, pp. 289-330.

[10] Shanhe Yi, Zhengrui Qin, and Qun Li, 2015 “Security and Privacy Issues of Fog Computing: A Survey”, Conference on wireless algorithms, systems, Springer.

[11] P. Zhang, T. Zhuo, W. Huang, K. Chen, M. Kankanhalli, Online object tracking based on CNN with spatial-temporal saliency guided sampling, Neurocomputing 257 (2017) 115–127.

[12] J. Zhang, K.A. Ehinger, H. Wei, K. Zhang, J. Yang, A novel graph-based optimization framework for salient object detection, PatternRecognit. 64 (1) (2017) 39–50.

[13] H. Chen, Y. Li, D. Su, Multi-modal fusion network with multi-scale multi– path and cross-modal interactions for RGB-D salient object detection, Pattern Recognit. 1 (1) (2018).1–1.

[14] E. Macaluso, C.D. Frith, J. Driver, Directing attention to locations and to sensory modalities: multiple levels of selective processing revealed with PET, Cerebral Cortex 12 (4) (2002) 357–368.

[15] T.S. Lee, D. Mumford, Hierarchical bayesian inference in the visual cortex, JOSAA 20 (7) (2003) 1434–1448.

[16] Q. Yan, L. Xu, J. Shi, J. Jia, Hierarchical saliency detection, in: IEEE Conference on Computer Vision and Pattern Recognition, 2013, pp. 1155–1162.

[17] . Achanta, R., Hemami, S., Estrada, F., Susstrunk, S.: Frequency-tuned salient region detection. In: IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2009, pp. 1597–1604. IEEE (2009)

[18] Cheng, M.M., Zhang, G.X., Mitra, N.J., Huang, X., Hu, S.M.: Global contrast based salient region detection. In: 2011 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 409–416. IEEE (2011)

[19] Cui, X., Liu, Q., Metaxas, D.: Temporal spectral residual: fast motion saliency detection. In: Proceedings of the ACM International Conference on Multimedia (2009).

[20] B. X. Nie, P. Wei, and S.-C. Zhu, "Monocular 3D human pose estimation by predicting depth on joints." in IEEE International Conference on Computer Vision, 2017

[21] D. Zhang, J. Han, C. Li, J. Wang, and X. Li, "Detection of co-salient objects by looking deep and wide", International Journal of Computer Vision, vol. 120, no. 2, pp. 215–232, 2016.

[22] X. Dong et al., "Occlusion-aware real-time object tracking," IEEE Trans. Multimedia, vol. 19, no. 4, pp. 763–771, Apr. 2017.

[23] X. Dong, J. Shen, L. Shao, and L. Van Gool, "Sub-Markov random walk for image segmentation," IEEE Trans. Image Process., vol. 25, no. 2, pp. 516–527, Feb. 2016.

[24] J. Shen et al., "Real-time superpixel segmentation by DBSCAN clustering algorithm", IEEE Trans. Image Process., vol. 25, no. 12, pp. 5933–5942, Dec. 2016.

[25] Y. Yuan, C. Li, J. Kim, W. Cai, D.D. Feng, Dense and sparse labeling with multidimensional features for saliency detection, IEEE Trans. Circuits Syst. Video Technol. 28 (5) (2018) 1130–1143.

[26] W. Wang, J. Shen, F. Guo, M.-M. Cheng, A. Borji, Revisiting video saliency: a large-scale benchmark and a new model, in: IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 4894–4903.

[27] Li Q., Chen S., Zhang B. (2012) Predictive Video Saliency Detection. In: Liu CL., Zhang C., Wang L. (eds) Pattern Recognition. CCPR 2012. Communications in Computer and Information Science, vol 321. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33506-8_23.

[28] Wang, Wenguan et al. "Deep Learning For Video Saliency Detection." ArXiv abs/1702. 00871 (2017): n. pag.

[29] F. Guo et al., "Video Saliency Detection Using Object Proposals," in IEEE Transactions on Cybernetics, vol. 48, no. 11, pp. 3159-3170, Nov. 2018, doi: 10.1109/TCYB.2017.2761361.

[30] Karthik, A., MazherIqbal, J.L. Efficient Speech Enhancement Using Recurrent Convolution Encoder and Decoder. Wireless Pers Commun 119, 1959–1973 (2021).

[31] Yuming Fang, Xiaoqiang Zhang, Feiniu Yuan, NevrezImamoglu, Haiwen Liu, Video saliency detection by gestalt theory, Pattern Recognition, Volume 96,2019,106987, ISSN 0031-3203.

[32] https://docs.microsoft.com/en-us/cpp/build/reference/clr common language runtime compilation? View = msvc-160

[33] https://docs.microsoft.com/en-us/cpp/dotnet/walkthrough-compiling-a-cpp-program-that-targets-the-clr-in-visual-studio?view=msvc-160

[34] https://en.wikipedia.org/wiki/Common_Language_Runtime

[35] https://www.red-gate.com/simple-talk/dotnet/net-development/creating-ccli-wrapper/

[36] Wang, Bofei et al. "Object-based Spatial Similarity for Semi-supervised Video Object Segmentation." (2019).

[37] Li F., Kim T., Humayun A., Tsai D., Rehg J. M.,"Video Segmentation byTracking Many Figure-Ground Segments" In:IEEE International Conference onComputer Vision (ICCV), 2013.

Journal's webpage: http://univagora.ro/jour/index.php/ijccc/

This journal is a member of, and subscribes to the principles of,
the Committee on Publication Ethics (COPE).
https://publicationethics.org/members/international-journal-computers-communications-and-control

Cite this paper as:
Arul Sindhia.P; Bharathi.R; (2022). Bi-Level Minimal Resource Protected Key Generation Framework For Fog Computing Applications, *International Journal of Computers Communications & Control*, 17(6), 4363, 2022.
https://doi.org/10.15837/ijccc.2022.6.4363