Received: August 12, 2021. Revised: September 15, 2021

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Fog Computing with IoT Device's Data Security Management Using Density Control Weighted Election and Extensible Authentication Protocol

Jalasri Mahendran[1]* **Lakshmanan Lakshmanan**[1]

[1]*Department of CSE, Sathyabama Institute of Science and Technology, India*
* Corresponding author's Email: jalasrimani@gmail.com

Abstract: Nowadays, most people utilize the Internet of Things (IoT) to gather private information and the gathered details are saved in a third-parties database. During this process, fog computing is worked with IoT devices because it collects a large volume of data and is computationally intensive. Although these techniques provide valuable services, data security, privacy, edge node latency, and energy consumption are still significant problems. Therefore in this paper, the Data Security Management model (DSMM) has been proposed to overcome all the security and privacy issues during the data transmission among IoT devices. DSMM involves the density control weighted election that uses the effective clustering method to group the data into clusters to overcome these security issues. Authentication protocol technique is applied to manage the data security, privacy and eliminate intermediate attacks. The Density Control Weighted (DCW) election protocol is applied to select the cluster head and respective members for the clustering process. From the chosen routing process, the data has been transmitted by applying the extensible authentication protocol. DSMM ensures data security and reduces intermediate attacks successfully. Then the efficiency of the system is evaluated using the experimental results and compared with existing protocols. The experimental results of DSMM achieve data processing time ratio of 86.3%, data security 98.09%, precision 97.23%, performance 92.21%, effective data authentication ratio 94.91%, recall 97.25%, response time 96.18%, when compared to other methods.

Keywords: Internet of things (IoT), Fog computing, Energy consumption, Latency, Density control weighted election protocol, Extensible authentication protocol.

1. Introduction

Private data information is about an individual that can fairly be assumed and be guarded by public manner [1]. A single corporation can have millions of users' records, and it maintains a private identity that must be as secured and protected as possible [2]. Data collection aims to ensure quality by maintaining the data in statistical analysis and making scientific choices based on the gathered data [3]. An agency gathers data from third parties with no clear link with the person on whom the data are collected [4]. Data are created by third parties on numerous websites and forums and gathered by third parties such as a data management platform (DMP) [5]. Data security is a process of protection of network files, databases. It accounts for implementing a collection of controls, applications, and techniques defining various dataset's relative significance, sensitivity, and regulative compliance requirements and applying appropriate safeguards [6, 7]. Data security relates to procedures of data protection against undesirable access and data degradation [8]. Data security encryption, hash, tokenization, and key management activities across systems and networks are included [9].

Data management is a safe, reliable, and cost-effective practice for third-party data collection, maintenance [10]. A reliable data collection approach is becoming more important as organizations depend on intangible assets to produce value [11]. A company uses a private data network to send and receive essential data for everyday operations [12]. Data collected must be safe, stable, high-speed, and trustworthy without public wireless carriers [13]. Private data transmission may be implemented either as private lines secured from common companies and architected completely by the network as a virtual private network (VPN) infrastructure provided either over the internet within the network of a carrier [14, 15]. However, IoT-based sensors and tools face various protection, privacy challenges. These devices are primarily employed to collect information on consumers' vital signs in the surrounding atmosphere [16, 17]. Traditional protection and privacy protocols for IoT devices have not been well optimized due to their restricted energy, storage capacity, communications, and computational capacity, influencing researchers to provide these restrictions in new solutions and algorithms [18]. Safe data aggregation protocols drive effective and private data collection to store in the database. [19] Due to many connected computers, a centralized database could not connect the processing and storage requirements of the data gathered [20].

An authentication protocol is a communication or encryption protocol designed to transmit authentication data among two organizations [21]. It allows the beneficiary to identify the connected entity by specifying the syntax of the needed information [22]. For safe communication within computer networks, the authentication protocol is the most critical security layer required. Authentication protocols are among the most offered data privacy and ensure that a person, program, or organization seeking access to information is one of the intended recipients [23]. The method suggested in this paper considers a mode in which the message is sent directly from cluster members to the cluster head [24]. The Cluster Head choice is dependent on the energy requirements and density-weighted cluster election protocol of the cluster nodes. The DCW concept decreases the distance between nodes dramatically. As a result, the conservation of resources is improved, and the DCW algorithm selects the next point for all nodes in the cluster when choosing Cluster Head. This transmission mode prevents losses from the transmissions of long nodes and decreases the number of routes and power usage in the WSN.

This article discusses the effective fog authentication protocol. Hence in this paper, DSMM has been proposed to improve data security and privacy in data transmission. The density control weighted (DCW) election protocols suggested providing a faster response time and fewer numerical overheads using the distributed design with other enhanced functionality of fog computing. Furthermore, structure DSMM utilizes fine-grained energy usage and data confidentiality with data protection processes in fog computing. The extensive performance assessment findings show that the proposed protocols are superior to cloud-assisted schemes without data aggregation in data transference and capacity availability. The main contribution of DSMM is described below:

- DSMM consists of weighted choices for density control grouped into clusters using the efficient clustering method to solve these security problems.
- Authentication is used for data protection, privacy management, and the removal of intermediate attacks. To pick the cluster head and the individual members in the clustering process, the Density Control Weighted (DCW) election protocol is applied.
- The highest efficiency is achieved when compared with the existing methods.

The rest of the paper is organized as follows as Section 2 encompasses various background studies regarding data security and protection. Section 3 explores the proposed DSMM for enhancing the security level in the data transfer level among IoT devices. The findings that demonstrate the performances with the relevant specifications are presented in Section 4. Finally, Section 5 summarizes and concludes with prospects.

2. Background study on data management and security maintenance

This section highlights several works carried out by different researchers. In [25] deliberated the secure authentication protocol for user addition in distributed IoT. Rapid growth in smart device adoption in the IoT spread has resulted in increased data. Data security has become a prominent driver to boost the IoT ecosystem with resource-constrained sensor nodes and insecure communication networks.

In [26], suggested the foundation for privacy preservation for trustworthy context-aware computing. Systems for Location-based (LBS) services evolve exponentially with a radio communication service positioning feature. LBS faces various problems relating to privacy in three distinct formats to include points of interest (POI), such as Trusted Third Party (TTP), Non - trusted Third Party (NTTP) and mobile peer-to-peer (P2P). Simulation results suggest that LBS may be regarded as a promising model to secure user characteristics in an LBS-based TTP system because of increased privacy and performance.

In [27] discussed the Compressed and Private Data Sharing framework (Cpds) to permit confidential and compressed data exchange. The Internet of Things (IoT) is a high-profile technology that offers industrial systems product traceability. With IoT-enabled industrial systems, sensing and networking techniques allow participants to monitor the goods effectively and register their status during manufacturing processes. $Cpds$ is creating two new frameworks for stored commodity data on the blockchain compressed and implemented policy.

Privacy-preserved data-sharing framework (PPDSF) for multiple parties in industrial IoT is described in [28]. The physical data can create serious data protection problems for both employees and suppliers, essential for a device's aspects. The platform enables data contributors to communicate their contents on request. To maintain the delicate condition of contributors, the material submitted is disrupted.

Ant Colony optimization with Multi Kernel Support Vector Machine Model (ACOMKSVM) for secure and reliable IoT data sharing is explored in [29]. Elliptical Curve cryptosystem (ECC) is used to establish efficient and precise privacy that safeguards protected ACOMKSVM learning. The protection review shows that the particular data guarantees each data supplier's sensitive and confidential system and preserves data criteria in an ACOMKSVM model.

Blockchain technology with Wireless Body Area Networks (BC-WBANM) Model for secure data sharing is developed in [30]. To address the security problem, BC-WBANM proposes a model in the architecture of WBANs to ensure security in the blockchain data transmission mechanism in the wireless network context, built as an Authentication and blind signature protocol between nodes. Experimental findings indicate that the approach suggested is promising and exhibits greater protection and stability than other approaches.

This document's main purpose and contribution are to reduce resource constraints and impediments in developing an effective security protocol for efficient scaling in distributed IoT.

Data security efficiency and stability increased positive and negative time-and-space approaches like encryption and decryption. LBS system band increases the user-location server (LS) privacy concerns. Lightweight blockchain system adapted to industrial IoT situations with restricted resources. To maximize the advantage of limited resources to maintain the usefulness of the results obtained.

Based on these analyses, some issues in the existing methods CPDS, PPDSF, ACOMKSVMM, BC-WBANM. Therefore, DSMM has been proposed to reduce data security risk factors and improve data transmission performance.

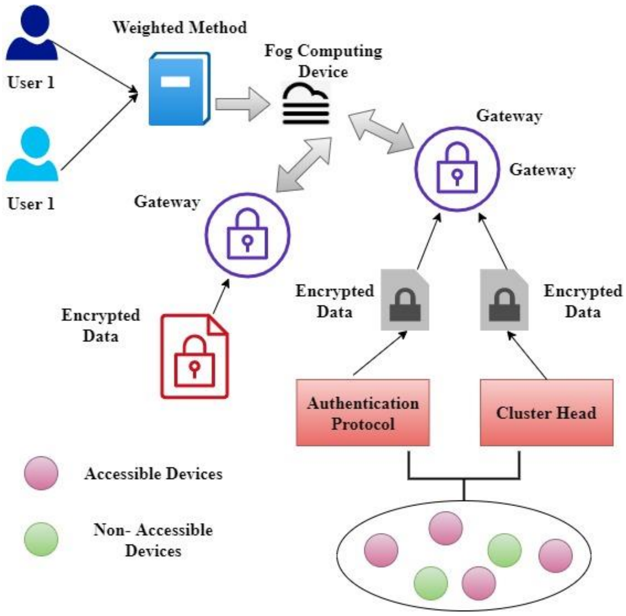


Figure. 1 The architecture of DSM

3. Data security management model

DSM is implemented to settle all security and privacy problems during IoT system data transmission. In the DSM, weighted density control choices are used to group data into clusters and address security issues using an efficient clustering method. The effective data authentication protocol methodology is utilized to ensure data protection management, privacy management, and removal of transitional attacks. The entire architecture of DSM is shown in figure.1. The secured amount of data transfer among the users and the devices in the form of Encrypted data between the gateway in density control weighted method. The DCW has both accessible and non-accessible devices.

3.1 Density control weighted method (DCW)

The density control weighted method uses three stages: accessing, viewing, and all query distribution forms. Perhaps the information on the fog computing device is being read by the user; a username and user Identification would grant the user approval. If the user asks for uploading contents from the database, the bio-metrics are requested from the Fog user. The user can access both the passwords and the recipient's identity concerning biometric data. The trustworthy authorities grant the user authorization to enter the fog computing services in all performance situations, the petition, and their application is refused. The workflow of

Received: August 12, 2021. Revised: September 15, 2021

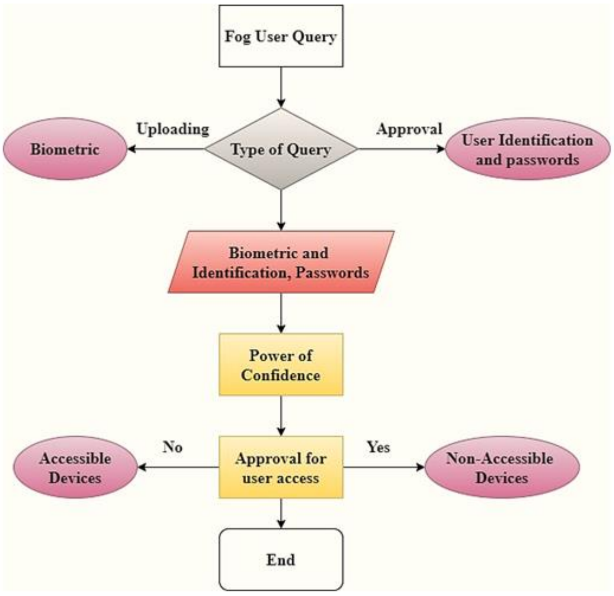


Figure. 2 The workflow of DCW

DCW is illustrated in Fig. 2. Users' queries and usage of biometric and identification, passwords for each user, are checked to access users' confidence. The users implement either accessible or non-accessible devices.

IoT devices like accessible devices are represented as $(I_1, I_2, \ldots\ldots I_m)$, non-accessible devices are represented as $(nI_1, nI_2, \ldots.nI_m)$ are included in the fog computing IoT infrastructure. The network systems, participants, and the gateway are the devices accessible in the IoT platform. DCW offers users multi-factor Encryption to secure stored data from unauthorized users in the fog computing device.

An authentication protocol is used to protect confidential data from protected IoT devices. The classified data is privately maintained in fog computing. In a private cloud, people preserve extremely confidential data to ensure high levels of data protection. It is important to detect hacking; sensitive data are encrypted with the two devices. The DCW encrypts non-accessible IoT data because individuals include non-accessible data contained in a public database.

In the fog computing device, accessible and non-accessible information is deposited through a gateway device, respectively. DCW introduces user authorization to connect deposited documents to deliver strong protection for the collected data. The Authorized Entity authenticates its users using recorded verification information known as user identification, username, and biometric data. The Authorized Entity offers three verification rates if a user checks or installs a public and private cloud document. Finally, the third encryption stage is carried out. The Authorized Entity collects user identification and biometric data and permits the personal fog computing device to read and download files.

IoT devices can detect, communicate and access information with integrated sensors to link things to the Internet. The data is generated and distributed through a wireless communications network to the gateway. The gateway is a portal of exchange from the fog computing device to the IoT. Simultaneously, information from IoT devices is received, and the detected data is transferred to fog.

The Authorized Entity is a trustworthy external party that protects unauthorized users' saved information and verifies fog services. The Authorized Entity often verifies registered users.DCW uses virtual fog computing devices to conduct separate tasks throughout companies as a computer system consisting of common and private data blends. With a hybrid data organization, the public data resources for senseless knowledge help to boost profitability. It is not just protection rather the applicable data management and storage specifications provided by a personal fog computing device.

To defend everyone from unauthorized users, the confidential system in the form of information is separated into two sections: Authentication and clustering. The authentication process encrypts one section of the information, and the remaining section is authenticated with the encrypted message. Although an unauthorized user may receive an encryption key, the user still cannot read the full information.

The authentication process's encoding and decoding process consist of two stages (a) pre-stage processing (b) post-stage processing. Due to Pre and post-stage steps, the cipher text would disclose the information in the first authentication round. The cipher code can disclose a portion of the information in the final clustering phase. The Authentication and the clustering process lead to data variation. For storing the analytical solution, different parameters are used. The portion of the broken data is needed to encode, and it is obtained by clustering protocol. The clustering protocol is asymmetrical technology, and Encryption is being used to build frame chips. Encryption is identical in the encoding system and can be easily carried out. The data management stage with the encryption and decryption stage with the subkey usage, as illustrated in Fig. 3.

The DCW divides the information into two sections to enhance data protection. The encryption system of the authentication process gains information at a significant level for

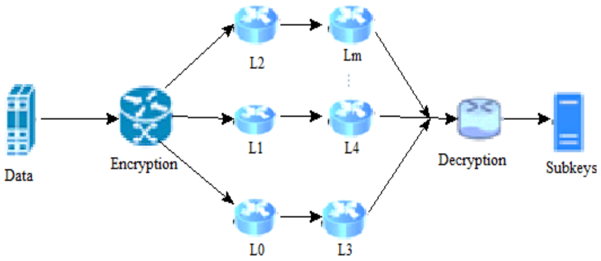


Figure. 3 The encryption and decryption for each stage of subkeys

Authentication. The authentication process requires several managing cycles of raw information. Each phase is controlled by a variation method for replacement. Almost every phase of the authentication phase in the authentication process is identical. The authentication process has a circular feature that is represented as G, and the subkeys for each stage are collectively represented as $L_0, L_1, \ldots\ldots L_m$.

Information T_{jv} is divided into two sequences that are represented as T_{jv_x}, T_{jv_y}. For every circle keys $s = 0{,}1 \ldots\ldots m$ the calculation can be represented as shown below:

$$T_{jv_x}(s+1) = T_{jv_y}(s) \tag{1}$$

$$T_{jv_y}(s+1) = T_{jv_x}(s) \otimes G(T_{jv_y}, G_j) \tag{2}$$

The circle key representation for two sequences T_{jv_x}, T_{jv_y} can be obtained from Equation (1) and (2), here G_j represent the main factor, $\otimes$ represent the AND function, the circle representation for each key is represented as s, $(s+1)$, G represents the key values.

The encryption and decryption stage of the authentication process of two sequences are represented with circle keys. The main benefit of the actual data is divided and then encrypted. A new range of security issues arises from the Internet of Things (IoT). In contrast to VPN cryptography, which guarantees network protections through an embedded and anonymized tunnel with IoT devices, robust safety and encryption requirements must be integrated throughout. This encryption and decryption system makes both activities more effective. The decryption stage is the opposite of the encoding from the first element to the first level, main parameters are presented.

The protection of IoT data is achieved by utilizing the two compact encryption protocols like authentication and clustering data processing time. The encoded information would be maintained via the virtual network that connects the IoT and distributed fog. Many protocols employed the creation of clusters and various data distribution interaction techniques. In addition to non-routing approaches, the cluster-oriented protocols use sensory modules more effectively for secured data transmission and response time.

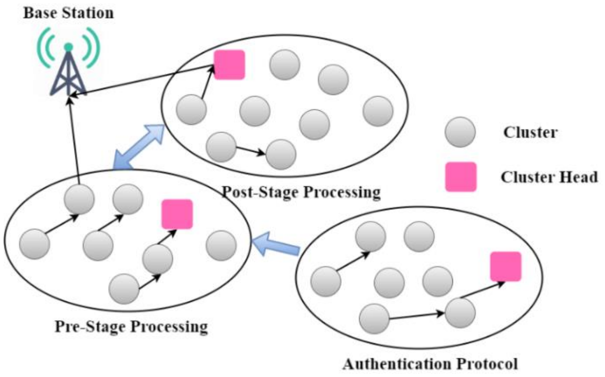


Figure. 4 The stages in the authentication protocol

The entire network of sensors is classified into separate clusters. The cluster head branch's responsibility is to acquire, add, and distribute data from their cluster into the node. To send the information immediately to the platform, the attack of data is therefore minimized. Several cluster-based networking protocols are explicitly used to improve the sensor nodes overall network life to secure various data theft. The routing protocol utilized the most commonly used clusters without centralized power for efficient data grouping the data transfer between the base stations. Fig. 4 shows the protocol for the authentication with the pre-processing and post-processing stage of data collection transmission between the access point. The information management between both the classification, the cluster head and the base station is shown in Fig. 4.

The cluster heads are chosen based on likelihood. The DCW election protocol is centered on secured data transfer, and it operates in a centralized environment. DCW shows a greater capacity similar to standard senor nodes for certain cluster heads in the system. There is a greater chance of a specialized node being a Cluster Head than a regular node.DCW is more effective, and it is selected repetitively to increase network durability and performance in the form of security. Furthermore, DCW is used extensively to pick the best cluster heads and improve sensor system capacity and reliability for the secured transfer of precise data.

Authentication process strength value (G) combines with the overall range of separation, and the minimum amount of cluster heads are described below:

$$G = u \times (E - SEP) + (1 - u) \times (M - cluster\ head) \tag{3}$$

The overall range of separation SEP and the minimum number of cluster heads $cluster\ head$ is obtained from Eq. (3); here, G represents the authentication process strength value, u represents the scaling parameter, E, M represents the scaling parameter quality value. Specified quality values are described below:

$$G = \sum_x \beta(u_x, g_x), \forall g_x = (T, R, SV, TE, P) \tag{4}$$

The specified quality values are obtained from Eq. (4). Besides, DCW proposed a toughness-based strength feature (T), specific sensor device range to the access point (R), system separated variance (SV), energy used for transmission (TE), and numerous transmitted packages (P). u_x represent the scaling parameter, $g_x$represent the quality of the given data, β represents the number of data used for transmission.

DCW is extended to include remaining energy (re) and several shared points (sp) in the above fitness mechanism, and it is shown below:

$$G = \sum_x \beta(u_x, g_x), \forall g_x = (T, R, SV, TE, P, re, sp) \tag{5}$$

The fitness mechanism is obtained from Eq. (5), T, R, SV, TE, P are the parameters explained in Eq. (4), here re represent remaining energy, (sp) represent several shared points, the quality of given data is represented as g_x, the number of data used for transmission is represented as β.

To protect the data transfer among sensor nodes, DCW uses a technique based on authentication and clustering. The authentication process considers the best cluster set, while the clustering process is often used to pick the cluster participants. The objective functions regarded as described below:

$$G = u_1 \times \left(\frac{1}{sch}\right) + u_2 \times sgd \times u_3 \times schd \times u_4 \times sep \tag{6}$$

$$G = u_1 \times \left(\frac{1}{tml}\right) + u_2 \times \left(\frac{1}{sp}\right) + u_3 \times se \tag{7}$$

The objective function to maintain the security level is obtained from Eqs. (6) and (7), here sch refers to the interpretation of all clusters to base station length, sgd represents each clusters intensity number, $schd$ is the clusters heads core value number, sep represent the secret and protected range of data transmission, tml refers to the total gap between individual and cluster. tml represents the distance between the actual system and the strongest regional server. The total security data management is indicated byse.

Furthermore, DCW transfers data to all cluster heads with the cumulative grouped resources at the head and eventually the volume of the received resources in the transfer of data gathered to Base Station by considering the total amount of energy absorbed by non-cluster heads. The transfer activity mechanism of data is described below:

$$G = (\sum_{j=1}^{md} \sum_{r \in D_j} C_{tr,cluster_j} + C_{RC} + C_B + \sum_{j=1}^{md} C_{tr,cluster_j} \tag{8}$$

The transfer activity mechanism of data is obtained from Eq. (8), here md represent the complete cluster head, $r \in D_j$ represent the non-cluster head related with j-th cluster head, $C_{tr,cluster_j}$, C_{RC} represent the transmitting and receiving activity of data. C_B represent the activity mechanism for data.

To improve a stable authentication process's efficiency, the cluster heads are centered on a furious approach. Three parameters, including sink duration, diversity level, and knot strength, set out the fuse-based deduction principles in the clustering stage. In the DCW method, implementing multi-hop interaction through the cluster heads on the sink and among sensor nodes onto the clusters gives better security options. The authentication process suggested a new clustering technique that is focused on geographical optimization data transmission. The appropriate cluster heads are chosen to minimize the cluster intensity and optimize cluster dispersions based on the represented goals.

The DCW specification separates its usability into two main parts. The first part of the DCW protocol is the Hidden Exchange Clustering System for safe forwarding and the optimal hierarchical route configuration. The optimized cluster heads calculate the efficient data transfer and match the dispersed clusters based on multiple parameters and quality restrictions. The proposed clustering system often enhances system capacity with low bandwidth and power usage among the sensor nodes. The second component is a safe and reliable route among the cluster heads and the base station to prevent malicious activity from intruding.

At the start of the configuration process, the nodes' collection is uniformly distributed in a curved channel area. Each node is fixed and has a single with minimal identified data. Because of countless capital, the Base Station has no limit on the secured amount of data management. Base Station is spreading the tracking area through its localization and has obtained all the initial stage points. Besides, each node's forwarding list is modified by including the details from the neighbor. Cluster Protocol then dispersedly reveals the protocol for cluster head collection in the system region.

The importance for all domains is calculated by utilizing residual energy (RE), Obtained Data Transmission (ODT), range from one Base Station to another base station (R), and line duration (LD). Each node collects input from its neighbor by exchanging a code of authority. First of all, node energy contributes most to the station's existence, which gives a node greater importance to the full cluster head. Second, recall the RSSI helps calculate the wireless connection output, which provides a better transmission level if the ODT quality is more than one limit.

The cluster protocol calculates the ODT limit that is the mean receipt rate for Mneighbor heads at a specific time, and it is described below:

$$ODT_{limit} = \frac{y}{M} \times RE + R + LD \tag{9}$$

The ODT limit at a specific time is obtained from Eq. (9), y represent the attempt to decide the node packet transmission rates, M represents the neighboring cluster head, RE represent the residual energy, R represent the distance from one base station to another base station, LD represents the line duration for each data.

The simplest node route to Base Station reduces energy use and the lifespan of the system. The length duration element ultimately increases data supply efficiency and tests the node congestions. The length of data and the security management of each transmission are described below:

$$LD_j = \frac{SS_j}{PQ} + ODT_{limit} \tag{10}$$

The length of the data and the security management between nodes is obtained from Eq. (10), here SS_j represent the data transfer between receipts for each packet, PQ represents the buffer values, j represent the node's length. The transmission of data is balanced, and the security level is described as shown below:

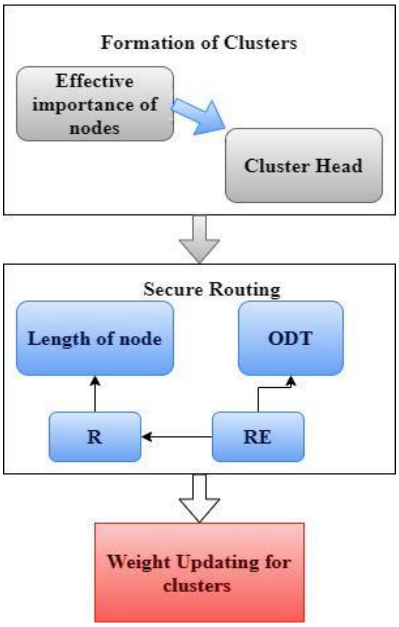


Figure. 5 The transmission of data and the security level in each cluster heads

$$D_u = u_1 \times a_j + u_2 \times ODT_{limit} + u_3 \times \left(\frac{1}{R}\right) + u_4 \times LD \tag{11}$$

The transmission of data is balanced, and the security level is obtained from Eq. (11), here u_1, u_2, u_3, u_4 represent the weighting variables for the various choice components of the node, such as residual energy (RE), Obtained Data Transmission (ODT), range from one Base Station to another base station(R), and line duration (LD).The transmission of data and the security level in each cluster head are illustrated in Fig. 5. The formation of clusters and the security routing among all the weighing variables play a major role in DCW. The data transfer between nodes and cluster head is defined in the below equations.

All weights indicate the special impact in the calculation of the profitable node value throughout the selection procedure while $u_1 + u_2 + u_3 + u_4 = 1$. Eventually, the balanced data transmissionis used for summarizing all the variables as shown in Eq. (11), and D_u represent the first cluster head for the node. The proposed DCW protocol is, therefore, more flexible in selecting optimizing cluster heads related to internal properties and generating clusters

Besides, the ODT portion is integrated with the cluster head collection system showing wireless connectivity efficiency. A suitable node is the cluster head's choice centered on the shortest number from R. At a specified distance, each node transfers lightning packs to its neighbors. The neighboring node calculates its ODT value and returns it to the

Received: August 12, 2021. Revised: September 15, 2021

source node after acquiring the data. After the processing stage, the length duration element must be easily integrated into the cluster head's distribution process. Thus, the node is chosen more than a certain limit as a cluster head.

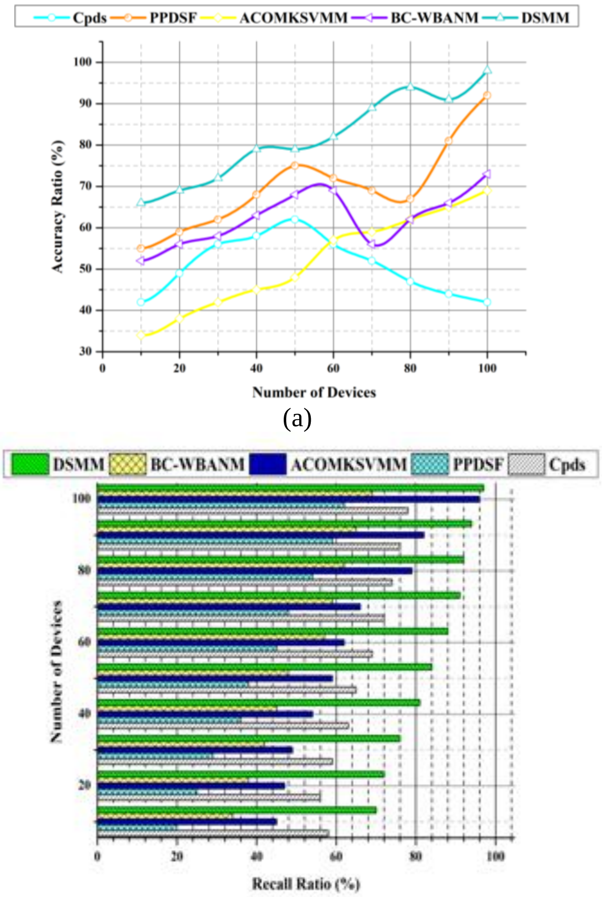
4. Numerical results and discussion

This paper discussed the fog computing-based IoT devices data processing stage, and a huge amount of information is stored on the third-party database. Although these strategies provide useful additional benefits to the customer, data storage, anonymity, latency at the edge of nodes, and energy usage continue to be major issues. This article addresses and uses the efficient fog authentication protocol as an alternative tool for recovering and storing data from third parties connected with data transmission. Due to the distributed architecture and other improved fog computation features, the density control weighted (DCW) election protocols proposed a fast response time and fewer overheads. In addition, the privacy of the fine-grained energy use of data is preserved in the data privacy and the data aggregation processes of DSMM structures. Comprehensive performance evaluation results indicate that the proposed protocols are superior in data transmission and storage utilization to DCW without data aggregation. The effects of each protocol are analyzed in terms of the transmitting and storage performance.

The efficiency of the DSMM is considered based on the parameters like data processing time, accuracy, recall, precision, response time, security rate, and effective data authentication ratio compared to Compressed and Private Data Sharing framework (Cpds) [27], Privacy-preserved data-sharing framework (PPDSF) [28], ACOMKSVM [29], Blockchain technology with Wireless Body Area Networks (BC-WBANM) Model [30].

4.1 Accuracy ratio and recall ratio (%)

Fog computing still selects their next fog server directly, and the fog node would certainly realize that the third party using their computational power is close at hand. The best way to maintain the site's anonymity is by identifying obstruction, which allows the user to locate a neat user even though the fog node knows it is nearby. The authors use a trustworthy third party to create a false Identification for the end-user. The fact is that a customer does not choose the closest fog node and selects one of the fog nodes they can enter, such as latency, credibility, load balance, etc. The accuracy and the recall ratio is shown in Fig. 6(a) and 6(b)



(a)

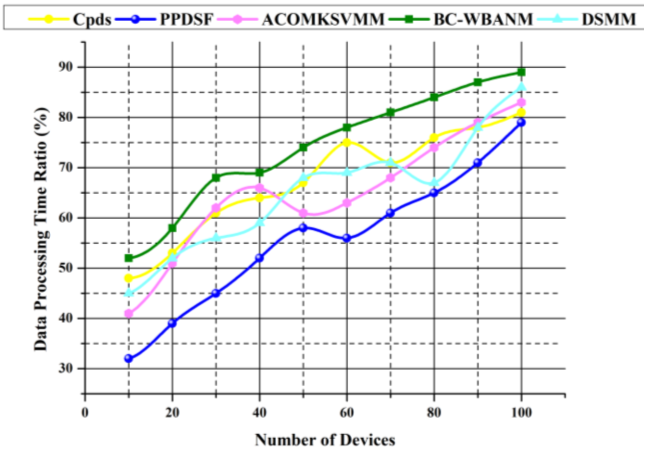
(b)

Figure. 6: (a) Accuracy ratio and (b) Recall ratio (%)

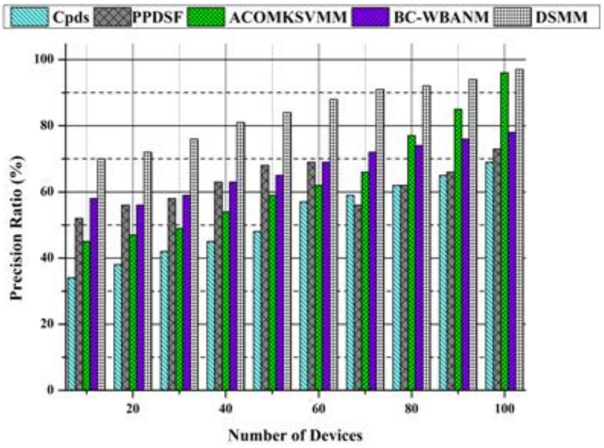
Furthermore, the proposed authentication protocol is based on a dynamic, key-driven approach that makes a good balance between security and computer complexity. Any fragments, along with the appropriate dynamic key, should be obtained to recall the data. This makes the attacker work difficult to reveal the encrypted details, which must compromise fog nodes. In addition, attackers can search for the dynamic key, in which each input data is different. Safety and consistency checks demonstrate a high degree of reliability and robustness in the proposed safety system.

4.2 Data processing time ratio and precision ratio (%)

From an attacker's perspective, the fog computing-based data transmission node has the same chance of being a cluster head before the election process. The attacker cannot foresee an election mechanism and would affiliate with some association unpredictability for each node to become a cluster of the election process. The attacker cannot find the node's position, and every member sends



(a)



(b)

Figure. 7: (a) Data processing time and (b) Precision Ratio

data to inform the cluster head is a member in the final stage of the algorithm. The cluster head wants to know their cluster partners to assign tasks and organize the data transfer for collective processing. The data processing time and the precision rate is shown in Fig. 7(a) and 7(b)

Clustering with the hierarchical structures is based on nodes and more effectively uses finite resources, such as frequency spectrum, bandwidth, and power. The cluster size approximately coincides with the direct nodes' connectivity simpler protocols for routing and broadcasting within the cluster. Clustering can monitor network health and identify malfunctioning nodes since some nodes in a cluster can play watchdogs over another node. Finally, networks may consist of node mixtures with stronger features or special characteristics, such as an expanded contact range.

4.3 Response time ratio (%)

Centralized training methods are ideal for networks where the computing power is mostly based on a single computer. The cluster nodes play various roles by their cluster tasks. The gateways can turn off to minimize energy use, and the lead agents detect many gateways that bind the same leading nodes. The proposed DSMM describes a range of reliability characteristics to compare current solutions of cluster heads. These properties are essential to ensure a stable and efficient cluster head election protocol. The series of properties includes fundamental concepts and advanced concepts. The response time of DSMM is illustrated in Fig. 8.

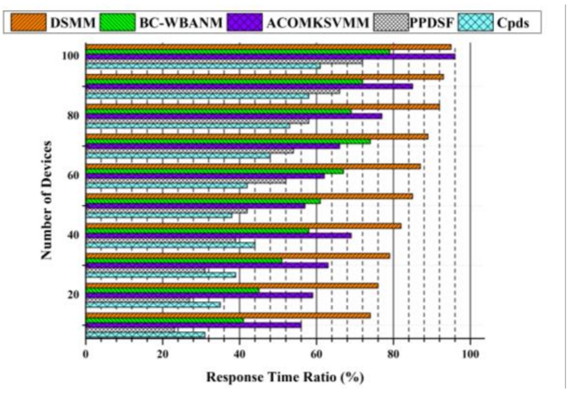


Figure. 8 Response time ratio (%)

4.4 Data security rate (%)

DSMM is focused on enhancing the data security level during the transfer of data among IoT devices. The IoT uses fog computing devices for data transfer protection and database privacy problems. Although certain problems can be dealt with current systems, new difficulties are faced because of different fog computing features such as fog node heterogeneity and fog networks, mobility service requirements, and low latency. User data is outsourced to the fog node, where access to the cloud node. Initially, it is difficult to guarantee data accuracy since the outsourced data can be protected. Secondly, authorized parties may use the uploaded data for other purposes. The data security rate of DSMM is shown in Fig. 9.

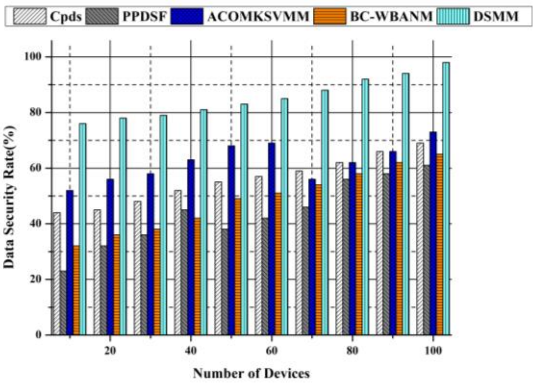


Figure. 9 Data security rate (%)

Table 1. Performance ratio (%)

Number of Devices	Cpds	PPDSF	ACOMKSVMM	BC-WBANM	DSMM
10	56.21	65.24	51.23	42.44	71.24
20	60.33	67.12	54.28	44.22	71.38
30	61.47	68.25	57.35	45.38	74.14
40	69.35	69.27	59.21	57.45	76.27
50	72.21	67.19	62.26	59.11	79.25
60	71.15	65.14	65.29	59.29	82.26
70	68.25	69.19	68.19	56.11	87.13
80	66.69	64.21	69.21	61.29	88.38
90	66.17	67.22	73.22	65.11	91.89
100	68.16	68.34	75.24	68.17	92.21

Table 2. Effective data authentication ratio (%)

Number of Devices	Cpds	PPDSF	ACOMKSVMM	BC-WBANM	DSMM
10	44.11	23.21	52.12	32.21	75.11
20	45.23	32.43	56.33	36.13	77.12
30	48.01	36.15	58.24	38.25	78.26
40	52.13	45.52	63.61	42.43	80.48
50	55.16	38.67	68.31	49.22	82.61
60	57.24	42.31	69.22	51.27	84.81
70	59.38	46.23	56.17	54.31	86.12
80	62.22	56.42	62.14	58.12	90.28
90	66.56	58.18	66.02	62.18	91.33
100	69.16	61.51	73.09	65.19	94.91

4.5 Performance ratio (%)

The most significant data value is a direction consistency defining variable dependent on metrics. Many additional protocols for WSNs are suggested, and DCW has additional energy targets, for which its key priority is network security. Clustering for large-scale WSNs is to increases the scalability of the network and achieves high levels of scalability. Many research projects have suggested a multi-hop connectivity to minimize energy usage and prolong the sensor network's existence. However, the node's intermediate routing is eliminated with the multi-hop algorithms, reducing energy consumption. The Performance Ratio of DSMM is shown in Table 1.

4.6 Effective data authentication ratio (%)

A new and appropriate architecture for sensor networks is an authentication and key energy-efficient framework. Data confidentiality and authenticity are required for DCW and encryption algorithms. The attack's consequences are reduced by following three steps are i) a primary pre-delivery process, (ii) an initialization phase of the network, and (iii) an authentication protocol. The first phase is initially performed during the node production period. The device generates and safely stores the asymmetrical master key for the whole network. The second stage occurs during network deployment, where each node finds its neighbors within the contact range and establishes network security. The Effective Data Authentication Ratio (%) is shown in Table 2.

5. Conclusion

In this paper, DSMM has been proposed to address all the security and privacy issues among IoT devices during data transmission. The proposed DSMM includes the density control weighted election that uses the efficient clustering approach to organize the data into clusters to solve these security issues. Authentication protocol technology is used for computer authentication, privacy management, and the elimination of intermediate attacks. The Density Control Weighted (DCW) election protocol uses the clustering procedure to select a cluster leader and participants. The data were transferred through the application of the extensible authentication protocol from the chosen routing method. DSM guarantees privacy protection and effectively eliminates mid-term attacks. Thus the experimental results of DSMM achieve a data processing time ratio of 86.3%, data security 98.09%, precision 97.23%, performance 92.21%, effective data authentication ratio 94.91%, recall 97.25%, response time 96.18% when compared to other methods. Our plan on other aspects of the protocol to be extended in the future. To demonstrate our protocol's higher computing efficiency and dependability, it investigates lightweight ciphers and applies formal approaches to optimize encryption techniques.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization Jalasri.M; methodology Jalasri.M; software, Jalasri.M; validation, Jalasri.M; formal analysis, Jalasri.M; investigation, Jalasri.M; resources, Jalasri.M; data curation, Jalasri.M; writing—original draft preparation, Jalasri.M; writing—review and editing, Jalasri.M; visualization, Jalasri.M; supervision, Dr.L.Lakshmanan;

Received: August 12, 2021. Revised: September 15, 2021

References

[1] Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. A. Ahmad, "Fog computing security and privacy for the Internet of Thing applications: State of the art", *Security and Privacy*, Vol. 4, No. 2, pp. 1-26, 2021.

[2] L. Wang, H. An, and Z. Chang, "Security enhancement on a lightweight authentication scheme with anonymity fog computing architecture", *IEEE Access*, Vol. 8, pp. 97267-97278, 2020.

[3] F. Y. Okay, S. Ozdemir, and Y. Xiao, "Fog computing based privacy preserving data aggregation protocols", *Transactions on Emerging Telecommunications Technologies*, Vol. 31, No. 4, 2020.

[4] C. Rupa, R. Patan, F. A. Turjman, and L. Mostarda, "Enhancing the access privacy of IDaaS system using SAML protocol in fog computing", *IEEE Access*, Vol. 8, pp. 168793-168801, 2020.

[5] Y. Qu, L. Gao, T. H. Luan, Y. Xiang, S. Yu, B. Li, and G. Zheng, "Decentralized privacy using blockchain-enabled federated learning in fog computing", *IEEE Internet of Things Journal*, Vol. 7, No. 6, pp. 5171-5183, 2020.

[6] U. Verma and D. Bhardwaj, "Design of Lightweight Authentication Protocol for Fog enabled Internet of Things-A Centralized Authentication Framework", *International Journal of Communication Networks and Information Security*, Vol. 12, No. 2, pp. 162-167, 2020.

[7] E. Alemneh, S. Senouci, P. Brunet, T. Tegegne, "A two-way trust management system for fog computing", *Future Generation Computer Systems*, Vol. 106, pp. 206-220, 2020.

[8] T. Khalid, M. Abbasi, M. Zuraiz, A. Nasir Khan, M. Ali, R. Ahmad, J. P. C. Rodrigues, M. Aslam, "A survey on privacy and access control schemes in fog computing", *International Journal of Communication Systems*, Vol. 34, No. 2, 2021.

[9] B. Mohanta, D. Jena, and S. Sobhanayak, "Multi-party computation review for secure data processing in IoT-fog computing environment", *International Journal of Security and Networks*, Vol. 15, No. 3, pp. 164-174, 2020.

[10] T. Wenyi, B. Qin, L. Yanan, and W. Qianhong, "Functional privacy-preserving outsourcing scheme with computation verifiability in fog computing", *KSII Transactions on Internet and Information Systems*, Vol. 14, No.1, pp. 281-298, 2020.

[11] H. Ali, K. M. L. Mat, N. B. Anuar, R. Noor, and M. Ahmad, "Performance and security challenges digital rights management (DRM) approaches using fog computing for data provenance: a survey", *Journal of Medical Imaging and Health Informatics*, Vol. 10, No. 10, pp. 2404-2420, 2020.

[12] A. Muhammad, G. Wang, V. E. Balas, O. Geman, A. Castiglione, and J. Chen, "Sdn based communications privacy-preserving architecture for vanets using fog computing", *Vehicular Communications*, Vol. 26, 2020.

[13] A. Patwary, A. Fu, S. Battula, R. Naha, S. Garg, and A. Mahanti, "FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain", *Computer Communications*, Vol. 162, pp. 212-224, 2020.

[14] A. H. M. Ali, G. F. A. Ahammed, and R. Banu, "Energy Aware Hierarchal Data Aggregation and Trust Based Data Integrity Verification for WSN", *Psychology and Education Journal*, Vol. 58, No. 1, pp. 5637-5643, 2021.

[15] T. Liu, Y. Liu, J. Liu, L. Wang, L. Xu, G. Qiu, and H. Gao, "A Bayesian learning based scheme for online dynamic security assessment and preventive control", *IEEE Transactions on Power Systems*, Vol. 35, No. 5, pp. 4088-4099, 2020.

[16] T. Hidayat and I. Riadi, "Optimation Wireless Security IEEE 802.1 X using the Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP)", *International Journal of Computer Applications*, Vol. 174, No. 11, pp. 25-30, 2021.

[17] J. S. Gomez, D. G. Carrillo, R. M. Perez, and A. F. Skarmeta, "Secure authentication and credential establishment in narrowband IoT and 5G", *Sensors*, Vol. 20, No. 3, p. 882, 2020.

[18] N. Marques, A. Zúquete, and J. P. Barraca, "EAP-SH: An EAP Authentication Protocol to Integrate Captive Portals in the 802.1 X Security Architecture", *Wireless Personal Communications*, Vol. 113, No. 4, pp. 1891-1915, 2020.

[19] S. Hong, "P2P networking based internet of things (IoT) sensor node authentication by Blockchain", *Peer-to-Peer Networking and Applications*, Vol. 13, No. 2, pp. 579-589, 2020.

[20] M. Das, P. Kumar, and A. Martin, "Secure and privacy-preserving rfid authentication scheme for internet of things applications", *Wireless*

Personal Communications, Vol. 110, No. 1, pp. 339-353.

[21] X. Jia, N. Hu, S. Su, S. Yin, Y. Zhao, X. Cheng, and C. Zhang, “IRBA: an identity-based cross-domain authentication scheme for the internet of things”, *Electronics*, Vol. 9, No. 4, p. 634, 2020.

[22] H. Zhong, Y. Geng, J. Cui, Y. Xu, and L. Liu, “A weight-based conditional privacy-preserving authentication scheme in software-defined vehicular network”, *Journal of Cloud Computing*, Vol. 9, No. 1, pp. 1-13, 2020.

[23] L. Ding, W. Zhongsheng, W. Xiaodong, and W. Dong, “Security information transmission algorithms for IoT based on cloud computing”, *Computer Communications*, Vol. 155, pp. 32-39, 2020.

[24] L. H. Álvarez, J. M. D. Fuentes, L. G. Manzano, and L. H. Encinas, “Privacy-preserving sensor-based continuous authentication and user profiling: a review”, *Sensors*, Vol. 21, No. 1, 2021.

[25] H. S. Trivedi and S. J. Patel, “Design of secure authentication protocol for dynamic user addition in distributed Internet-of-Things”, *Computer Networks*, Vol. 178, 2020.

[26] M. U. Ashraf, K. M. Jambi, R. Qayyum, and H. Ejaz, “IDP: A Privacy Provisioning Framework for TIP Attributes in Trusted Third Party-based Location-based Services Systems”, *International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 7, pp. 604-617, 2020.

[27] S. Qi, Y. Lu, Y. Zheng, Y. Li, and X. Chen, “CPDS: enabling compressed and private data sharing for industrial internet of things over blockchain”, *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 4, pp. 2376-2387, 2021.

[28] X. Zheng and Z. Cai, “Privacy-preserved data sharing towards multiple parties in industrial IoTs”, *IEEE Journal on Selected Areas in Communications*, Vol. 38, No. 5, pp. 968-979, 2020.

[29] B. L. Nguyen, E. L. Lydia, M. Elhoseny, I. V. Pustokhina, D. A. Pustokhin, M. M. Selim, N. N. Gia, and K. Shankar, “Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data”, *Computers, Materials & Continua*, Vol. 65, No. 1, pp. 87-107, 2020.

[30] L. Xiao, D. Han, X. Meng, W. Liang, and K. C. Li, “A secure framework for data sharing in private blockchain-based WBANs”, *IEEE Access*, Vol. 8, pp. 153956-153968, 2020.