# A Secure Recommender System Model for Service Placement in Wireless Networks

https://doi.org/10.3991/ijim.v17i11.37369

Luan Gashi[1(✉)], Artan Luma[1], Halil Snopçe[1], Ylber Januzaj[2]
[1] South East European University, Tetovo, N. Macedonia
[2] University of Business "Haxhi Zeka", Peja, Kosovo
lg29758@seeu.edu.mk

**Abstract—**Edge or fog computing is being used to reduce latency between end devices and traditional cloud computing. The latest developments that have improved the hardware aspects of wireless sensors and mobile networks, allowed other enhancements if such technologies are integrated between them. Regarding this enhanced heterogeneous environment, the approach of placing services needs to reconsider the cybersecurity aspects. Reviewing the related work on service placement and clustering, we have seen that no technique could be used as a template for finding the most valuable node about its cybersecurity metrics when multi-tier computing networks are used. So, we have developed a baseline method of a solution that fulfills the cybersecurity requirements converging with a proposed integrated multi-tier wireless networking model. This is achieved by enhancing the K-means algorithm with added processing steps. Initially, K-means clustering is executed, then three more specific parameters will define the cluster members' status, respectively about its confidentiality, integrity, and availability. The summarized results provided at the end of the process determine the most trusted cluster member within a cluster of 50 networked nodes which is recommended to serve as a node for placing securely the requested service. Results show that our proposal stands and that further studies based on this approach have enough arguments to be researched.

**Keywords—**networks service placement, fog and edge clustering, wireless networks, mobile communication, CIA triad

## 1 Introduction

Wireless sensor networks (WSNs) have opened many new possibilities for emerging applications in event tracking and surveillance [1]. WSNs collect environmental data, so this information can be used to support the decision-making process in critical situations if such sensors are installed for this purpose. Nevertheless, there are challenges regarding all these new technological paradigms, especially where mobility and security are concerned.

According to our earlier research [2], the model for a recommender system that transmits WSN data through Next Generation of Mobile Networks (NGMN) can be deployed by using multi-tier computing networks. There are plenty of indications that an integrated model which transmits WSNs data through NGMN, can be deployed using edge, fog, and cloud computing. Moreover, our findings show that WSNs are considered a subset of IoT and have the same limitations considering their processing, storing, and transmitting data. So far, cloud computing is shown as a helpful technology, but it must be deployed closer to sensor gateways to decrease network latencies and response time, and this issue would be mitigated by using edge or fog and cloud computing, where the next generation of mobile networks such as 5G and 6G play the leading role by improving the latency during data transmission [2].

On the other hand, even though sensitive information and data are hosted in their environment, the security of customers' data traditionally has been the direct responsibility of the cloud service provider [3]. But, assessing and managing risk in cloud-based computing systems can be a challenge, since significant portions of the computing environment are under the control of the cloud provider and may be beyond the organization's purview, however, accountability for security and privacy in public cloud deployments cannot be delegated to a cloud provider and remains an obligation for the organization to fulfill [4]. Related to this, the Cloud Standards Customer Council (CSCC) Security for Cloud Computing at 10 Steps to Ensure Success white paper [5] prescribes a series of ten steps that cloud service customers should take to evaluate and manage the security of their cloud environment to mitigate risk and deliver an appropriate level of support [6]. The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment and, according to their security guidance v4.0, cloud users should consider the use of data masking or obfuscation when considering a service that does not meet security, privacy, or compliance requirements [7].

Regarding previous statements and since fog and edge computing are considered extensions of cloud services to the network nodes [8], we will construct and present in this paper such a model to define how this integrated solution would be organized considering information security. The paper aims to provide a baseline for a secure recommender system that can support the decision-making for service placement fulfilling the CIA (Confidentiality, Integrity, and Availability) triad principles. The focus of the study is going to be on edge network nodes using wireless communication. Additionally, composing likewise a system will help the process of making decisions for service placement, dependable on various properties of network nodes that might belong to this proposed solution model.

This paper is structured as follows: Section 2 shows the related work on service placement, clustering techniques, and cybersecurity used in WSNs, edge, and fog computing. Section 3 presents the formulation of the problems and Section 4 presents the methodology for solving the problem based on k-mean clustering enhancement. Section 5 shows the results and their analytic interpretation based on the conducted experiment. Lastly, Section 6 are presented the future research that is obtained from analyses according to this ongoing study.

Our results show that using the CIA triad is possible even in the clustering phase of network nodes, by giving this an enhanced security approach to placing services for heterogeneous wireless networks which is the aim of this study. We believe that this study will serve as a basis to explore further research towards the integration and optimization of information systems according to today's security challenges.

## 2 Related work

According to our model promises and the aim of our study where the wireless networks are on focus, we consider that the proper parameters to be used for service placement should be those which are deployed on a distributed design of control plane, in an online manner, a dynamic approach of service placement and the mobility support.

### 2.1 Service placement

Cloud computing networks have a centralized nature of services which does not meet most of the requirements that decentralized sensors nature and, consequently fog and edge computing networks have, so this means that placing a service in such networks that optimize the node request might be a serious challenge, but it might be improved by applying different techniques [9].

Salaht et al. in their study give an overview of service placement problems in fog and edge computing. Among others, they present a taxonomy based on their summarized literature review which classifies service placement on required support of parameters like centralized or distributed, offline or online, static, dynamic, and mobile or not mobile. Also, they give the currently considered metrics being used to optimize the deployment of service placement such as latency, resource utilization, cost, energy consumption, quality of experience, and in a summarized way the availability of network nodes [10].

Susa et al. in their study combined two layers of fog-cloud architecture, aiming to reduce cloud access latency in IoT scenarios. Accordingly, services can use geographically distributed network elements in scenarios such as smart cities or intelligent transportation systems, reducing the requirement for additional cloud resources and avoiding high latency. The presented results demonstrate the benefits of service distribution across multiple low-latency fog nodes, thus avoiding high-latency access to upper layers. Furthermore, using a second fog layer enables low latency in moderate volume service request scenarios where not enough IoT resources are available in a single-hop wireless connection, but on the other hand no connection to the cloud [11].

To facilitate the bottlenecks of processing data on the cloud due to large communication latency to real-time applications, Singh et al. by considering the multi-tier nature of the Edge/Cloud architecture, have proposed an algorithm named RT-SANE which is security and performance aware. This algorithm provides better performance by scheduling applications and jobs to be executed in several places based on the distributed orchestrator and its protocol, compared to all execution to the cloud [12].

There are different system models for fog computing frameworks based on resource provisioning that are presented like that of Skarlat et al. where the time-shared provisioning for fog services together with space-shared provisioning decreased by up to 39% [13]. Similarly, a greedy algorithm that optimizes service placement by considering the gradient approach of bandwidth consumption of both the cloud links and the fog crosslinks avoids bottlenecks and impairment of applications [14]. A near-optimal latency while effectively offloading computational tasks across fog and cloud layers based on an online algorithm can avoid the unpredictable arrival of available neighboring fog nodes and can be used as an optimization framework for fog formation [15] and minimizing the latency by suitably selecting the neighboring nodes while effectively offloading the tasks to the neighboring fog nodes and the cloud [16] as well as reducing the service delays during fog offloading [17]. This can be enhanced even more by allocating resources to meet service level agreement (SLA) and QoS for optimizing big data distribution in fog and cloud environments [18] like placing end device services on virtual distributed fog resources [19].

At edge networks, there is an approach of increasing the utilization of edge resources by collaborative execution of application modules between neighboring edge nodes [20] where latency improvement and cost reduction based on the magnitude and location of user demands are clustered in multiple small geographical areas through a decentralized dynamic replica placement algorithm [21]. Dynamic, distributed service placement can potentially provide workload orchestration and higher QoE [22].

Besides minimizing cost, maximizing reliability by monitoring the resource requirements, usages, and available capacities is considered as well for service placement in fog and edge networks, so, increasing reliability is another consideration in service placement at fog computing which increases the overall cost as well. There is a proposed algorithm that provides placement decisions ensuring timely service responses known as the Cost and Reliability-aware Eagle-Whale (CREW) policy which considers the distinct types of failures in hierarchical Fog environments [23].

The requirements for most delay-sensitive services are to be treated in an online manner with a dynamic approach and mobility of service placement. Supporting mobility has always been a challenge in dynamic online service placement. Programming a mobile fog was one of the first ideas when the concept of fog networks came as a solution for delay-sensitive services [24], [25].

Mobile fog led to the concept of Mobile edge computing (MEC) once the edge devices increased their capabilities due to technological developments. MEC emerged as a promising solution for servicing delay-sensitive tasks at the edge network where request scheduling [26] and an online service tree placement in edge networks, to jointly optimize the received utility and network congestion by mapping hierarchically subtasks are considered [27], and where the Lyapunov and Markov algorithm for a centralized scheme are used as the optimization technique for service placement [28], [29].

Mobile edge computing reflected poorly on cellular networks. To cover the non-cellular networks which require edge computing, in 2017 the European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG) changed the name of Mobile Edge Computing to Multi-Access Edge Computing which supports heterogeneous networks using LTE™, 5G, fixed and WiFi technologies [30]. An interesting and motivated approach to service placement is that of using the state of the underlying community networks to optimize service deployment where a new placement heuristic based on bandwidth and availability is used to deploy the service [31].

According to this, we can say that elements of the CIA triad are treated as related works, even though not fully like our study intends to do.

### 2.2 K-means algorithm and technique

K-means is a technique of the unsupervised clustering methods, which was first proposed as an algorithm by Stuart Lloyd in 1957 but was published just later in 1982 [32], while as a term was used by James MacQueen in 1967 [33]. The K-means algorithm is referred to as the Lloyd–Forgy algorithm since Edward W. Forgy published the same method in 1965 [34].

Being considered the simplest learning algorithm that classifies a given dataset, K-means defines clusters and their centroids, respectively one centroid for each cluster, through which the issue of clustering is solved [35]. Each cluster represents data with equivalent properties and is represented by its centroid which is the mean of cluster members, defined through a process that uses squared Euclidean distance as the similarity measure for cluster membership [36], which is presented by the formula:

$$J=\sum_{i=1}^{n}\sum_{j=1}^{k} d(x_i,\ x_c)^2\ ,\ for:\ i=1,2,\ldots,n\ \ and\ \ j=1,2,\ldots,k \qquad (1)$$

Where $d(x_i, x_c)^2$ represents the Euclidean distance that is used to determine the distance between node $x_{ij}$ with its cluster centroid $c_j$, “i” refers to the number of nodes, and “j” refers to the cluster number. According to Hasan, A. et al. there are four algorithmic phases of this process:

**Phase 1:** Locate the k centroids node in the space which is represented by the data set, where K is a predefined number;

**Phase 2:** Allocate every node of data to the specific cluster, which has the nearest centroid distance;

**Phase 3:** Once all nodes of data have been clustered, re-determine the locations of the k centroids;

**Phase 4:** Reiterate Phase 2 and Phase 3 till no shown change in the location of centroids [37].

Since clustering is used in most studies as a basic technique to define the centroid which is the cluster’s head node that commonly routes the communication to the base station, many authors have focused their studies on improving these algorithmic phases [38-41].

### 2.3 CIA triad components

Several frameworks define and treat the CIA triad components like the Information Systems Audit and Control Association (ISACA), the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (ISO/IEC) 27001 standard series [42-44]. The CIA triad consists of three processes which are also the goals of cybersecurity. These frameworks offer the best practices and guidelines for information security, as well as requirements to be processed that contain actions through which is provided the protection of confidentiality, the maintenance of integrity, and the assurance of availability.

Frameworks that define and treat the CIA triad are more specifically related to traditional information technologies and are not adequate for technologies such as sensors, respectively IoT devices. Due to this doubt, we have explored other standards developers such as the International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC) which deal closer to the nature of sensors, but from their perspective, only the availability is treated as a critical aspect of security [45, 46].

## 3 Problem statement

Concluding the related work in Section 2 on service placement and clustering, we can see that no technique could be used as a template for finding the most valuable node regarding its cybersecurity metrics when multi-tier computing networks are used. All the related studies contribute separately to specific issues within its tier of a homogenous network like cloud, edge, or fog and give solutions through which optimize properties like delays, latency, resource utilization, cost, energy consumption, quality of service and experience, availability of network nodes or cost minimization by choosing the proper network node which can provide such as optimized service. This is achieved by developing new algorithms for specific issues or by enhancing the existing ones mentioned in earlier sections, and where initially the clustering algorithm such as K-means is used to serve as a starting configuration which is based only on the distance mean of the cluster members.

Accordingly, since there is found partially or not any clustering method which considers more than one property of the network node to be employed for serving, there must be a solution developed which uses K-means clustering as a pre-processing step and then adds summarized node's properties based on CIA triad requirements to define the most trusted cluster member to be chosen for placing services or even representing the cluster. The solution should be deployed in heterogeneous networks, where the end devices such as wireless sensors or nodes, respectively communicate between them through a mesh type of communication topology.

## 4 Proposed methodology

Since K-means clustering is used specifically for a homogenous network and it is based on only one property of the node, first we proposed a topology model that consists of heterogenous networks shown in Figure 1.

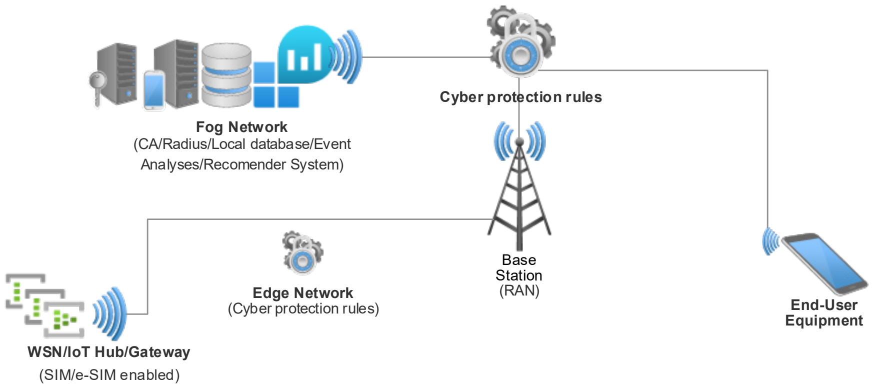

**Fig. 1.** Topology model of the proposed solution

Accordingly, to be adapted to our topology model and the aim of this study, its clustering technique must be enhanced with additional algorithms based on more properties of the network nodes. Since there is not found any adequate solution to be implemented in our model which is shown in Figure 1, we have developed the baseline methodology of a solution that fulfills the cybersecurity requirements defined by the CIA triad converging with the proposed topology model.

Our methodology is based on the K-means algorithm which is augmented with additional processing steps to fulfill the criteria of the CIA triad. Initially, K-means clustering is executed, then three more specific parameters will define the cluster members' status, respectively regarding confidentiality, integrity, and availability. This protocol will be executed at the edge or fog computing networks, respectively on a dedicated server. The summarized results provided at the end of the processes will determine the most trusted cluster member within the cluster. This cluster member will be recommended to serve as a node for placing securely the wanted service. Bellowed are the defined steps to accomplish this process:

**Step 1.** Initiate the network such as node location as the default K-mean parameters. If a node is not supplied constantly with energy, take the initial node energy.

**Step 2.** Apply the K-means approach through which the cluster head will be selected according to the initial network parameters to establish the communication by using the formula:

$$D_L = d\ (x_i,\ x_c)^2 \tag{2}$$

or with initial node energy:

$$D_{LE} = e/d\ (x_i,\ x_c)^2 \tag{3}$$

where d is the distance, and e is the energy.

**Step 3.** Gather the parameters of each cluster node that relate to confidentiality (i.e., identity management and or others), integrity (i.e., data encryption and or others), and availability (i.e., resource utilization and or others). The related parameters are summarized according to each CIA component and bring the respective weight for each of them.

**Step 4.** Evaluate nodes by highest weight to generate a trusted value per each of them. After computing the parameters, a threshold is applied to define the eligibility of node selection to be recommended.

**Step 5.** Recommend the most trusted node based on the selection function formula:

$$R_L(f) = w_1 * d + (w_2 + w_3 + w_4) * trusted\ value \tag{4}$$

or:

$$R_{LE}(f) = w_1 * (e/d) + (w_2 + w_3 + w_4) * trusted\ value \tag{5}$$

where $w_1$, $w_2$, $w_3$, and $w_4$ have their weight values which are between 0 and 1. Wherefore, the sum of $w_1$, $w_2$, $w_3$ and $w_4$ should not exceed the value 4.

$$(w_1 + w_2 + w_3 + w_4) \leq 4 \tag{6}$$

where $w_1$ and the *trusted value* might be optional thresholds of the vendor, respectively might be an optional threshold of service commitments for QoS/QoE according to SLA with the service provider.

**Step 6.** Decide for accepting the recommended node and initiate service placement or cluster head selection.

**Step 7.** Perform encrypted data transmission according to chosen cryptography technique.

**Step 8.** Keep monitoring, if parameters change to perform a new gathering of node's parameters, if not stop the process, and continue the service.

## 5 Setup and results of the experiment

To initiate the simulated experiment, first, we built the layout of the node's network which represents the edge or fog devices. We considered an optimal network that would be according to our problem statement and sufficiently to the aim of this study, using MATLAB as a programming and numeric computing platform [47]. This network consists of 50 wireless nodes, randomly distributed within a space of 10 square kilometers, whose parameters are presented in Table 1.

**Table 1.** Network parameters

| Number of nodes | Network length | Network width | Nodes alignments |
|---|---|---|---|
| 50 | 10 km | 10 km | Randomly |

Since we want the nodes of the network to be part of a wireless mesh topology of the communication network which is randomly distributed throughout the environment, we developed the first algorithm that is used to represent their layout, as follows:

```
Algorithm 1: Node alignments
Require the inputs:
Number of nodes__
Networks length__
Network width__
  for i=1 to the number of nodes do
    initialize coordinates of x(i) and y(i) by random values
    plot the nodes in the location
    text the nodes accordingly
  end
write locations to the dataset file
```

This algorithm requires the network environment parameters that are the first data of our dataset defined in Table 1. Execution of the algorithm provided us with the figure of node alignments within the network perimeter, as well as the dataset file which we used for further work. Figure 2 shows the nodes' alignment and the properties of the network.

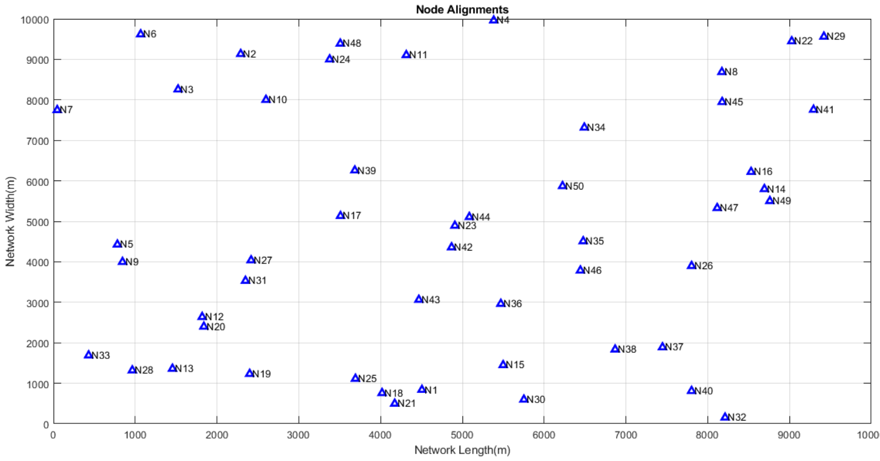

**Fig. 2.** Node alignments

Next, we used the generated file as a dataset with the node's location to do clustering with K-means. To achieve this, we build the following algorithm running the pseudo-code of K-means:

```
Algorithm 2: K-means clustering and Centroid selection
Require:
Load the dataset file from Algorithm 1
Read distance values from KmeansFunction()
  for i=1 to 5 do
```

```
      build a numeric matrix and assign it to input as-
signments (X)
      k-mean clustering of nodes into one cluster
      calculate cluster center location
    end
  plot the nodes in their clustered location
  plot the centroid of the cluster
```

The second algorithm first loads the dataset that is built by the first algorithm and then applies the K-mean function. This gives us the clustered nodes and defines the position of the centroid, respectively the cluster head, according to the K-means default algorithm which is expressed by equation (1). Then this is plotted as shown in Figure 3 which shows the output of the second algorithm.

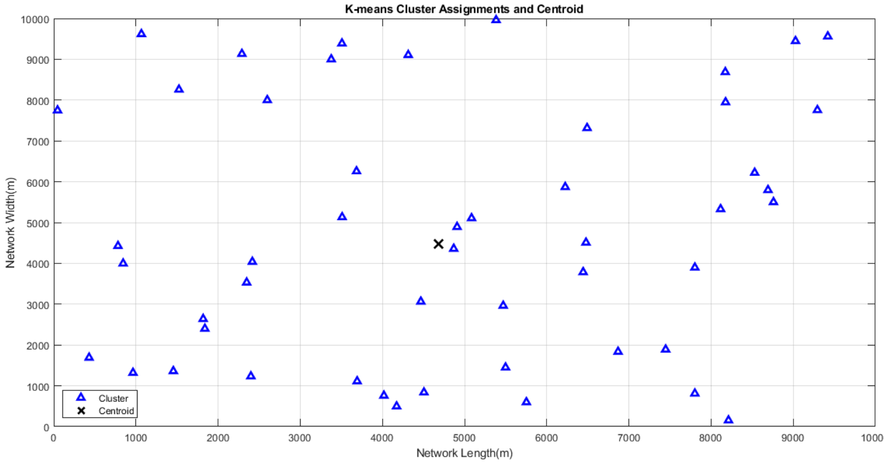

**Fig. 3.** K-means clustering and cluster head (centroid) selection

Then in the third algorithm, we added the parameters of confidentiality, integrity, and availability. Since we do not have the real parameters, we added random values according to our commitment in Section 4 of our proposed methodology, based on the given equitation (6), where we skipped the optional values.

```
  Algorithm 3: Random values
  Require: Results of Algorithm 2
  for i=1 to the number of weight calculations of CIA pa-
rameters do
    random values for confidentiality from 0 to 1
    random values for integrity from 0 to 1
    random values for availability from 0 to 1
    calculate the total sum of values per row
  end
```

```
find the coordinates of the node with the highest value
show the recommended node for service placement
plot the cluster with all information
```

The third algorithm first requires the results of the second algorithm, then it gives the random cybersecurity values at each node and finds the coordinates of the preferred node for recommended service placement. In the end, the algorithm plots the results. Figure 4 shows the results of our simulated experiment, where are presented the nodes, their centroid node, and the recommended node to be chosen for service placement based on CIA parameters.

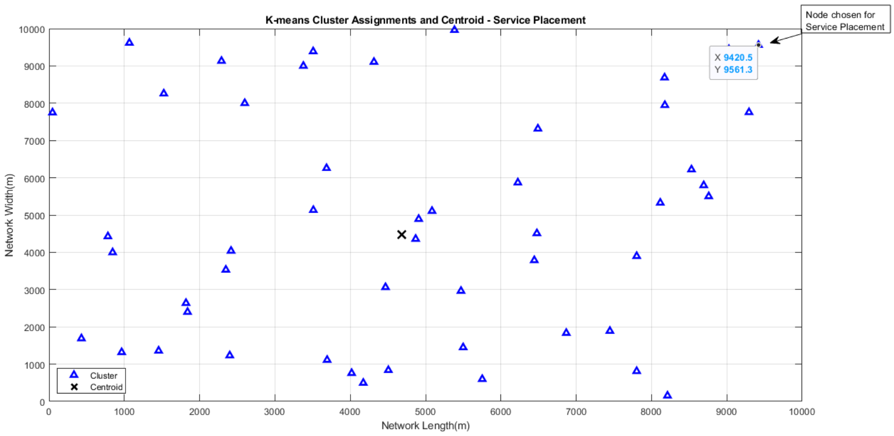

**Fig. 4.** Summarized results of the experiment

As it seems in Figure 4 the recommended node is different from the centroid, which means that the most trusted node for placing a service by taking into consideration parameters of the CIA triad would be deployed at different locations, respectively cluster members.

## 6 Conclusions and future work

Confidentiality, integrity, and availability, known as the CIA triad, have been used as a framework for information technology by excluding the sensor networks due to their computational limitation. According to this, we have developed a baseline methodology of a solution that shows how to fulfill the cybersecurity requirements in the clustering algorithm, converging with the proposed model that integrates WSNs, edge, fog, and cloud computing. Our methodology is based on the K-means algorithm which is enhanced with additional processing steps to provide the criteria of the CIA triad. The study uses the CIA triad as metrics considering a distributed design with dynamic systems that supports mobility and satisfies the private cloud deployment, which allows different case scenario deployments that use the wireless mesh topology of the communication network.

To accomplish this, initially, we referred to our ongoing research which is based on published results of a systematic literature review [2]. Then, we continued with findings on related works which supported us to formulate the problem statement regarding placing a service considering the cybersecurity manner. This led us to the baseline methodology of a solution that fulfills the cybersecurity requirements defined by the CIA triad converging with the proposed model. To achieve this, we proposed the solution by using the K-means algorithm which is enhanced with additional processing steps to provide the criteria of the CIA triad. Results provided by our basic experiment, conducted using MATLAB, show that our proposal stands and that further studies based on this approach have enough arguments to be researched.

In this paper, which is the first try to include CIA parameters in a clustering algorithm, we treated the problem in a general manner by doing the simulated experiment taking random values. These values need to be more deeply analyzed to find specific values which present the weight of CIA triad components on placing a network service according to a secure recommender system, respectively its algorithm. Consequently, the continuity of future research needs to treat this proposed solution. Since we considered, based on our survey in Section 2, that availability is more treated by respective authors in their studies about wireless communication and heterogeneous networks, our future work will be focused on confidentiality and integrity as a cybersecurity need for such technologies.

## 7 References

[1] Kim, K.-I., Yang, S., & Lee, E. (2021). "Communications and Networking for Mobile Sink in Wireless Sensor Networks." *Wireless Communications and Mobile Computing*, 2021, 1–2. https://doi.org/10.1155/2021/9845850

[2] Gashi, L., Luma, A., & Januzaj, Y. (2022). *The integration of Wireless Sensor Networks, Mobile Networks, and Cloud Engineering for a decision support system—A Systematic Literature Review*. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 1–8. https://doi.org/10.1109/HORA55278.2022.9799924

[3] Pearson, S., & Benameur, A. (2010). *Privacy, Security and Trust Issues Arising from Cloud Computing*. 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 693–702. https://doi.org/10.1109/CloudCom.2010.66

[4] Jansen, W., & Grance, T. (n.d.). *Guidelines on Security and Privacy in Public Cloud Computing*. 80. (NIST SP 800-144; 0 ed., p. NIST SP 800-144). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-144

[5] Cloud Standards Customer Council. *Security for Cloud Computing: 10 Steps to Ensure Success* (2016), [Online]. Available: http://www.cloud-council.org/deliverables/security-for-cloud-computing-10-steps-to-ensure-success.htm [Accessed: Jun. 9, 2022].

[6] Cloud Security Compliance Consultancy. (n.d.). [Online]. Available: https://itgovernance.co.uk/cloud-security-compliance [Accessed: Jun. 9, 2022].

[7] Cloud Security Alliance. *Security Guidance for Critical Areas* (2017). [Online]. Available: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ [Accessed: Jun. 21, 2022].

[8] De Donno, M., Tange, K., & Dragoni, N. (2019). "Foundations and Evolution of Modern Computing Paradigms:" *Cloud, IoT, Edge, and Fog*. IEEE Access, 7, 150936–150948. https://doi.org/10.1109/ACCESS.2019.2947652

[9] Apat, H. K., Sahoo, B., & Maiti, P. (2018). *Service Placement in Fog Computing Environment.* 2018 International Conference on Information Technology (ICIT), 272–277. https://doi.org/10.1109/ICIT.2018.00062

[10] Salaht, F. A., Desprez, F., & Lebre, A. (2021). *An Overview of Service Placement Problem in Fog and Edge Computing*. ACM Computing Surveys, 53(3), 1–35. https://doi.org/10.1145/3391196

[11] Souza, V. B. C., Ramirez, W., Masip-Bruin, X., Marin-Tordera, E., Ren, G., & Tashakor, G. (2016). *Handling service allocation in combined Fog-cloud scenarios*. 2016 IEEE International Conference on Communications (ICC), 1–5. https://doi.org/10.1109/ICC.2016.7511465

[12] Singh, A., Auluck, N., Rana, O., Jones, A., & Nepal, S. (2017). *RT-SANE: Real Time Security Aware Scheduling on the Network Edge*. Proceedings of the The10th International Conference on Utility and Cloud Computing, 131–140. https://doi.org/10.1145/3147213.3147216

[13] Skarlat, O., Schulte, S., Borkowski, M., & Leitner, P. (2016). *Resource Provisioning for IoT Services in the Fog*. 2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA), 32–39. https://doi.org/10.1109/SOCA.2016.10

[14] Faticanti, F., De Pellegrini, F., Siracusa, D., Santoro, D., & Cretti, S. (2019). *Cutting Throughput with the Edge: App-Aware Placement in Fog Computing*. 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 196–203. https://doi.org/10.1109/CSCloud/EdgeCom.2019.00026

[15] Lee, G., Saad, W., & Bennis, M. (2017). *An online secretary framework for fog network formation with minimal latency*. 2017 IEEE International Conference on Communications (ICC), 1–6. https://doi.org/10.1109/ICC.2017.7996574

[16] Lee, G., Saad, W., & Bennis, M. (2019). *An Online Optimization Framework for Distributed Fog Network Formation With Minimal Latency*. IEEE Transactions on Wireless Communications, 18(4), 2244–2258. https://doi.org/10.1109/TWC.2019.2901850

[17] Yousefpour, A., Ishigaki, G., Gour, R., & Jue, J. P. (2018). *On Reducing IoT Service Delay via Fog Offloading.* IEEE Internet of Things Journal, 5(2), 998–1010. https://doi.org/10.1109/JIOT.2017.2788802

[18] Alsaffar, A. A., Pham, H. P., Hong, C.-S., Huh, E.-N., & Aazam, M. (2016). *An Architecture of IoT Service Delegation and Resource Allocation Based on Collaboration between Fog and Cloud Computing*. Mobile Information Systems, 2016, 1–15. https://doi.org/10.1155/2016/6123234

[19] Skarlat, O., Nardelli, M., Schulte, S., & Dustdar, S. (2017). *Towards QoS-Aware Fog Service Placement.* 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), 89–96. https://doi.org/10.1109/ICFEC.2017.12

[20] Shurman, M. M., & Aljarah, M. K. (2017). *Collaborative execution of distributed mobile and IoT applications running at the edge*. 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), 1–5. https://doi.org/10.1109/ICECTA.2017.8252057

[21] Aral, A., & Ovatman, T. (2018). *A Decentralized Replica Placement Algorithm for Edge Computing*. IEEE Transactions on Network and Service Management, 15(2), 516–529. https://doi.org/10.1109/TNSM.2017.2788945

[22] Malazi, H. T., & Clarke, S. (2021). *Distributed Service Placement and Workload Orchestration in a Multi-access Edge Computing Environment*. 2021 IEEE International Conference on Services Computing (SCC), 241–251. https://doi.org/10.1109/SCC53864.2021.00037

[23] Paul Martin, J., Kandasamy, A., & Chandrasekaran, K. (2020). "CREW: Cost and Reliability aware Eagle-Whale optimizer for service placement in Fog." *Software: Practice and Experience*, 50(12), 2337–2360. https://doi.org/10.1002/spe.2896

[24] Hong, K., Lillethun, D., Ramachandran, U., Ottenwälder, B., & Koldehofe, B. (2013). *Mobile fog: A programming model for large-scale applications on the internet of things*. Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing - MCC '13, 15. https://doi.org/10.1145/2491266.2491270

[25] Wang, P., Liu, S., Ye, F., & Chen, X. (2018). *A Fog-based Architecture and Programming Model for IoT Applications in the Smart Grid* (arXiv:1804.01239). arXiv. https://doi.org/10.48550/arXiv.1804.01239

[26] Su, L., Wang, N., Zhou, R., & Li, Z. (2021). *Online Service Placement and Request Scheduling in MEC Networks* (arXiv:2108.11633). arXiv. http://arxiv.org/abs/2108.11633

[27] Wang, Y., Li, Y., Lan, T., & Choi, N. (2019). *A Reinforcement Learning Approach for Online Service Tree Placement in Edge Computing*. 2019 IEEE 27th International Conference on Network Protocols (ICNP), 1–6. https://doi.org/10.1109/ICNP.2019.8888150

[28] Ouyang, T., Zhou, Z., & Chen, X. (2018). *Follow Me at the Edge: Mobility-Aware Dynamic Service Placement for Mobile Edge Computing*. IEEE Journal on Selected Areas in Communications, 36(10), 2333–2345. https://doi.org/10.1109/JSAC.2018.2869954

[29] Ning, Z., Dong, P., Wang, X., Wang, S., Hu, X., Guo, S., Qiu, T., Hu, B., & Kwok, R. Y. K. (2021). *Distributed and Dynamic Service Placement in Pervasive Edge Computing Networks*. IEEE Transactions on Parallel and Distributed Systems, 32(6), 1277–1292. https://doi.org/10.1109/TPDS.2020.3046000

[30] Dahmen-Lhuissier, S. (n.d.). *Multi-access Edge Computing starts the second phase and renews the leadership team*. ETSI. [Online].
Available: https://www.etsi.org/newsroom/news/1180-2017-03-news-etsi-multi-access-edge-computing-starts-second-phase-and-renews-leadership-team [Accessed: Jul. 31, 2022].

[31] Selimi, M., Cerdà-Alabern, L., Freitag, F., Veiga, L., Sathiaseelan, A., & Crowcroft, J. (2019). *A Lightweight Service Placement Approach for Community Network Micro-Clouds.* Journal of Grid Computing, 17(1), 169–189. https://doi.org/10.1007/s10723-018-9437-3

[32] Lloyd, S. (1982). Least squares quantization in PCM. IEEE Transactions on Information Theory, 28(2), 129–137. https://doi.org/10.1109/TIT.1982.1056489

[33] MacQueen, J., 1967, June. Classification and analysis of multivariate observations. In *5th Berkeley Symp. Math. Statist. Probability* (pp. 281-297). Los Angeles LA USA: University of California.

[34] Forgy, E.W., 1965. Cluster analysis of multivariate data: Efficiency vs. interpretability of classifications. *biometrics*, 21, pp.768-769.

[35] Benmahdi, M. B., & Lehsaini, M. (2020). *A GA-based Multihop Routing Scheme using K-Means Clustering Approach for Wireless Sensor Networks*. 2020 Second International Conference on Embedded & Distributed Systems (EDiS), 155–160. https://doi.org/10.1109/EDiS49545.2020.9296444

[36] Kodinariya, T.M. and Makwana, P.R., 2013. Review on determining number of Cluster in K-Means Clustering. *International Journal*, 1(6), pp.90-95.

[37] Hassan, A. A., Md Shah, W., Iskandar Othman, M. F., & Hussien Hassan, H. A. (2020). *Evaluate the performance of K-Means and the fuzzy C-Means algorithms to form balanced*

*clusters in wireless sensor networks*. International Journal of Electrical and Computer Engineering (IJECE), 10(2), 1515. https://doi.org/10.11591/ijece.v10i2.pp1515-1523

[38] S.V., M., & T, P. (2019). *An Efficient Cluster Head Selection and Routing in Mobile WSN*. International Journal of Interactive Mobile Technologies (IJIM), 13(10), 56. https://doi.org/10.3991/ijim.v13i10.11303

[39] Fethellah, N. E. H., Bouziane, H., & Chouarfia, A. (2019). *New Efficient Caching Strategy based on Clustering in Named Data Networking*. International Journal of Interactive Mobile Technologies (IJIM), 13(12), 104. https://doi.org/10.3991/ijim.v13i12.11403

[40] Fang, J. (2019). *Clustering and Path Planning for Wireless Sensor Networks Based on Improved Ant Colony Algorithm*. International Journal of Online and Biomedical Engineering (IJOE), 15(01), 129. https://doi.org/10.3991/ijoe.v15i01.9784

[41] Echoukairi, H., Idrissi, A., & Omary, F. (2022). *New Hierarchical Routing Protocol Based on K-Means Clustering with Exploiting Free Time Slot for Wireless Sensor Networks*. International Journal of Interactive Mobile Technologies (IJIM), 16(08), 165–181. https://doi.org/10.3991/ijim.v16i08.29863

[42] ISACA. “Advancing IT, Audit, Governance, Risk, Privacy & Cybersecurity.” (n.d.). [Online]. Available: https://www.isaca.org/ [Accessed: Aug. 6, 2022].

[43] NIST. “SP 1800-25 documentation.” (n.d.). [Online]. Available: https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html [Accessed: Aug. 12, 2022].

[44] ISO/IEC 27001:2013(en). “Information technology, Security techniques, Information security management systems Requirements.” (n.d.). [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en [Accessed: Aug. 12, 2022].

[45] Agency (IAEA), I. A. E. (n.d.). Official Web Site of the IAEA [Text]. International Atomic Energy Agency (IAEA). [Online]. Available: https://www.iaea.org [Accessed: Aug. 12, 2022].

[46] IEC. “Standards development” (n.d.). [Online]. Available: https://iec.ch/standards-development [Accessed: Aug. 17, 2022].

[47] MATLAB - MathWorks. (n.d.). [Online]. Available: https://ch.mathworks.com/products/matlab.html [Accessed: Jun. 12, 2022].

## 8 Authors

**Luan Gashi** has graduated in Faculty of Computer Science and Engineering in UBT College in Prishtina. He is a Senior Computer Networks and Systems Engineer, currently working as Cybersecurity Officer at energy sector and Senior University Lecturer. He is doing doctoral studies (candidate) in Computer Science at South-East European University in Tetovo. Area of research is focused on Cyber/ICT Protection at Critical Infrastructures (email: lg29758@seeu.edu.mk).

**Artan Luma** has graduated in Faculty of Contemporary Sciences in University of Tetova in Tetovo. He holds a PhD diploma in Computer Sciences from 2010. He is Full Professor in South East European University. His scientific research is cryptography and cyber security (email: a.luma@seeu.edu.mk).

**Halil Snopçe** Associate Professor of computer science and applied mathematics in South East European University in Tetovo, Republic of North Macedonia. He covers the courses of Caclulus, linear algebra, probability and statistics, discrete structure and research methodology. Area of research is in parallel processing, optimization methods, data analysis and statistics (email: h.snopce@seeu.edu.mk).

**Ylber Januzaj** is an Assistant Professor in University "Haxhi Zeka", Peja, Faculty of Business, Kosovo. He is Professor in the area of Informatics. He holds a PhD diploma on E-Technologies. His research interests areas are: Machine Learning, Computer Networks, and Database (email: ylber.januzaj@unhz.eu).

Article submitted 2022-12-11. Resubmitted 2023-03-16. Final acceptance 2023-04-03. Final version published as submitted by the authors.