International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol.10 No.1 September – October 2022

INTUITIONISTIC INTERVAL-VALUED INTERVALS THE FUZZY ANALYTIC HIERARCHY PROCESS IS USED FOR THE PURPOSE OF DETERMINING THE INFLUENCE OF VARIOUS SECURITY FEATURES

Sushama Maroti Bokde[1] & Dr.Vineeta Basotia[2]

[1]Ph.D. Research Scholar, Department of Mathematics, Shri JJTU, Rajasthan, India

[2]Professor & Research Guide, Department of Mathematics, Shri JJTU, Rajasthan, India

Corresponding Author –Sushama Maroti Bokde

DOI - 10.5281/zenodo.7890235

Abstract:

The term "Internet of Things" (IoT) refers to a network of connected, intelligent devices that are responsible for the collecting and dissemination of data. Because the technology automates the tasks we do on a daily basis, our lives have become simpler as a result. But in a typical cloud-IoT architecture, real-time data analysis is not always practicable, particularly for latency-sensitive applications. This is especially the case when there are several cloud services involved. This ultimately resulted in the development of fog computing. On the one hand, fog layer may perform computations and data processing at the very edge of the network, which enables it to provide results more quickly. On the other hand, this pushes the attack surface closer to the devices themselves, which is a security risk. Because of this, the sensitive data that is stored on the layer is now susceptible to assaults. Therefore, giving consideration to the security of the fog-IoT is of the utmost significance. A system or platform's level of security is determined by a number of different elements. When it comes to conducting an accurate risk assessment, the sequence in which these considerations are considered is of the utmost importance. Because of this, the topic of assessing the security of fog-based Internet of Things networks becomes a Multi-Criteria Decision-Making (MCDM) dilemma. As a result, the authors have developed an Analytical Hierarchy Process (AHP) that is based on an Interval-Valued Intuitionistic Fuzzy Set (IVIFS) for the aforementioned setting. The fog-iot security factors and their subfactors are prioritised and graded with the help of this integrated strategy. The findings that were achieved by utilising the hybrid strategy described above are verified by comparing them with the results obtained using the Fuzzy-AHP (F-AHP) and the Classical-AHP (C-AHP) methods, and it is discovered that these three methods have a statistically significant correlation. This study has produced an ideology as well as findings that will assist security practitioners in successfully accessing the security of a fog-based Internet of Things environment. In addition, the findings of this investigation will assist in laying the groundwork for future study by directing scientists' attention to the element that should get the highest priority, so ensuring environmental safety.

Keywords:*Fog computing IoT Fog-IoT security Interval-valued intuitionistic fuzzy AHP*

Introduction:

It would seem that fog computing is an emerging technology that enhances cloud computing by placing auxiliary processing, networking facility, and storage in close proximity to ground devices that create and absorb the generated data segments [1]. As the Internet of Things (IoT) network continues to grow and new application areas are developed, an increasingly large amount of data is being generated by the ground IoT devices that are located at the network's edge. When this happens, it is frequently not a practical option to send all of the created data to a faraway cloud data centre and expect excellent results in terms of Quality of Service (QoS). This is especially true in the realm of application fields that have requirements for low latency. In addition, in a purely cloud-based situation, all of the private and confidential data that is created by the devices is uploaded to high-end cloud servers in order to be processed. As a result, the user has very little or no control over the data associated with their account. Therefore, the existence of the evident fog in the scene may be rationalised.

The fog nodes are strategically placed at various locations between the ground device and the cloud, which is the location of all of the business logic. As a result, the fog node is able to access all of the data, whether it is in the form of the data that is sensed from the ground devices or the control data that is delivered back to the devices. In addition to this, they are in possession of information on the real source of the data. This introduces a new security flaw, since any weakness in the security of the fog layer might put the total security of the IoT system at risk due to the interconnected nature of the devices. The fact that the processing of the vast majority of the data generated by IoT devices takes place at the network edge itself [3] is evidence of the severity of the problem. In the context of the implementation of fog-based Internet of Things scenarios, security is identified as one of the primary threats. As a result, acquiring a firm grasp on it is of the biggest significance [4,5].

Security in a fog environment is made up of a number of different aspects, all of which need to be taken into consideration when thinking about the system's overall security. When taken into consideration collectively, these aspects may help to maintain the integrity of the whole system. However, determining the sequence in which they need to be treated is still another significant obstacle that must be overcome. Using a method known as Multi-Criteria Decision Making (MCDM), it is possible to find a solution to this problem. The MCDM technique is used to solve situations in which there are several potential solutions and a variety of vantage points from which to evaluate them [6]. The MCDM method to decision making takes into consideration both objective and subjective measurement data throughout the process of making decisions. In the beginning of the traditional technique, crisp values were the only ones that were employed for subjective assessment. Later on, in 1965, L. A. Zadeh presented fuzzy set theory in order to address the imprecision and uncertainty that were present in the decision-making process. [7] In addition to this, it was said that the fuzzy system was only able to cope with the membership function. This was considered to be one of its most significant weaknesses. Atanassov in 1986,1989 [8, 9] presented a novel scheme of Intuitionistic Fuzzy Set (IFS) by attaching a non-membership function to the fundamental fuzzy set. This was done in an effort to eliminate the disadvantages associated with fuzzy sets. In addition, Atanassov and Gargov (1989, 1994) [9,10] enhanced the IFS to become the Interval-Valued Intuitionistic Fuzzy Set (IVIFS) by defining an interval for both membership and non-membership functions. This was done in order to widen the IFS's application. When compared to IFS and other fuzzy systems, IVIFS produces more accurate findings and excels at describing fuzzy information [11]. The operational approach of setting goals and alternative weights is where a number of the current MCDM systems separate themselves from one another [6,12]. Among them, the Analytic Hierarchy Process (AHP) is recognised as an organised method that can be put to use in order to determine the relative importance of the various criteria and components [12].

Related Work:

In the past, a substantial amount of work has been carried out in the context of ensuring the safety of the Fog-IoT environment. Despite all of the efforts, the environment is still not safe enough to be considered acceptable. Over the course of the last several years, there has been a discernible rise in the number of breaches of security. It's possible that this is due to an expanded attack surface or a rise in the total number of IoT devices. Even while the researchers have put in a significant amount of work to address the concerns of security, there has only been a very little amount of forward movement. Defining the components of security and placing them in a precise sequence according to their importance is still another difficulty [20].

According to Gireesha et al. [9], the selection of a Cloud service provider is dependent on a wide variety of criteria, including relations between numerous qualities, alternative solutions, and industry expertise. The researchers believe that MCDM is the approach that would work best in this particular scenario. Improved Interval-Valued Intuitionistic Fuzzy Sets-Weighted Aggregate Sum and Product Assessment (IIVIFS-WASPAS) is the approach that they have presented for selecting a reliable cloud service provider. The researchers have also undertaken comparisons of their suggested method with many other methodologies and discovered that their proposed method has performed better than the other methodologies. A unique decision-making framework for Cloud Vendor Selection (CVS) has been provided by Krishankumar et al. [28], which allows for the efficient selection of cloud suppliers by addressing the difficulty of unjustified weight assignment and poor uncertainty management. The authors have aggregated the results of their preference analysis using an intuitionistic weighted geometry operator after representing the preferences using an Intuitionistic Fuzzy-Valued (IFV) model. After that, the criterion weights are generated via the use of an intuitionistic fuzzy statistical variance approach, and the Vikor methodology is used for the ranking of cloud service providers.

The preceding discussion has made it abundantly clear that there is a considerable need to address the issue of security inside a system that utilises fog computing. Because there are many different components that make up security, each of these components has to be addressed separately if there is to be any assurance that the environment will be safe. When it comes to ensuring the safety of the whole scenario, the sequence in which these individual aspects of security are addressed is also a very important one. In addition, the researchers are using MCDM strategies in order to rank the many contributing components. In light of the information supplied above, the authors have provided a hierarchy of security factors and subfactors and rated them with the assistance of a hybrid multi-criteria decision making (IVIFS-AHP) method.

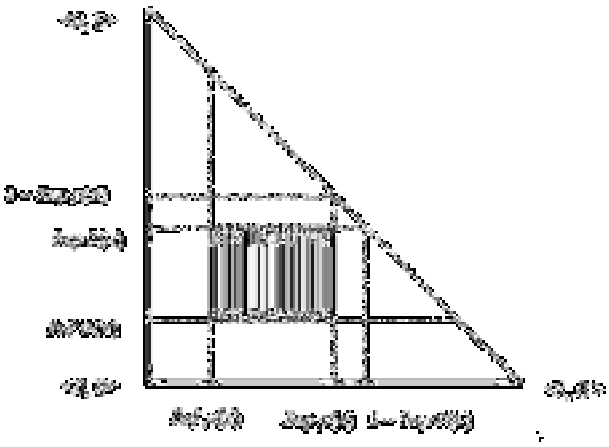

Fig. 1. Representation of Interval-valued intuitionistic fuzzy set

Fog-Internet of Things Security:

The issue of security is often regarded as the most significant barrier to overcome before widespread adoption of Internet of Things services and technology [4,31]. When opposed to traditional IT systems, the Internet of Things' integration of physical and technological elements makes the prevalence of security vulnerabilities much greater than it already was. Because of the development of Fog computing, data is now processed at locations that are geographically closer to its points of origin. The fact that it is, as described above, makes it much more vulnerable to breaches of security. Data breaches open the door to the easy disclosure of sensitive personal information about people. The security assaults may even be able to interfere with the real operation of the IoT-enabled system, which may lead to a scenario that poses a risk to users' lives. Fog computing is expected to become the most important component of the Internet of Things in the not-too-distant future [32], as stated by a scientific forecast. Inevitably, the consequence that stems from this merging is that the security component has to be designated high on the priority list in order to assure the successful deployment of this integration. This may be done by marking it as one of the highest priorities. Intrusion detection, authentication, trust management, privacy, and other related topics are among the most common concerns about this environment's security [33,34].

The fact that fog nodes are tiny data handlers that are dispersed over a broad geographical region and are difficult to safeguard physically is the most major challenge for fog computing. When taking into consideration the data that is created by the nodes as a result of this, it is necessary to check the legitimacy of the nodes [34]. The primary purpose of this contribution is to cut down on the amount of work that has to be done in order to prioritise the many aspects of security. It's possible that using a security rating in a fog-IoT environment can help you improve security at the appropriate time. The authors of this research have discovered many security variables and subfactors that are associated with the Fog-IoT environment. There are many different aspects of Fog-IoT security that are taken into consideration, such as Authentication (C1), Access Control (C2), Intrusion Detection (C3), Trust (C4), and Integrity (C5), which are to be used for the purpose of strengthening the overall security of the Fog-IoT ecosystem. Figure 2 illustrates the security factors, as well as the subfactors, which may be characterised as follows:

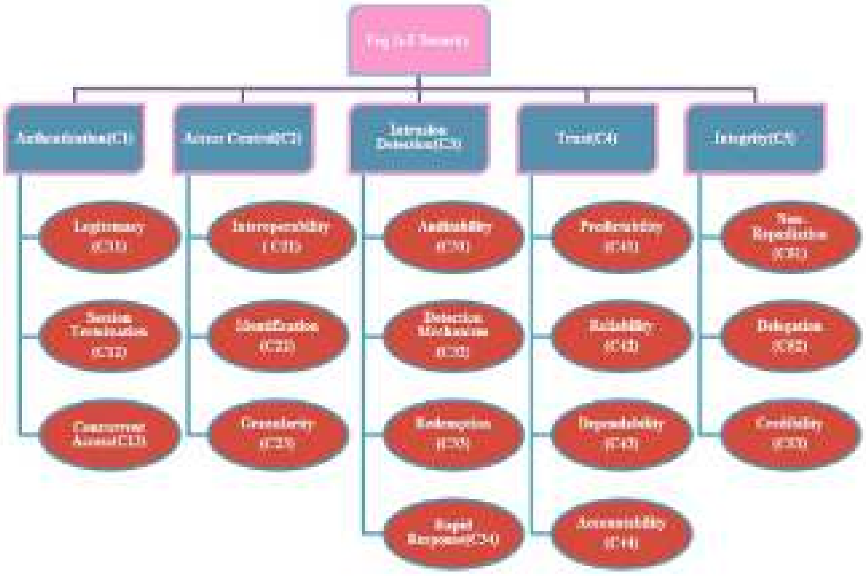

Fig. 2. Hierarchy of Fog-Internet of Things security

Authentication:

Since IoT services are provided to a large number of end users via front fog nodes [35], authentication is the most important issue that needs to be taken into consideration in order to guarantee data safety in a Fog-IoT environment. Authentication is cited as a critical concern regarding security by a number of researchers working at a variety of fog node levels [36,37]. Authentication was not given a lot of thought in the early stages of Internet of Things design, which consisted mostly of feeding data straight into cloud servers. On the other hand, the introduction of a fog layer in the centre has led to a rise in the number of fog nodes that are scattered throughout a large geographical region, which has led to an increase in the difficulty of authenticating users. The old Public Key Infrastructure cannot be used since it has lower efficiency and limited scalability [35]. Authentication may be controlled by identifying its component parts and then focusing on those parts individually.

Trust:

The decentralised system's most fundamental component is trust in its users. Because of the lack of overall system security, it is impossible to place complete faith in the individual computing nodes that make up a distributed system [33]. Therefore, a trust assessment is of the highest necessity in order to guarantee safe and effective communication. Because of the heterogeneity of the nodes, the trust mechanism that was used in the cloud scenario is unable to be immediately adapted to the Fog-IoT environment. As a result, in order to address concerns about dependability and security, an effective trust model is necessary [22].

Conclusion:

It is necessary to classify security concerns and describe their underlying driving forces in order to offer comprehensive protection for an environment in which network devices are spread out across a large geographic region and communication takes place at a steady clip. It is clear from the research that was conducted and the literature that was examined that there is no such known, thorough, and full method that provides security throughout the whole Fog-IoT situation. It is necessary to prioritise the many security criteria in order to have access to security in a comprehensive Fog-IoT environment. The hybrid technique that has been suggested provides a quantitative study of the security elements in accordance with the hierarchy that has been provided, as well as their ranking according to that analysis. The rating that is provided will be of use in determining the amount of work that is required when dealing with various aspects of security. The assertion that the evaluations of experts are taken into account when calculating the risk variables in a fog-based Internet of Things environment has been validated by statistical research.

References:

[1]. F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proc. MCC Workshop on Mobile Cloud Computing, 2012.

[2]. OpenFog Consortium, Openfog reference architecture for fog computing, 2017, https://www.openfogconsortium.org/ra/, Accessed 24 2020.

[3]. A. Weissberger, IDC directions: IoT forecast, 5G and related sessions, 2017, http://techblog.comsoc.org/2017/03/04/idc-directions-2017-iot-forecastrelated-sessions/, MarAccessed 24 2020.

[4]. M.A. Khan, K. Salah, Iot security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.

[5]. S. Ganguli, T. Friedman, IoT Technology Disruptions: A Gartner Trend Insight Report, Tech. rep., Gartner Inc., 2017, https://www.gartner.com/en/documents/ 3738060/iot-technology-disruptions-a-gartner-trend-insight-report, Accessed 24 2020.

[6]. CengizKahraman, SeziCevikOnar, BasarOztaysi, Fuzzy multicriteriadecisionmaking: a literature review, Int. J. Comput. Intell. Syst. 8 (4) (2015) 637–666.

[7]. L.A. Zadeh, Fuzzy sets, Inform. Control 8 (1965) 338–353.

[8]. K.T. Atanassov, Intuitionistic fuzzy sets, Fuzzy Sets and Systems 20 (1986) 87–96.

[9]. ObulaporamGireesha, NivethithaSomu, KannanKrithivasan, V.S. Shankar Sriram, IIVIFS-WASPAS: An integrated Multi-Criteria Decision-Making perspective for cloud service provider selection, Future Gener. Comput. Syst. 103 (2020) 91–110.

[10]. Mohamed Abdel-Basset, GunasekaranManogaran, Mai Mohamed, A neutrosophictheory based security approach for fog and mobile-edge computing, Comput. Netw. 157 (2019) 122–132.

[11]. J. Wu, F. Chiclana, Non-dominance and attitudinal prioritisation methods for intuitionistic and interval-valued intuitionistic fuzzy preference relations, Expert Syst. Appl. (2012) 13409–13416.

[12]. SerafimOpricovic, Gwo-HshiungTzeng, Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS, European J. Oper. Res. 156 (2) (2004) 445–455.

[13]. B. Liu, Why is there a need for uncertainty theory, J. Uncertain Syst. 6 (2012) 3–10.

[14]. L. Mikhailov, Deriving priorities from fuzzy pairwise comparison judgments, Fuzzy Sets and Systems 134 (3) (2003) 365–385.

[15]. HosseinSayyadiTooranloo, AsiyehIranpour, Supplier selection and evaluation using interval-valued intuitionistic fuzzy AHP

method, Int. J. Procure. Manag. 10 (5) (2017) 539–554.

[16]. Jian Wu, Hai bin Huang, Qing wei Cao, Research on AHP with interval-valued intuitionistic fuzzy sets and its application in multi-criteria decision making problems, Appl. Math. Model. 37 (24) (2013) 9898–9906.

[17]. Shengping Long, ShuaiGeng, Decision framework of photovoltaic module selection under interval-valued intuitionistic fuzzy environment, Energy Convers. Manage. 106 (2015) 1242–1250.

[18]. Omkarprasad S. Vaidya, Sushil Kumar, Analytic hierarchy process: An overview of applications, Eur. J. Oper. Res. 169 (1) (2006) 1–29.

[19]. Wen-Liang Hung, Jong-Wuu Wu, Correlation of intuitionistic fuzzy sets by centroid method, Inform. Sci. 144 (1–4) (2002) 219–225.

[20]. S. Pešić, M. Radovanović, M. Ivanović, C. Badica, M. Tošić, O. Iković, D. Bošković, CAAVI-RICS model for analyzing the security of fog computing systems, in: International Symposium on Intelligent and Distributed Computing, 2019, pp. 23-34.

[21]. Praveen Kumar, NabeelZaidi, TanupriyaChoudhury, Fog computing: Common security issues and proposed countermeasures, in: IEEE International Conference System Modeling & Advancement in Research Trends (SMART), 2016, pp. 123-129.

[22]. PeiYun Zhang, MengChu Zhou, Giancarlo Fortino, Security and trust issues in Fog computing: A survey Future Generation Computer Systems, 88, 2018, pp. 16–27.

[23]. RichaVerma, Shalini Chandra, Security and privacy issues in fog driven IoT environment, Int. J. Comput. Sci. Eng. 7 (5) (2019) 367–370.

[24]. R. Verma, S. Chandra, A systematic survey on fog steered IoT: Architecture, prevalent threats and trust models, Int. J. Wirel. Inf. Netw. (2020) 1–18.

[25]. J. Kaur, A. Agrawal, R.A. Khan, Security issues in fog environment: A systematic literature review, Int. J. Wireless Inf. Netw. 27 (2020) 467–483.

[26]. Seema Gupta Bhol, J.R. Mohanty, Prasant Kumar Pattnaik, Cyber security metrics evaluation using multi-criteria decision-making approach, Smart Intell. Comput. Appl. Springer (2020) 665–675.

[27]. Song-Man Wu, Xiao-Yue You, Hu-Chen Liu, Li-En Wang, Improving quality function deployment analysis with the cloud MULTIMOORA method, Int. Trans. Oper. Res. 27 (3) (2020) 1600–1621.

[28]. Krishankumar, K. Raghunathan, SoundarapandianRavichandran, Sanjay K. Tyagi, Solving cloud vendor selection problem using intuitionistic fuzzy decision framework, Neural Comput. Appl. 32 (2) (2020) 589–602.

[29]. K.T. Atanassov, More on intuitionistic fuzzy sets, Fuzzy Sets and Systems 33 (1989) 37–46.

[30]. K.T. Atanassov, Operators over interval-valued intuitionistic fuzzy sets, Fuzzy Sets and Systems 64 (1994) 159–174.

[31]. D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Internet of things: Vision, applications and research challenges, Ad hoc Netw. 10 (7) (2012) 1497–1516.

[32]. Microsoft IoT, Five ways edge computing will transform business, 2017, Available: https://blogs.microsoft.com/iot/2017/09/19/five-ways-edgecomputingwill-transform-business/ Accessed 29 2020.

[33]. M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M.A. Ferrag, N. Choudhury, V. Kumar, Security and privacy in fog computing: Challenges, IEEE Access 5 (2017) 138–152.

[34]. D. Puthal, S.P. Mohanty, S.A. Bhavake, G. Morgan, R. Ranjan, Fog computing security challenges and future directions [energy and security], IEEE Consum. Electron. Mag. 8 (3) (2019) 92–96.

[35]. ProsantaGope, Ashok Kumar Das, Neeraj Kumar, Yongqiang Cheng, Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks, IEEE Trans. Ind. Inform. 15 (9) (2019) 4957–4968.

[36]. Pengfei Hu, SahraouiDhelim, HuanshengNing, Tie Qiu, Survey on fog computing: architecture, key technologies, applications and open issues, J. Netw. Comput. Appl. 98 (2017) 27–42.

[37]. I. Stojmenovic, S. Wen, The fog computing paradigm: Scenarios and security issues, in: FedCSIS, IEEE, 2014.