RESEARCH ARTICLE OPEN ACCESS

SQL and Data Inference Injection and Enhancing Website Security

Dr. A. Poomari
Lecturer In Ayya Nadar Janaki Ammal Polytechnic College-Sivakasi

ABSTRACT
Web applications are utilized on an extensive scale worldwide, which handles sensitive individual information of users. Structured Query Language (SQL) Data Inference (DI) and injection is a procedure that abuses a security defenselessness occurring in the database layer of an application. In this paper we will research the website page database security help of optimization and encryption method. At long last, the attack will be detected dependent on the user query with the assistance of query tree Mechanism. For enhancing the security level of attack detection and prevention. Fully Homomorphic Encryption (FHE) encryption is proposed.
Keywords: Webpage database, Injection, prevention, optimization, attack and security.

I. INTRODUCTION

In recent times, web application is widely utilized in different kind of organization, business or commerce field because of its reliable and efficient solution to the various challenges of communication over the internet [1-10]. Similar to some evolving structures gained high interest databases [11-15] and thus malicious users who want to exploit their weaknesses and imperfections for their personal goals [16-25]. The security of databases isn't unimportant is as yet a developing concern considering the number of occurrences reported constantly [26-30]. The attack marks at injection focuses will contain examples of SQL tokens and images as SQLIA positive while substantial web requests would appear as expected information from the application [31-39]. SQL injection alludes to that the attacker works the database by embeddings a progression of SQL statements in the query task [40]. Likewise, there are different assets on the web that discloses point by point methodology to ordinary users on the best way to attack web applications with various sorts of attacks all in all and with SQL injection specifically [41].

In order to overcome the SQL injections, the traditional SQL injections are easily detected with lot of procedures and methodologies [42]. By utilizing different Database Management Systems (DBMS) [43-50], the developed organizations have the level of assurance and security for the cloud storage data [51]. For the purpose of securing data and preventing unauthorized access from unprivileged entities, DBMS is engaged with access control [52-60].

II. LITERATURE REVIEW

The detection process of SQL injection attacks is a one of the challenging tasks in cloud database security because of its extreme heterogeneity of the attack vectors. One of the novel approaches to deal with SQL injection attack detection as graph of tokens and the centrality measures is trained by Support Vector Machine (SVM) [61] Though we center fundamentally around web applications created with PHP and MySQL, the methodology can be effortlessly ported to different stages. A Gap-Weighted String Subsequence Kernel technique is actualized to recognize subsequences of shared characters between query strings for the yield of a similarity metric by Paul R. McWhirter et al, [62]. At last, SVM algorithm is trained on the basis of similarity measure (between known and unknown query strings which are utilized to classification). By social occasion all component information from the query strings, extra data from the source application isn't required. An effective SQL injection attack forces a genuine risk to the database, web application, and the whole web server and this attack is extremely normal attack that controls the information going through web application to the database servers through web servers so that it changes or uncovers database substance.

III. PROBLEM STATEMENT OF CURRENT STRATEGY

The attempt of SQL injection and DI attack is unbeaten only when an infused with web server database. In existing literary works numerous administrations are infused to secure the webpage, this is driven by the way that new types of SQL

injection attacks often do not qualify as completely new, yet minor and imaginative varieties of already observed attack vectors. In the existing filtering model removing the special characters, operators, brackets and the final solution this is to standardize SQL questions totally into a text form that is reasonable for applying document similarity measure calculation. Additionally, for security different encryption procedure like AES, DES, RSA, and ECC are utilized. The security parameters have not been instated and the attacker can access the sensitive content without checking the personality of the user. In this way, the attacker misuses this defenselessness to infuse SQL injection model.

IV. INNOVATIVE DATABASE SECURITY MECHANISM

Databases turned out to be highly robust and refined structures during multiple decades of evolvement. Databases like all other developing structures gained. Secure database in Cloud inject multi-attacks in webservers, our work query attack and DI attack are utilized by using the optimization technique. The database server side being related with a distributed cloud environment to give a security controlling system for guaranteeing the secure execution of all requested queries without any database hacking. Webserver security model generate the dummy SQL query to the database server, this generation is done by the presented DBCO technique. After embeddings, the SQL and DI in web data the proxy filtering method is to remove the unwanted server information to secure the web server database. This filtering technique is to recognize the special form like, characters, ID, and so on, Finally the admin will detect the query from the database belongs to the query user help of query tree Mechanism. For enhancing the security, we utilizing FHE algorithm to encrypted and decrypted identified query. Its helps queries to get compared from the original one using similarity measure stored over the security tool that filters out the malicious queries.

4.1 Database Interferences Problem

Sorting database inference to a group of data security attacks is very hard, because of the way that it leverages the human personality and a logic approach in order to derive secure data. Inference occurs when a malicious user infers some ensured or private data without directly accessing it. Database security depends on availability, integrity, and confidentiality, whereby availability deals with the avoidance of hardware and software. Information whenever needed, integrity with the assurance from unauthorized data access and illegal change; and confidentiality with the insurance of unauthorized data to webpage database security.

4.2 Query Preprocessing

For query preprocessing the front-end restricts inquiries to aggregate results only. Each item being chosen is checked to guarantee that just a supported aggregate function is used for each. Additionally, a count is added for each of the chosen items to assist with later analysis. From this preprocessing system to avoid non-valuable queries are neglected to the webpage data security model. Moreover, by decreasing the number of on operations, the performance of query processing can be greatly improved. When the data had been accessed by a lot of unknown people, the chances of the data threats is increases. Furthermore, the database attacks are to make a lot of money by offering sensitive information in illegal ways.

4.3 Proxy Server and Filtering

In view of optimal quires, filtering model is considered to evacuating the uncommon characters utilizing proxy filtering model and it's transferred in the server. This server can likewise be utilized to expand security for a business. A [27] server can give network address interpretation, which makes the individual users and PCs on the system mysterious when they are utilizing the Internet. Attack the ordinary strings and characters are changed over into hexadecimal, ASCII and Unicode.

As a result of this, the input inquiry is gotten away from the channel which checks the question for some awful character which results. This filtering to captures web demands at a proxy for ideal SQL and DI detection and counteractive action appears in figure 3. It's having the upside of having the capacity to decode obfuscated internet traffic for careful investigation.

Homomorphic Encryption

The completely homomorphic encryption is performed on the multiple nodes to diminish the processing time. This FHE [30] is a kind of encryption that enables specific calculations to be led on cipher query and restore an encoded outcome, the decoded of the result is equivalent the aftereffect of directing the activity on the plain query. This webpage security the ideal questions re-infused to

enhance the security included four processes which are {Key Initialization, encryption, decryption, and analysis}.

Key Initialization: Initialize encryption key is secret and consists of the set of the relatively prime moduli and two sets of vectors and optimal queries with the corresponding database.
Encryption: An Encryption algorithm is currently functional to the secret data of the first data. In the encryption process review, the ideal public key has to encode each byte of cipher query.
Decryption: This process that uses the secret key and the cipher query returns the original information in a web database. From this process evaluation of a permitted circuit yields the correct result.

V. RESULTS AND ANALYSIS

Our proposed SQL and DI attack injection webpage database security model is implemented in the platform of Net beans and JAVA language along with the cloud sim, here cloudsim act as the web server. The proposed innovative approach is executed and its performance measures are analyzed and compared with other security algorithms.

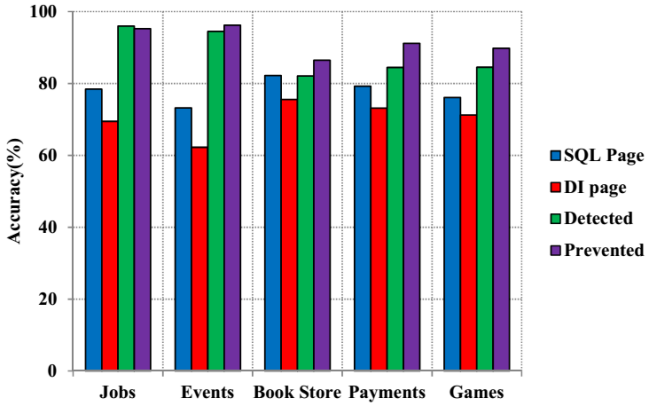

Fig 1: Detection Accuracy Vs Web application

The detection accuracy of different web applications such as jobs, events, book store, payments, and games are analyzed in figure 1. For each web application, the accuracy of SQL page, DI page, detection, and prevention are examined and compared. Considering job application, the SQL page is 79%, DI page is 70%, query detected is in the range of 97.23% and prevented is 96.89%. Similarly, the parameters are analyzed for other applications like events, book store, payments, and games. The graph concludes that the prevention rate is high in the events web application compared to other.

VI. CONCLUSION

The method is working over the database server side being related with a dispersed cloud condition to give a security controlling framework. FHE utilized to analyzed the security level of our work. SQL and DI injection is a common technique hacker utilize to assault general databases. The attack modifies the SQL queries and behavior of the framework for the advantages of behavior. From this proposed technique analyzed all generated optimal SQL and DI queries related with user input and catches the first structure of the query statement. From the implementation results, its produce 93.56% of security level of prevented webpage applicated based databases.

REFERENCE

[1] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, Dac Nhuong Le, Smart Surveillance Robot for the Real Time Monitoring and Control System in Environment and Industrial Applications, Advances in Intelligent System and Computing, pp 229-243, Springer

[2] Ezhilarasu, P., & Krishnaraj, N. (2015). Applications of Finite Automata in Lexical Analysis and as a Ticket Vending Machine–A Review. Int. J. Comput. Sci. Eng. Technol, 6(05), 267-270.

[3] Agrawal, U., Arora, J., Singh, R., Gupta, D., Khanna, A., & Khamparia, A. (2020). Hybrid Wolf-Bat Algorithm for Optimization of Connection Weights in Multi-layer Perceptron. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 16(1s), 1-20.

[4] Prasanna, S., & Ezhilmaran, D. (2016). Association rule mining using enhanced apriori with modified GA for stock prediction. International Journal of Data Mining, Modelling and Management, 8(2), 195-207.

[5] Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. IEEE Access, 8, 107112-107123.

[6] Shankar, K., Zhang, Y., Liu, Y., Wu, L., & Chen, C. H. (2020). Hyperparameter tuning deep learning for diabetic retinopathy fundus image classification. IEEE Access, 8, 118164-118173.

[7] Joshi, G. P., Perumal, E., Shankar, K., Tariq, U., Ahmad, T., & Ibrahim, A. (2020). Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. Electronics, 9(9), 1358.

[8] Saračević, M. H., Adamović, S. Z., Miškovic, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., & Shankar, K. (2020). Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures. IEEE Transactions on Reliability.

[9] Namasudra, S., & Roy, P. (2017). Time saving protocol for data accessing in cloud computing. IET Communications, 11(10), 1558-1565.

[10] Elsir, A., Elsier, O., Abdurrahman, A., & Mubarakali, A. (2019). Privacy Preservation in Big Data with Data Scalability and Efficiency Using Efficient and Secure Data Balanced Scheduling Algorithm.

[11] Ezhilarasu, P., Krishnaraj, N., & Babu, S. V. (2015). Applications of finite automata in text search-a review. International Journal of Science, Engineering and Computer Technology, 5(5), 116.

[12] Huyen, D.T.T., Binh, N.T., Tuan, T.M., Nguyen, G.N, Dey, N., Son, L.H, Analyzing trends in hospital-cost payments of patients using ARIMA and GIS: Case study at the Hanoi Medical University Hospital, Vietnam, Journal of Medical Imaging and Health Informatics, 7(2), pp. 421-429.

[13] Prasanna, S., & Maran, E. (2015). Stock Market Prediction Using Clustering with Meta-Heuristic Approaches. Gazi University Journal of Science, 28(3).

[14] Pustokhina, I. V., Pustokhin, D. A., Rodrigues, J. J., Gupta, D., Khanna, A., Shankar, K., ... & Joshi, G. P. (2020). Automatic Vehicle License Plate Recognition using Optimal K-Means with Convolutional Neural Network for Intelligent Transportation Systems. IEEE Access.

[15] Namasudra, S. (2018). Cloud computing: A new era. Journal of Fundamental and Applied Sciences, 10(2).

[16] Uthayakumar, J., Elhoseny, M., & Shankar, K. (2020). Highly Reliable and Low-Complexity Image Compression Scheme Using Neighborhood Correlation Sequence Algorithm in WSN. IEEE Transactions on Reliability.

[17] Deepalakshmi, P., & Shankar, K. (2020). Role and Impacts of Ant Colony Optimization in Job Shop Scheduling Problems: A Detailed Analysis. Evolutionary Computation in Scheduling, 11-35.

[18] Ashwin, M., Kamalraj, S., & Azath, M. (2019). Multi objective trust optimization for efficient communication in wireless M learning applications. Cluster Computing, 22(5), 10687-10695.

[19] Ezhilarasu, P., & Krishnaraj, N. (2015). Double Substring based Classification for Nondeterministic Finite Automata. Indian Journal Of Science And Technology, 8, 26.

[20] Amira S. Ashour, Samsad Beagum, Nilanjan Dey, Ahmed S. Ashour, Dimitra Sifaki Pistolla, Gia Nhu Nguyen, Dac-Nhuong Le, Fuqian Shi (2018), Light Microscopy Image De-noising using Optimized LPA-ICI Filter, Neural Computing and Applications, Vol.29(12), pp 1517–1533, Springer, ISSN: 0941-0643.

[21] Prasanna, S., Govinda, K., & Kumaran, U. S. (2012). An Evaluation study of Oral Cancer Detection using Data Mining Classification Techniques. International Journal of Advanced Research in Computer Science, 3(1).

[22] Sankhwar, S., Gupta, D., Ramya, K. C., Rani, S. S., Shankar, K., & Lakshmanaprabu, S. K. (2020). Improved grey wolf optimization-based feature subset selection with fuzzy neural classifier for financial crisis prediction. Soft Computing, 24(1), 101-110.

[23] Namasudra, S., & Deka, G. C. (2018). Introduction of DNA computing in cryptography. In Advances of DNA computing in cryptography (pp. 1-18). Chapman and Hall/CRC.

[24] Mubarakali, A., Srinivasan, K., Mukhalid, R., Jaganathan, S. C., & Marina, N. (2020). Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems. Computational Intelligence.

[25] Le Nguyen Bao, Dac-Nhuong Le, Gia Nhu Nguyen, Vikrant Bhateja, Suresh Chandra Satapathy (2017), Optimizing Feature Selection in Video-based Recognition using Max-Min Ant System for the Online Video

Contextual Advertisement User-Oriented System, Journal of Computational Science, Elsevier ISSN: 1877-7503. Vol.21, pp.361-370.

[26] Ezhilarasu, P., Thirunavukkarasu, E., Karuppusami, G., & Krishnaraj, N. (2015). Single substring based classification for nondeterministic finite automata. International Journal on Applications in Information and Communication Engineering, 1(10), 29-31.

[27] Bhateja, V., Gautam, A., Tiwari, A., Nhu, N.G., Le, D.-N, Haralick features-based classification of mammograms using SVM, Advances in Intelligent Systems and Computing, Volume 672, 2018, Pages 787-795.

[28] Latha, A., Prasanna, S., Hemalatha, S., & Sivakumar, B. (2019). A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks. Cognitive Systems Research, 56, 14-22.

[29] Krishnaraj, N., Elhoseny, M., Lydia, E. L., Shankar, K., & ALDabbas, O. (2020). An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment. Software: Practice and Experience.

[30] Namasudra, S., Roy, P., Vijayakumar, P., Audithan, S., & Balusamy, B. (2017). Time efficient secure DNA based access control model for cloud computing environment. Future Generation Computer Systems, 73, 90-105.

[31] Lakshmanaprabu, S. K., Shankar, K., Rani, S. S., Abdulhay, E., Arunkumar, N., Ramirez, G., & Uthayakumar, J. (2019). An effect of big data technology with ant colony optimization based routing in vehicular ad hoc networks: Towards smart cities. Journal of cleaner production, 217, 584-593.

[32] Namasudra, S., & Deka, G. C. (Eds.). (2018). Advances of DNA computing in cryptography. CRC Press.

[33] Mubarakali, A., Ashwin, M., Mavaluru, D., & Kumar, A. D. (2020). Design an attribute based health record protection algorithm for healthcare services in cloud environment. Multimedia Tools and Applications, 79(5), 3943-3956.

[34] Dey, N., Ashour, A.S., Chakraborty, S., Le, D.-N., Nguyen, G.N, Healthy and unhealthy rat hippocampus cells classification: A neural based automated system for Alzheimer disease classification, Journal of Advanced Microscopy Research, 11(1), pp. 1-10

[35] Krishnaraj, N., Ezhilarasu, P., & Gao, X. Z. Hybrid Soft Computing Approach for Prediction of Cancer in Colon Using Microarray Gene Data. Current Signal Transduction Therapy, 11(2).

[36] Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. (2020). The revolution of blockchain: State-of-the-art and research challenges. Archives of Computational Methods in Engineering.

[37] Goel, N., Grover, B., Gupta, D., Khanna, A., & Sharma, M. (2020). Modified Grasshopper Optimization Algorithm for detection of Autism Spectrum Disorder. Physical Communication, 101115.

[38] Prasanna, S., Narayan, S., NallaKaruppan, M. K., Anilkumar, C., & Ramasubbareddy, S. (2019). Iterative Approach for Frequent Set Mining Using Hadoop Over Cloud Environment. In Smart Intelligent Computing and Applications (pp. 399-405). Springer, Singapore.

[39] Le, D.-N.a, Kumar, R.b, Nguyen, G.N., Chatterjee, J.M.d, Cloud Computing and Virtualization, DOI: 10.1002/9781119488149, Wiley.

[40] Raj, R. J. S., Shobana, S. J., Pustokhina, I. V., Pustokhin, D. A., Gupta, D., & Shankar, K. (2020). Optimal Feature Selection-Based Medical Image Classification Using Deep Learning Model in Internet of Medical Things. IEEE Access, 8, 58006-58017.

[41] Namasudra, S., & Deka, G. C. (2018). Taxonomy of DNA-based security models. In Advances of DNA Computing in Cryptography (pp. 37-52). Chapman and Hall/CRC.

[42] Mubarakali, A., Ramakrishnan, J., Mavaluru, D., Elsir, A., Elsier, O., & Wakil, K. (2019). A new efficient design for random access memory based on quantum dot cellular automata nanotechnology. Nano Communication Networks, 21, 100252.

[43] Ramakrishnan, J., Mavaluru, D., Sakthivel, R. S., Alqahtani, A. S., Mubarakali, A., & Retnadhas, M. (2020). Brain–computer interface for amyotrophic lateral sclerosis patients using deep learning network. NEURAL COMPUTING & APPLICATIONS.

[44] Van, V.N., Chi, L.M., Long, N.Q., Nguyen, G.N., Le, D.-N, A performance analysis of openstack open-source solution for IaaS cloud computing, Advances in Intelligent Systems and Computing, 380, pp. 141-150.

[45] Sinha, A., Shrivastava, G., Kumar, P., & Gupta, D. (2020). A community-based hierarchical user authentication scheme for Industry 4.0. Software: Practice and Experience.

[46] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. Computer Communications, 151, 539-547.

[47] Mubarakali, A., Durai, A. D., Alshehri, M., AlFarraj, O., Ramakrishnan, J., & Mavaluru, D. (2020). Fog-Based Delay-Sensitive Data Transmission Algorithm for Data Forwarding and Storage in Cloud Environment for Multimedia Applications. Big Data.

[48] Reshmi, T. R., & Azath, M. (2020). Improved self-healing technique for 5G networks using predictive analysis. Peer-to-Peer Networking and Applications, 1-17.

[49] Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2020). Securing multimedia by using DNA based encryption in the cloud computing environment. ACM Transactions on Multimedia Computing Communications and Applications.

[50] Patro, K. K., Reddi, S. P. R., Khalelulla, S. E., Kumar, P. R., & Shankar, K. (2020). ECG data optimization for biometric human recognition using statistical distributed machine learning algorithm. The Journal of Supercomputing, 76(2), 858-875.

[51] Rajagopal, A., Joshi, G. P., Ramachandran, A., Subhalakshmi, R. T., Khari, M., Jha, S., ... & You, J. (2020). A Deep Learning Model Based on Multi-Objective Particle Swarm Optimization for Scene Classification in Unmanned Aerial Vehicles. IEEE Access, 8, 135383-135393.

[52] Chakchai So-In, Tri Gia Nguyen, Gia Nhu Nguyen: Barrier Coverage Deployment Algorithms for Mobile Sensor Networks. Journal of Internet Technology 12/2017; 18(7):1689-1699.

[53] Mubarakali, A., Bose, S. C., Srinivasan, K., Elsir, A., & Elsier, O. (2019). Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. Journal of Ambient Intelligence and Humanized Computing, 1-9.

[54] Devaraj, A. F. S., Murugaboopathi, G., Elhoseny, M., Shankar, K., Min, K., Moon, H., & Joshi, G. P. (2020). An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme. IEEE Access, 8, 144310-144320.

[55] Mubarakali, A. (2020). Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN (SRHB) Approach. MOBILE NETWORKS & APPLICATIONS.

[56] Namasudra, S. (2019). An improved attribute-based encryption technique towards the data security in cloud computing. Concurrency and Computation: Practice and Experience, 31(3), e4364.

[57] Kathiresan, S., Sait, A. R. W., Gupta, D., Lakshmanaprabu, S. K., Khanna, A., & Pandey, H. M. (2020). Automated detection and classification of fundus diabetic retinopathy images using synergic deep learning model. Pattern Recognition Letters.

[58] Govinda, K., & Prasanna, S. (2015, February). Medical dialysis prediction using fuzzy rules. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-5). IEEE.

[59] Sujatha, R., Navaneethan, C., Kaluri, R., & Prasanna, S. (2020). Optimized Digital Transformation in Government Services with Blockchain. In Blockchain Technology and Applications (pp. 79-100). Auerbach Publications.

[60] Govinda, K., & Prasanna, S. (2015, February). A generic image cryptography based on Rubik's cube. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-4). IEEE.

[61] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, BioSenHealth 1.0: A Novel Internet of Medical Things (IoMT) Based Patient Health Monitoring System, Lecture Notes in Networks and Systems. Springer, 2019

[62] Prasanna, S., & Narayanan, V. (2017). A Novel Approach for Generation of All-Optical OFDM Using Discrete Cosine Transform Based on Optical Couplers in a Radio-Over-Fiber Link. International Journal of Advanced

Research in Engineering and Technology, 8(3).

[63] Sanjeevi, P., Prasanna, S., Siva Kumar, B., Gunasekaran, G., Alagiri, I., & Vijay Anand, R. (2020). Precision agriculture and farming using Internet of Things based on wireless sensor network. Transactions on Emerging Telecommunications Technologies, e3978.

[64] Rathi, V. K., Chaudhary, V., Rajput, N. K., Ahuja, B., Jaiswal, A. K., Gupta, D., ... & Hammoudeh, M. (2020). A Blockchain-Enabled Multi Domain Edge Computing Orchestrator. IEEE Internet of Things Magazine, 3(2), 30-36.

[65] Khanna, A., Rodrigues, J. J., Gupta, N., Swaroop, A., & Gupta, D. (2020). Local mutual exclusion algorithm using fuzzy logic for Flying Ad hoc Networks. Computer Communications.