International Journal of Civil Engineering and Technology (IJCIET)
Volume 8, Issue 8, August 2017, pp. 898–904, Article ID: IJCIET_08_08_093
Available online at http://http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=8&IType=8
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

FRAMEWORK FOR EFFICIENT AUTHENTICATION MECHANISM FOR GENUINE USER'S PAYLOAD TRANSMISSION IN CYBERNETIC LOCATIONS

Dr. S. Sai S.N.Reddy, S. Nagarjuna Reddy
Department of Computer Science & Engineering
Vardhaman College of Engineering

N. Subba Reddy, M.Srinivasa Rao
Department of Computer Science & Engineering
MLR Institute of Technology, Hyderabad, India

ABSTRACT

The proposed system deals with efficient authentication mechanism for genuine user's payload insertion in cybernetic locations. The information is converted into small payload in cybernetic device readable signals. The signals being sent from a cybernetic device to another cybernetic device via cybernetic knob. Interrupt the payload by sending authentication mediator associated with source cybernetic device, inject the payload into scrutinizing authentication agent by a transmission channel through cybernetic knob. Scrutinize whether payload allowed for transmission, upon determining the payload is allowed, insert payload into source authentication mediator via transmission channel and forwarding payload to the destination cybernetic device via cybernetic knob.

Key words: Authentication Mechanism, Genuine Users, Payload Insertion, Packet Forwarding.

Cite this Article: S. Sai S.N.Reddy, S. Nagarjuna Reddy, N. Subba Reddy and M.Srinivasa Rao, Framework for Efficient Authentication Mechanism for Genuine User's Payload Transmission in Cybernetic Locations, International Journal of Civil Engineering and Technology, 8(8), 2017, pp. 898–904.
http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=8&IType=8

1. INTRODUCTION

With the advent of internet, the expectation of users towards copulation has rapidly increased. Not only increased speed but also correct information is expected to be transferred amongst different users. The users should be legitimate and the information should be authentic.

Technology has been kind enough to support the expectation. Since any years, scientists are working hard to achieve better results by upgrading the technology now and then.

They have tried with virtual private network, software defined network, cloud computing and the list goes endless. Virtual private network has given any advantages like robustness, increased speed in computation, scalability and authenticate service. Various protocols are implemented to transfer packets after checking the authenticity of the packets.

Software defined network works forwarding and control planes. The forwarding plane finds the logic how to forward incoming payload based on the MAC address, IP address and VLAN ID. The software decides whether to drop or forward the packet considering various parameters like authenticity and correct port to forward the packet. SDN gives ways for network control and it performs this functionality using its control plane and the controllers.

Another important aspect is cloud computing. Cloud and grid computing means robustness and excessive storage of data. Cloud also reduces computational cost and keeps the data protected.

The above mentioned technology has their own disadvantages as none of the guarantees immunity of service as they are purely based on internet connection. There can be hardware failure and they are open to attack.

In order to reduce the risk of all the threats, our proposed system works on the concept of virtual world and pledges to keep the users data ore safe. So we introduce the concept of Cybernetic Environment.

2. RELATED WORK

Moye Fraser [2002], Virtual private network helps the remote users to access secured network via non secure public network. For secured communication we need Firewalls for protection. Firewall helps to implement various control policies. Firewall protects the network from un-trusted public network i.e. the internet.

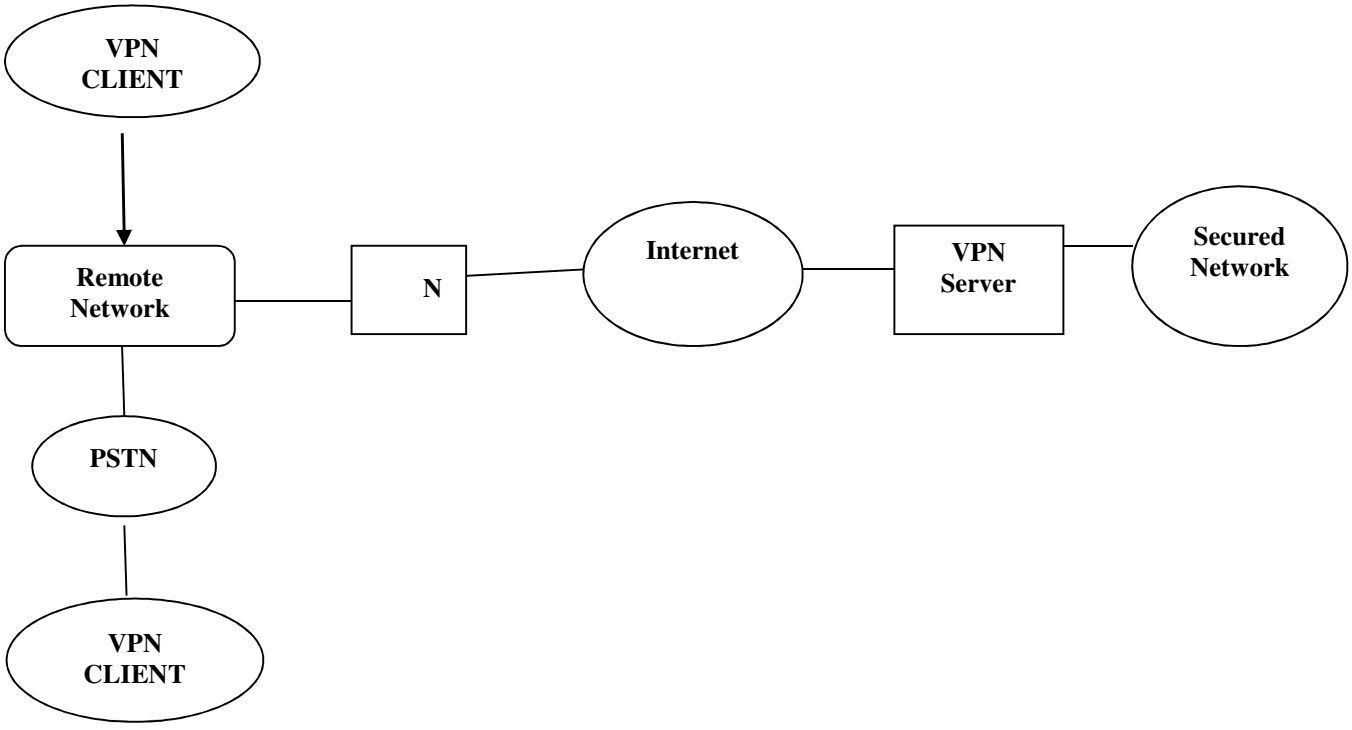


Figure 1 Virtual Private Network Architecture

Wolfgang Braun and Michael Menth [2014] Software –defined networking in the recent years has gained lots of importance as it implements software in complex networking domain. SDN uses the Open Flow Protocol. The Open Flow Protocol is built of switches and control plane. The control channel connects the switches with the control plane. There are few Open Flow Controllers for communicating with the switches.

David Hucaby [2004] Packets are to be forwarded between arbitrary hosts in the network. They should be forwarded in such a way that there should be performance optimization and scalability is increased. The technique applied is inter and intra domain routing. The packet forwarding mechanism matches the address of the incoming packet with the destination address. If there is a match found, then the packet is directed to the chosen output link. There is a switching fabric that directs packet from the input link to the output link. Various traffic control algorithms are used that helps to direct the traffic efficiently. The traffic is only given a clean cheat, after it is authenticated against various inbuilt algorithms.

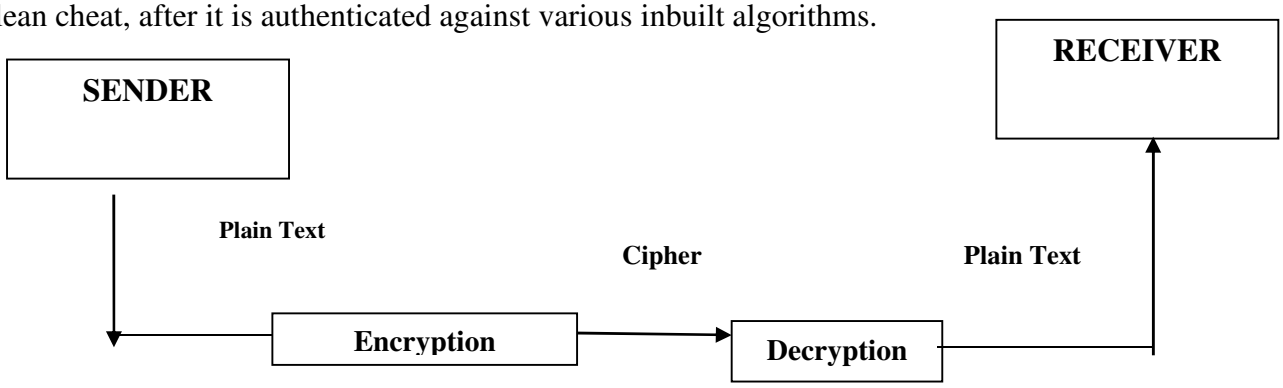


Figure 2 Cryptography Process

Dan Boneh Victor Shoup [August 17, 2015] There is a threat when a person with ale intention poses as a genuine user and tries to access the protected resources. The most widely used technique is Cryptography to track such attackers. Cryptography encrypts a plain text data in such a way that it becomes difficult for an in genuine user to understand. The original data is locked and the key to open it lies with legitimate users only.

Alexa Huth and James Cebula [2011] With the advent of cloud computing paradigm, the cost of computing is decreased with the increase in storage and efficient delivery system. The proposed system is based on the idea of cloud computing and guarantees to give much enhanced features. As cloud provides better authentication of genuine users, so does our proposed system. Another important feature that goes beyond comparison is the robustness of cloud environment. The proposed system also promises to give users a robust environment for payload transmission.

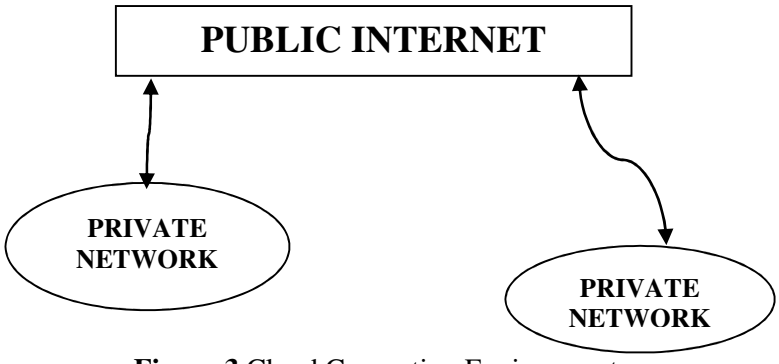


Figure 3 Cloud Computing Environment

3. PROPOSED SYSTEM

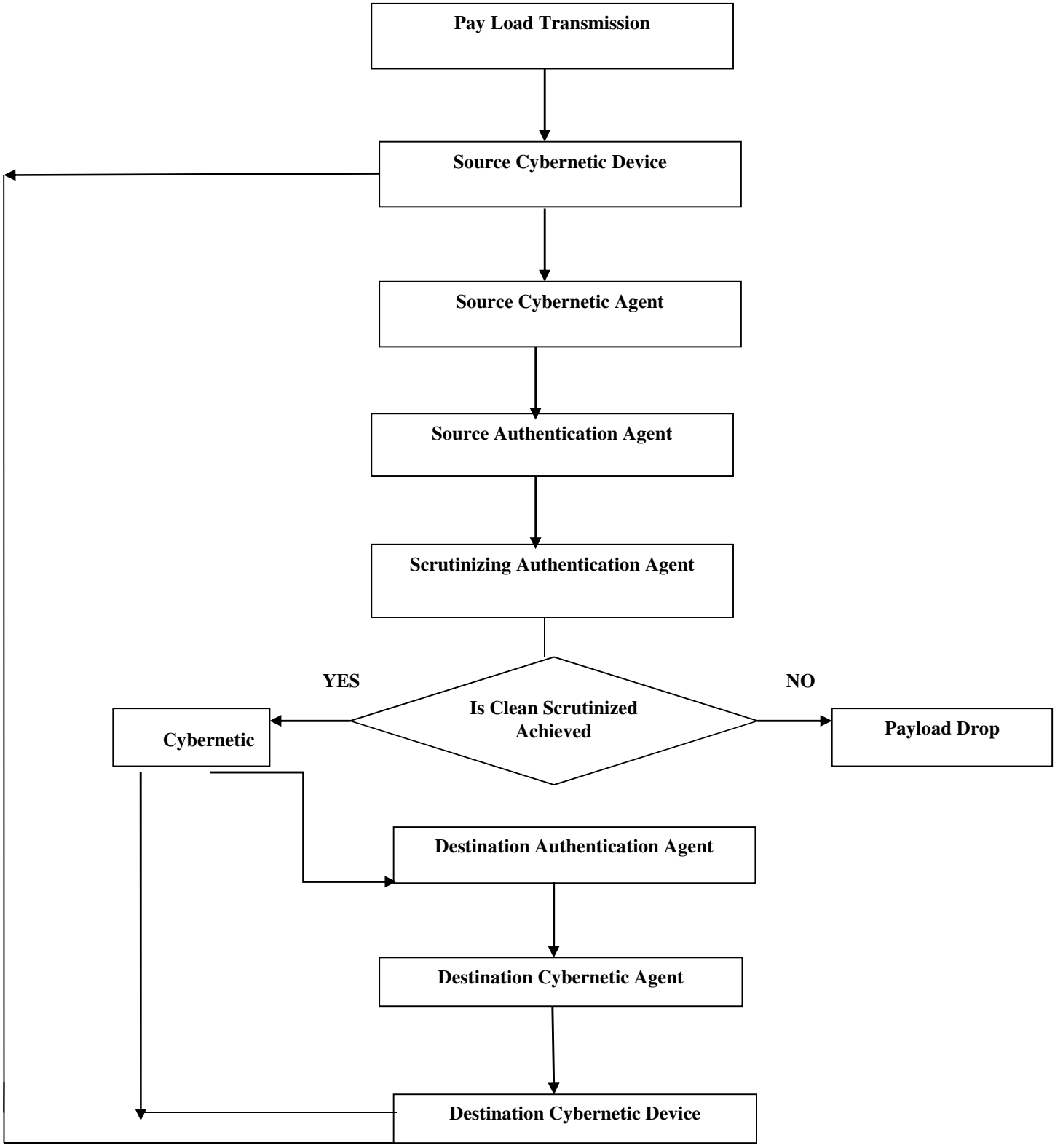
The proposed system provides a high-speed authentication scrutiny in cybernetic locations. The cybernetic solutions provide authenticated software with a choice to hook into all cybernetic network associations. The hooking to securitize all cybernetic network traffic, both in performance and in optimization of operating cost of the authentication process in the cybernetic locations. The performance enhancement may give way a boost in traffic scrutiny by a payload forwarding schemes. With this we will be able to offer the capability to competently and clearly forward system traffic between cybernetic network link and authenticating cybernetic device.

The proposed system has an ability to connect authentication agent on each port of a cybernetic knob. Such authentication agents have the ability to inject payload, received by an authentication agent, into a different port. The packet of data then undergoes authentication scrutiny, and is injected back into the cybernetic knob.

The proposed system provides for the first time a method for efficient authentication mechanism for scrutinizing in cybernetic locations, the system includes: (a) providing payload, in device-readable signals, being sent from a source cybernetic device to a destination cybernetic device via a cybernetic knob; (b) interrupting the payload by a source cybernetic agent associated with the source cybernetic device; (c) injecting the payload into an scrutinizing authentication agent associated with a source cybernetic device via a direct transmission channel which bypasses the cybernetic knob; (d) forwarding the payload to the source cybernetic device by employing a packet-forwarding mechanism; (e) determining, by the source cybernetic device, whether the payload is allowed for transmission; (f) upon determining the payload is allowed, injecting the payload back into the source authentication agent via the direct transmission channel; (g) forwarding the payload to the receiving cybernetic device via the virtual knob; (h) determining, by the source cybernetic agent, whether the payload is allowed for communication; (i) upon determining the data packet is allowed, continuing to step (g); (j) upon determining the data packet is not allowed, dropping the data packet; (k) upon determining the payload is permitted, tagging the payload as a clean scrutinized label; (l) injecting the clean scrutinized label by a destination authentication agent and destination cybernetic agent related with the destination cybernetic device; (m) scrutinizing, by the destination cybernetic agent, whether an incoming payload has a clean scrutinized label; and (n) upon determining the incoming payload has the clean scrutinized label, transmitting the received payload to the destination cybernetic device.

The authentication cybernetic device includes at least one authentic module nominated from the cluster comprising of a firewall, a Virtual Private Network (VPN), an Intrusion Prevention System (IPS), a Data-Loss Prevention (DLP) system, an Intrusion Detection System (IDS), a Uniform Resource Locator (URL) filter, a web filter and a malware filter.

DATAFLOW DIAGRAM OF THE PROPOSED SYSTEM



4. CONCLUSION

The proposed system provides a high-speed authentication system in cybernetic locations. The system uses authenticated software to check network traffic into all cybernetic locations. The software also provides optimization in performance and operating cost in the authentication process. As there is a performance enhancement, there is also a boost in traffic scrutiny by the payload forwarding scheme.

The proposed system can competently forward system traffic between cybernetic network link with the help of cybernetic authentication agent. The traffic checking mechanism is comparatively much more efficient using the cybernetic authentication agent and provides better results than directly passing the traffic between cybernetic knob and destination cybernetic device. The proposed system attaches the authenticating agent to each port of a cybernetic knob. The cybernetic knob along with the authenticating agent can forward the traffic to one of its other port. The proposed system increases the reliability and performance to a much greater extent.

REFERENCES

[1] G Julius Caersar, Igor, John F Kennedy, Cryptography, Security Engineering: A Guide to Building Dependable Distributed Systems

[2] Nigel Smart, Cryptography-An Introduction

[3] Professor Guevara Noubir Fundamentals of Cryptography, IEEE transactions on knowledge and data engineering, 23(4), pp. 496-511, 2011.

[4] Wolfgang Braun, Michael Menth, Software-Defined Networking Using Open Flow: Protocols, Applications and Architectural Design Choices", Department of Computer Science, University of Tuebingen, 12 May 2014

[5] Liu, Bing, Information retrieval and Web search. Springer, In Web Data Mining, pp. 211-268, 2011.

[6] Lee, Ming-Che, Kun Hua Tsai, and Tzone I. Wang, A practical ontology query expansion algorithm for semantic-aware learning objects retrieval, Elsevier, Computers & Education, 50(4), pp.1240-1257, 2008.

[7] Tamine-Lechani, Lynda, Mohand Boughanem, and Mariam Daoud., Evaluation of contextual information retrieval effectiveness: overview of issues and research, Springer, Knowledge and Information Systems, Volume. 24 (1), pp. 1-34, 2010.

[8] Ghorab, M. Rami, Dong Zhou, Alexander O'Connor, and Vincent Wade, Personalised information retrieval: survey and classification, Springer, User Modeling and User-Adapted Interaction, Volume. 23, (4), pp. 381-443, 2013.

[9] [9] Zhou, Dong, Séamus Lawless, and Vincent Wade, Improving search via personalized query expansion using social media, Springer, Information retrieval, Volume. 15 (3-4). pp. 218-242, 2012.

[10] Malizia, Alessio, Kai A. Olsen, Tommaso Turchi, and Pierluigi Crescenzi, An ant-colony based approach for real-time implicit collaborative information seeking, Elsevier, Information Processing & Management, 53(3), pp. 608-623, 2017.

[11] Jalali, Vahid, and Mohammad Reza Matash Borujerdi, Information retrieval with concept-based pseudo-relevance feedback in MEDLINE, Springer, Knowledge and information systems, 29(1), pp. 237-248, 2011.

[12] Gao, Ge, Yu-Shen Liu, Meng Wang, Ming Gu, and Jun-Hai Yong, A query expansion method for retrieving online BIM resources based on Industry Foundation Classes, Elsevier, Automation in Construction, Volume 56, pp. 14-25, 2015.

[13] Kuo, Yin-Hsi, Kuan-Ting Chen, Chien-Hsing Chiang, and Winston H. Hsu, Query expansion for hash-based image object retrieval, ACM, pp. 65-74, 2009.

[14] Melucci, Massimo, A basis for information retrieval in context, ACM, Transactions on Information Systems (TOIS), volume. 26, no. 3, pp.14, 2008.

[15] Nimisha Paulose, Sarika S, Effectiveness of Various User Authentication Techniques, Volume 5, Issue 12, December (2014), pp. 142-147, International Journal of Computer Engineering & Technology (IJCET).

[16] Prof. S. BalajI, Dr. Habibullah Khan, Dr. M. Janga Reddy and Dr. M. Gurunadha Babu, Authentication Frameworks for Enhancing Security in Biometric Systems, International Journal of Mechanical Engineering and Technology 8(7), 2017,pp. 1073–1080.

[17] Mohamed Basheer. K. P and Dr. T. Abdul Razak, Enhanced Biometric Based Authentication For Network Security Using Iris, Volume 4, Issue 6, November - December (2013), pp. 414-422, International Journal of Computer Engineering and Technology.

[18] K. Gnanalakshmi and G. Gayathri, Fact: A Framework for Authentication in Cloud-Based IP Traceback. International Journal of Computer Engineering & Technology, 8(4), 2017, pp. 53–56.

[19] Song, Wei, and Soon Cheol Park, Latent semantic analysis for vector space expansion and fuzzy logic-based genetic clustering, Springer, Knowledge and Information Systems, 22(3), pp. 347-369, 2010.