A Pragmatic Algorithm for Attack Prevention on Semantic Web Services

Nagendra Kumar Singh, Sandeep Kumar Nayak

***Abstract:** In this digital age, semantic Web services have emerged as services that are used in every field. Today various types of services like e-commerce, social networking, and online payment of various services, etc., are used by the user through the Semantic Web. The Semantic Web has emerged as a powerful medium for using online services. The use of semantic Web services greatly simplified the life of the common citizen. The database is used to hoard information related to various services provided by Semantic Web Services. It turns out to be indispensable that when a user communicates with the database then there should not be any interference in it. The expansion of semantic Web services led various assailants to start making various efforts to stop these services. The network assail for instance Man-in-middle or DoS assail has adverse effect on the performance of the Web service. This paper insinuates a principle server of ARP algorithm that uses IP-MAC trussing approach on the network to prevent Man-in-the-middle and DoS assail within a entreaty succumbed to the Web service. Aftermath revelations that after implementing the algorithms, the number of packet loss reduces drastically and enhancing the overall performance of Web service. The staple objective of this paper is how the services bestowed by the Web service can be protected from assailant.*

***Keyword:** Semantic Web, Security, CAP theorem,*

I. INTRODUCTION

In today's digital age, the development and expansion of Semantic Web services has been very rapid. A Web service is a type of amenity by one type of electronic processing device to exchange information over the Internet amid other electronic processing units [1]. A variety of functionalities that are available in a application, are condensed and reachable on the Internet through a Web service assemblage. The Internet and related technologies are the main contributors to the development of the Semantic Web. Web services have been identified as the major technique in providing a flexible solution to interact with the heterogeneous application system. Due to their knack to interact with heterogeneous software systems, Web services have fascinated the courteousness of many disseminated application developers. The amassed number of disseminated software applications has been published in the form of Web services on the Internet. Web services are the easiest way to implement a loose-fitting architecture for most organizations.

The market of doing business on the Internet under business to consumer (B2C) or Business to Business (B2B) model is growing beyond geographical limitations and its development is unprecedented.

Web services allow machines or software to communicate using a set of XML-based standards on different platforms. Security signposts to all the measures taken for the safety of a place or organization, as well as to corroborate that only those people, who have the necessary permission to use the resources of the organization, can only admittance them [2]. Security can be considered as a protection against unwanted or sudden assail s. Safety means an environment in which a person or group can feel secure against theft, espionage or misuse of their information, resources or things. The main purpose of security is to provide provision for personal services in the fortification of people, information and property for personal safety or community welfare.

Many fiscal online payment based applications are founded on the Web where a user's password, credit/debit card number, cvv number and other information will become the assailer's main target. There are innumerable straits for assailants to filch censored data, such as compromising Web application servers, snuffling networks or instilling malevolent client-side code. Acute data seepage causes considerable mutilation to the organization. To safeguard the assets of an organization from unauthorized or harmful assail s, it is necessary to implement certain special provisions in security.

Web services improve the interoperability by camouflaging the heterogeneity of the immeasurable platforms and thus are proficient to patronage multifaceted commercial applications. Web service model provides flexibility in implementing complex software systems. These services are important concepts that enable modularization of tasks or capabilities presented as services to remove intangible activities in complex business processes that can be re-organized at any time in an easy way.

Due to the brisk expansion of amenity-oriented computing, a growing number of disseminated software applications have been developed using services that are provided by existing Web services. As an innovative disseminated computing model, Web service is an enthralling mechanism for data and application amalgamation across the Web. Web services can be used to execute various applications that can be anything from simple Web entreaty to complex business processes.

E-commerce powered by computer and Internet technology has experienced generous augmentation in almost all sectors during the preceding years [3]. E-commerce has made significant changes in the ploy of doing business and has changed them completely. Transaction efficiency has steadily improved due to the advanced development of the Internet and other associative technologies, which has gradually led to decentralization of the market.

Revised Manuscript Received on October 15, 2019

Sandeep Kumar Nayak, Computer Applications, Integral University, Lucknow, India, Email: nayak.kr.sandeep@gmail.com

Nagendra Kumar Singh, Computer Applications, Integral University, Lucknow, India, Email: nksingh444@gmail.com

The CAP theorem affirms that any network system that shares data can have furthermost two desirable properties: consistency (C) high availability (A) and tolerance for partition network (P) [4]. CAP Theorem is very important in the Big Data world and e-commerce. A system that is partition-tolerant can sustain any network failure until the entire network fails. The data record is adequately replicated on different nodes to maintain the system through intermittent outages. A system has a consistent if a transaction starts with the system in a coherent state, and ends with the system in a coherent state. To achieve availability in dispersed systems, it is necessary that the system is running at all times. It develops the concept in disseminated computing that even an unreliable disseminated system has the potential to guarantee both security and availability.

Polyglot Persistence means that when data is hoard, it is best to use several data storage techniques, similar to the way data is used by individual applications or cogs of a sole application [5]. Different types of data are best coped with different database storage programs. In short, this means choosing the right database program to hoard the correct data.

Due to increasing trend of Web services like e-commerce, there is a need to give adequate attention to the security of these Web services. Web services such as e-commerce hoard different types of data and the Web service has to process this data to get the result of a query. In such a situation it becomes absolutely necessary to select a database program for Web services like e-commerce. This problem has been discussed in the foregoing paper and through the results it has been shown how messy database design can have an austere effect on Web services capability. It has also been demonstrated that having a man-in-the-middle or DoS assail present in the network increases the chances of packet loss in the network.

The Address Resolution Protocol (ARP) is used to identify the MAC address allied with the IP address of a node present in a network [6]. This protocol is widely used in existing Web service systems to obtain the client's corresponding MAC address from an IP address to validate the client's authenticity. There is a risk of frequent assail s because the ARP protocol is built on mutual trust of client and Web server. When a malicious node is involved in the network, it incorporates the IP address of the foregoingly connected node with its physical address, which causes the server to assume that the entreaty is coming from an already authorized node. This way the server can accept the entreaty of an unauthorized node and transfer the packet. The ARP protocol remains susceptible to assail by ARP sullying [7]. The main purpose of an ARP sullying assail is to maliciously amend the IP / MAC address plotting in a remote machine's ARP cache. The use of this ARP sullying is commonly chosen as Denial of Service (DoS) or MITM assail s to affect the ability of Web services.

In view of all these situations, a procedure is needed that protects Web services from network assail s. This paper proposes a concept of Principal Server of ARP to protect Web service server from network assail s such as man-in-the-middle or DoS assails. The proposed algorithms is based on the concept of IP-MAC trussing where Principal Server of ARP hoards combination of IP-MAC trussing for each entreatys generated from clients on the network.

If the assailer stabs assailing the Principal Server of ARP with newfangled IP-MAC combination, the Principal Server of ARP will remit ARP Entreaty packets towards the foregoing MAC of the IP-MAC trussing. If Principal Server of ARP can get ARP Riposte from the foregoing IP-MAC, the Principal Server of ARP will deteriorates the newfangled entreaty and clings to the foregoing IP-MAC trussing.

The paper is drafted as follows. Section II gives brief insight into foregoing literature related to Semantic Web and its security requirements. Section III provides a detailed overview and implementation of proposed algorithm for preventing assails on Semantic Web. Section IV briefly describes the results and discussion after implementing the proposed algorithms. Future discussions and conclusion has been given in Section 5.

II. RELATED WORK

Sim Kim Lau, Reza Zamani, Willy Susilo [8], Using ontology approach, an intelligent community transport service has given semantic Web vision for the brokerage system. Jelena Jovanovic and Ebrahim Bagheri [9] have given a systematic analysis of Semantic Web in the field of E-commerce. They presented a technological stack for Semantic Web based E-commerce applications and briefly portrays the challenges that are faced by the e-commerce applications. In [10], Lorenzo Bossi, Elisa Bertino, and Syed Rafiul Hussain have proposed a formal model to detect malicious behaviour executed by the foregoingly accredited application. The model hoards the signature and constraints for each query submitted to the database but do not estimate the amount of data returned by the query. A model for controlling admittance in online social platforms has been developed by the Yuan Cheng, Jaehong Park, and Ravi Sandhu [11] which uses regular manifestation annotation for policy specification. The proposed algorithms are used to verify the necessary connotation path amid users for a given admittance. Q. Chang, D. DiFranzo, M.J.K. Gloria, B. Makni and J.A. Hendler [12] have reviewed the research work done on trust in the simulated world and analyzed the inclusion of semantic Web in the social network.

In [13], two types of semantic amenities are specified. One service recognizes the events and other service handles the event. These events are matched by evaluating the word similarity that maneuvers with word embedding. It presents a hybrid approach to word embedding learning that treats words in different ways according to word occurrences. An integrated set of algorithms and tools have been proposed with the aim of reducing developers' work to develop, deploy, and migrate multiple data hoard applications in a cloud environment [14]. A unified data model has been provided to application developers to amalgamate with assorted relational and NoSQL data hoards. Developers can express queries using the OPEN-Paa-DataBase API (ODBAPI). It is a REST based API that allows programmers to transcribe their application code independently to the target data hoard.

A virtual data hoard has also been proposed which espouses the execution of sole or complex queries on assorted data hoards. A tactic to polyglot speech amalgamation based on cross-lingual frame selection has been proposed [15]. The proposed routine entails only mono-lingual dialogue data of unlike orators in diverse languages for amassing a polyglot synthesis system.

The authors proposed a methodology which is based on the CAP statement, as well as a framework for evaluating the CAP properties of NoSQL [16]. They have compared two different cloud NoSQL systems through the cap theorem and consider the cap properties for the selection of data storage solutions. A comprehensive literature has been provided regarding the CAP theorem that defines various components of the CF theorem in detail [17]. An automated polygon persistence approach has been proposed based on defined service level agreements on the operable and inoperable necessities of database systems [18]. The concept of Polyglot Persistence Mediator (PPM) allows runtime decisions to route data of unalike backends conforming to schema-based clarifications.

The authors insinuate the concept of the process profile by analyzing the internal behavioral relationships of each process and delineating the interrelations amid process segments [19]. Moreover, a method of behavioral consistency has been proposed that is centered on the process profile and can be calculated in polynomial time. An exploration has been commenced to analyze the behaviors of e-commerce organizations [20]. The primary focus is on analyzing both system behavior and user behavior in the context of e-commerce trading systems. The erstwhile objective is to analyze the stability of system behavior regarding the measurement and diagnosis of e-commerce trading systems. A conceptual framework has been put forward to extract the characteristics of fraudulent transactions, including personal and transaction-related indicators [21]. A fraud detection mechanism has been proposed to detect frauds related to transactions occurring in e-commerce [22]. Back propagation neural networks and game theory are introduced to design detection methods and defense mechanisms for DoS assail s [23]. The problem of decentralized adaptive output feedback control for denial-of-service (DoS) assail s has been investigated [24].

III. ALGORITHM FOR ASSAIL PREVENTION ON SEMANTIC WEB

This paper introduces algorithms to protect Web services from multiple network assails such as DoS and man-in-the-middle assail s by conceptualizing the principal server of ARP. The principle server of ARP will hoard the IP-MAC trussing of each entreaty originating from the client on the network. Whenever a newfangled client connects to the network, it will fling an entreaty to the principal server of the ARP to connect to the Web server providing a specific type of Web service. The principal server of the ARP will respond to the entreatying client, including the IP and MAC of the principal server of the ARP. This IP-MAC trussing is hoarded in the client host. This ploy is pursued at both ends. The proposed algorithm to maintain IP-MAC trussing at both client and server side is explained in the following section.

A. Algorithm 1: Client Side Implementation

The client host maintains an ancillary ARP index that will permanently hoard the IP-MAC trussing of the principal server of ARP. Whenever a client wants to communicate with the web server, its entreaty is transferred to the main server of ARP. The main server of the ARP flings its IP-MAC trussing to the client to let the client know that the retort to its entreaty is coming from a legitimate web server. The client preserves the IP-MAC trussing of the principal server of ARP in its ancillary index, so that the validity of the server can be identified next time.

1. When a newfangled node joins the network, it disseminates a “Who's going to be Principal Server of ARP” entreaty.
2. The Principal Server of ARP replies back which consists of IP-MAC trussing.
3. The client monitors its ARP cache for changes in IP-MAC trussing for the principal server of ARP. If there are any changes in IP-MAC trussing, the progress is checked against ancillary cache.
4. When the IP-MAC trussing occurs in ancillary cache, it is pondered as brand newfangled IP-MAC trussing in ARP index. Go to step 3.
5. The client guides an entreaty to Principal Server of ARP to the correct MAC address for the given IP address.
6. The IP-MAC trussing replied by the Principal Server of ARP is currently hoardd in ARP cache together with ancillary cache.
7. Go to step 3.

B. Algorithm 2: Principal Server of ARP Implementation

The Principal server of ARP will hoard the IP-MAC trussing for each client. When a client registered with the Web server, the principal server of ARP will hoard the IP-MAC trussing of the client. For this intention, the principal server of ARP will maintain the ancillary index which hoards the IP-MAC trussing for each client. Whenever a client flings an entreaty to the server, the main server of ARP will search the ancillary index for IP-MAC trussing. If such IP-MAC trussing has been found the ancillary index, it will permit the client to communicate with the Web server. The Algorithm is as follows:

1. The Principal Server of ARP server will uphold another elongated ARP cache index.
2. Each time a client node unifies the network and newscast an entreaty for Principal Server of ARP, the Principal Server of ARP will reply back which consists of IP and MAC address.
3. Whenever a client node entreaty for MAC address of an IP address, the Principal Server of ARP will seek out the trussing in its ancillary ARP index.
4. If the IP-MAC trussing is present to use ancillary ARP index, it will reply the trussing for the client node.
5. If the IP-MAC trussing is not present, it will newscast ARP Entreaty for the IP address. The MAC address received by ARP Reply is trapped in its ancillary ARP index.

C. Algorithm 3: Principal Server of ARP Antidote Implementation

The antidote ploy has been employed to protect principal server of ARP against an ARP sullying assail. When a client wants to communicate with the web server, the principal server of ARP will discover the client's IP-MAC trussing in its ancillary index. If there is a change in the client's IP-MAC trussing, the principal server of the ARP will fling 50 packets to the client's foregoing MAC address. If at least one packet is answered, the newfangled IP-MAC trussing entreaty will be rejected. If no packet is received, a newfangled IP-MAC trussing is assented.

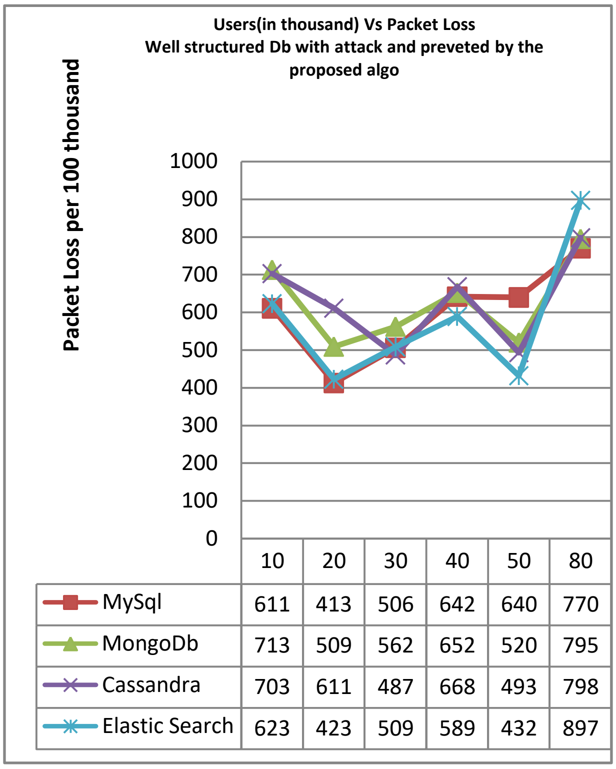
1. The Principal Server of ARP keeps an ancillary ARP index with lasting cache.
2. If find amend in its ARP cache, the advance is tested using its ancillary ARP index.
3. If the IP-MAC trussing is not precise for a entreaty coming from the foregoing registered client, the principal server of ARP fling 50 ARP Entreaty packets to the foregoing MAC address for the IP addresses.
4. If at least one of many retorts is received from foregoing IP-MAC trussing, the foregoing IP-MAC trussing is positioned in their ARP cache and newfangled IP-MAC trussing will be discarded. Goto step 2.
5. If no reply is received from the foregoing MAC address, the ancillary index as well as ARP cache is revised for the newfangled IP-MAC trussing.
6. Go to step 2

This antidote ploy affords constancy alongside ARP hoaxing assails against the Principal Server of ARP. If the assailer is able to register its IP-MAC trussing in the server, all erstwhile systems will respect that the IP-MAC trussing is as the assailer's real IP address. It attempts to poison the IP-collision problem. Thus the assailer will not be adept MITM amid nodes present on the network.

IV. RESULTS AND DISCUSSION

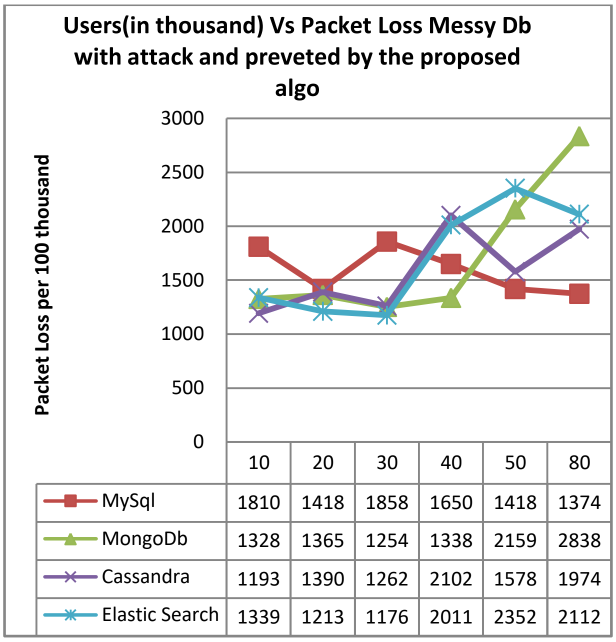
A test database has been used from Badhalia Gems [25], an e-commerce Web service that provides online shopping of stones. The Web service provides various services such as creating user account, managing user account, search for a product, adding product into cart, product order, order management, payment, product information and modification etc. The Web service has 1000 user and each user generating at least 10 queries from each database. The SOAPSonar [26] simulator has been used to tryout the effectiveness of using the correct database for various types of data hoard on the Web service.

The foregoing paper shows that how network assail affecting the performance of semantic Web services. Fig. 1 shows that after applying the proposed algorithm, the network assail s are reduced significantly for well-structured database. Fig. 2 also shows that after implementing the algorithm for messy database design, the number of packets that were lost due to network assail is decreases significantly. After injecting the network assail s such DoS and man-in-the-middle assail using the simulator, the performance of the Web service has been measured. The results shows that after implementing the algorithms, the number of packets that were lost during transmission has been reduced drastically compared to foregoing results. The following are the main findings after implementing the algorithms



	10	20	30	40	50	80
MySql	611	413	506	642	640	770
MongoDb	713	509	562	652	520	795
Cassandra	703	611	487	668	493	798
Elastic Search	623	423	509	589	432	897

Fig. 1: Assail prevention in well-structured database.



	10	20	30	40	50	80
MySql	1810	1418	1858	1650	1418	1374
MongoDb	1328	1365	1254	1338	2159	2838
Cassandra	1193	1390	1262	2102	1578	1974
Elastic Search	1339	1213	1176	2011	2352	2112

Fig. 2: Assail prevention in messy database

A. Assail with a node

If assailer performs ARP spoofing assails with a node against another node, the victim node will entreaty the Principal Server of ARP to ratify the IP-ARP trussing. The Principal Server of ARP will retort with correct trussing. Thus, assails done around the node won't lead to ARP cache sullying.

B. Assail on Principal Server of ARP when an entry is present

If the assailer tries assailing the Principal Server of ARP, the Principal Server of ARP will fling 50 ARP Entreaty unicast packets towards the foregoing MAC of the IP-MAC trussing. If the Principal Server of ARP can get ARP Retort from the foregoing node, the Principal Server of ARP will drop the newfangled entreaty and stab to the foregoing IP-MAC trussing.

C. Assail on Principal Server of ARP when entry just isn't foregoing present

If the assailer tries assailing the Principal Server of ARP with IP addresses not already assigned, the Principal Server of ARP will accept the entry. This assail will be as harvesting IP addresses. But as the server encourage the IP-MAC trussing; other nodes present for the network may also honor that trussing. This now becomes analogous to assailer actually seizing the IP address. However, in this situation that assailer cannot sully any other IP address to take assailer as gateway. The assail will reduced on the assailer seizing manifold IP addresses. MITM is not possible in this instance.

D. Assail against Principal Server of ARP and node

If assailer opts to assail a node and perform MITM amid Principal Server of ARP and node, and since the victim once provided with the IP-MAC trussing of Principal Server of ARP continues to make use of that and the assailer can only stab a race-condition. However, the assailer attempts to retort first to the Principal Server of ARP entreaty. If assailer wins the race, the assailer may actually sully the ARP cache entries of hosts.

But as, assailer will need to answer the entreaty, this causes assailer to simply get perceived by Intrusion Detection Systems present within the network. The IDS will occasionally entreaty for Principal Server of ARP and so can detect presence of any rogue Principal Server of ARP on the network. The similar assail can be doable to erstwhile elucidations precluding ARP sullying using extension of DHCP server by DHCP Spoofing.

V. CONCLUSION AND FUTURE WORK

This paper proposes the algorithms for preventing network assails on semantic Web services such as man-in-middle or DoS assail. The proposed algorithm shows that how the proposed algorithm will decrease the number of packet loss for semantic Web services due to network assails on semantic Web services. The first algorithm will significantly reduce the effect of network assails that were present on the network and affect the overall services of the semantic Web. In near future, the plan will be to further enhance the overall performance of proposed algorithm by extending the capability of the algorithms.

ACKNOWLEDGEMENT

We are heartily grateful to the Integral University for supporting this research with the Manuscript Communication Number (MCN) - IU/R&D/2019-MCN-000719.

REFERENCES

1. S. Badsha, X. Yi, I. Khalil, D. Liu, S. Nepal and K. Lam, “Privacy preserving user based web service recommendations”, IEEE Admittance , vol. 6, Oct. 2018, pp. 56647-56657.
2. S. Liang, Y. Zhang, B. Li, X. Gio, C. Jia and Z. Liu, “SecureWeb: Protecting Sensitive Information Through the Web Browser Extension with a Security Token”, Tsinghua Science and Technology, vol. 23(5), Oct. 2018, pp. 526-538.
3. Y. Huang, Y. Chai, Y. Liu and J. Shen, “Architecture of next-generation e-commerce platform”, Tsinghua Science and Technology, vol. 24(1), Nov. 2018, pp. 18-29.
4. S. Gilbert and N. Lynch, “Perspectives on the CAP Theorem”. Computer, vol. 45(2), Jan. 2012, pp. 30-36.
5. Maccioni, O. Cassano, Y. Luo, J. Castrej´on, and G. Vargas-Solar, “NoXperanto: Crowdsourced polyglot persistence”. Polibits, vol. 50, Jul. 2014 pp. 43-48.
6. W. Gao, Y. Sun, Q. Fu, Z. Wu, X. Ma, K. Zheng and X. Huang, “ARP Sullying Prevention in Internet of Things”, 2018 9th International Conference on Information Technology in Medicine and Education China, 2018, p. 733.
7. S. Y. Nam, D. Kim and J. Kim, “Enhanced ARP: Preventing ARP Sullying-Based Man-in-the-Middle Assail s”, IEEE Communications Letters, vol. 14(2), Feb. 2010, pp. 187-189.
8. M. Doroudian, N. Arastouie, M. Talebi and A. R. Ghanbarian, “Multilayered database intrusion detection system for detecting malicious behaviors in big data transaction”, IEEE International Conference on Information Security and Cyber Forensics (InfoSec) South Africa, 2015, p. 105.
9. J. Jovanovic and E. Bagheri, “Electronic Commerce Meets the Semantic Web”, IT Professionals, vol. 18(4), Aug. 2016, pp. 56-65.
10. L. Bossi, E. Bertino, and S. R. Hussain, “A System for Profiling and Monitoring Database Admittance Patterns by Application Programs for Anomaly Detection”, IEEE Transactions on Software Engineering, vol. 43, Aug. 2017, pp. 415-431.
11. Y. Cheng, J. Park, and R. Sandhu, “An Admittance Control Model for Online Social Networks Using User-to-User Relationships”, IEEE Transactions on Dependable and Secure Computing, vol. 13(4), Aug. 2016, pp. 424- 436.
12. Q. Chang, D. DiFranzo, M. J. K. Gloria, B. Makni and J.A. Hendler, “Analyzing the Flow of Trust in the Virtual World With Semantic Web Technologies”, IEEE Transactions on Computational Social Systems, vol. 5(3), Aug. 2018, pp. 807-815.
13. Liu, D. Deng, J. Jiang and Q. Tang, “Event-Driven Semantic Service Discovery Based on Word Embeddings”, IEEE Admittance , vol. 6, Oct. 2018, pp. 61030-61038.
14. R. Sellami, S. Bhiri and B. Defude, “Supporting Multi Data Hoards Applications in Cloud Environments”, IEEE Transactions on Services Computing, vol. 9(1), Jun. 2015, pp. 59-71.
15. Chen, Y. Huang, C. Hu and K. Lee, “Polyglot Speech Synthesis Based on Cross-Lingual Frame Selection Using Auditory and Articulatory Features”, IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 22, Oct. 2014, pp. 1558-1570.
16. S. Benefico, E. Gjeci, R. G. Gomarasca, E. Lever, S. Lombardo, D. Ardagna and E. Do. Nitto, “Evaluation of the CAP Properties on Amazon SimpleDB and Windows Azure Index Storage”, 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing Romania, 2012, p. 430.
17. Brewer, “CAP Twelve Years Later: How the Rules Have Changed”, IEEE Computer Society, vol. 45(2), Feb. 2012, pp. 23-29.
18. M. Schaarschmidt, F. Gessert and N. Ritter, “Towards Automated Polyglot Persistence”, Datenbanksysteme für Business, Technologie und Web Germany, 2015, p. 73.
19. M. Wang, Z. Ding, C. Jiang and P. Zhao, “A Process-Profile-Based Method to Measure Consistency of E-Commerce System”, IEEE Admittance , vol. 6, Apr. 2018, pp. 25100-25109.
20. P. Zhao, Z. Ding, M. Wang and R. Cao, “Behavior Analysis for Electronic Commerce Trading Systems: A Survey”, IEEE Admittance , vol. 7, Aug. 2019, pp. 108703-108728.
21. S. Luo and S. Wan, “Leveraging Product Characteristics for Online Collusive Detection in Big Data Transactions”, IEEE Admittance , vol. 7, Jan. 2019, pp. 40154-40164.
22. L. Zheng, G. Liu, C. Yan and C. Jiang, “Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity”, IEEE Transactions on Computational Social Systems, vol. 5(3), Aug. 2018, pp. 796-806.

23. L. Gao, Y. Li, L. Zhang, F. Lin, M. Ma, “Research on Detection and Defense Mechanisms of DoS Assail s Based on BP Neural Network and Game Theory”, IEEE Admittance , vol. 7, Mar. 2019, pp. 43018-43030.
24. L. An and G.H. Yang, “Decentralized Adaptive Fuzzy Secure Control for Nonlinear Uncertain Interconnected Systems Against Intermittent DoS Assail s”, IEEE Transactions on Cybernetics, vol. 49(3), Mar. 2019, pp. 827-838.
25. Badhalia Gems [Online], Available: http://jaipur.dkinfosolutions.com/badhaliagems/
26. SOAPSonar [Online], Available: https://www.crosschecknet.com/products/soapsonar/