Journal of Engineering and Applied Sciences

MEDWELL PUBLICATIONS

An Algorithm for Securing and Managing Hybrid Cloud Outsourced Data in Jordanian E-Governmental Services

Abdullah Alhaj
Department of BIT, Faculty of Information Technology and Systems, The University of Jordan, Aqqba, Jordan

Key words: Cloud computing, Information Transmission Algorithm (ITA), Jordanian E-governmental services

Corresponding Author:
Abdullah Alhaj
Department of BIT, Faculty of Information Technology and Systems, The University of Jordan, Aqqba, Jordan

Page No.: 2971-2976
Volume: 15, Issue 15, 2020
ISSN: 1816-949x
Journal of Engineering and Applied Sciences

Abstract: The cloud has become a noteworthy point in E-administrative governmental systems for providing E-services. In any case, governments and organizations must be prepared to meet the expanded solicitation of genuine and secure online administrations. The pattern has set up another scope of security gives that should be tended to. In cloud, the information and related E-administrations are not heavily influenced by them. Moreover, with the developing requests for cloud systems correspondence to give secure E-legislative administrations, it turns out to be progressively critical to make sure about information stream way. The current examination identified with security algorithm just spotlights on making sure about the progression of data in Jordanian E-legislative systems, improving the presentation of systems and to upgrade adaptability for different administrations. The security calculation work by encryption and unscrambling of the data, however don't think about the enhanced utilization of the system assets. This examination is relied upon to guide and benchmarks viably secure hybrid cloud outsourced data stream in Jordanian E-governmental services.

INTRODUCTION

"The concept of cloud computing offers new methods and approaches for information processing and data transmission"[1] and however, the Federal CIO Vivek Kundra has emphasized that "information security is still a top concern about cloud computing". "For instance, in cloud, the data and associated software are not under their control"[2]. Aljawarneh *et al*.[3] addresses the security threats that effect on the Jordanian E-governmental services. "A number of policies are suggested to face this kind of application vulnerabilities"[3].

"E-government is becoming a global phenomenon attracting the attention of politicians, policy makers and ordinary citizens". "A recent trend in the provision of public services has been to develop internet websites that provide easier access to government information and services"[4]. "Its main objectives can be categorized according to the promising benefits each government provides to citizens, businesses and other governmental agencies"[5]. "Using web technologies is providing governments with enormous chances to improve their offerings to their citizens and thus boosting the expectations of citizens towards public services"[6]. So,

governments must continue to improve their portals to comply with citizen's demands towards more information, better services and improved options. It is critical for governments to know what aspects of E-government websites are important to citizens. "Many E-government applications and tools would be left behind if their countries did not maintain the constant pressure for more online applications"[7]. Furthermore, successful understanding of citizen's expectations and feelings about websites is becoming very important. "Finally, delighted citizens are more effective and cheaper advertisers than all the paid advertisements placed in the media"[8]. Jordan is paying much attention to E-government initiative, especially, since, the last few years. "The Jordanian position in E-government readiness index improved from the 68th position in 2005 to the 50th position in 2008 which is considered the highest leap in the region"[7]. The same report indicated that Jordan has the highest jump in the world from the 90th position in 2005 to the 15th position in 2008 in the e-Participation index which indicates the high interest of the government in the success of such initiative.

By Devargas[9] " an overview of multi-processor scheduling algorithm is given without exploiting the two characteristics which are typical in IPsec packet processing". "There is also the discussion of the problem of load balancing on multiple processors which could cause many problems in data transmission for the E-governmental services"[10].

The proposed mechanism presented in this study allows scheduling packets to be processed either by the CPU or by the accelerators among the online E-governmental services. This also enhances scalability: one may use an accelerator tailored for the bandwidth normally required for VPNs and use the CPU to have a further processing capability when a higher bandwidth is required. In this study a proposed mechanism for securing hybrid cloud outsourced data in Jordanian E-governmental services. Our goal is to maximize the security to communications at the IP level to enhance scalability and to maximize throughput. It is explained by Raghuram and Chakrabarti[11] that "how to obtain data independency among packets for AES". Our approach fully exploits these characteristics to achieve high security and better performance.

Wang *et al.*[12] developed a mechanism to solve this issue in owner-write-users-read applications. They proposed to encrypt every data block with a different key, so that, flexible cryptography-based access control might be achieved. Through the adoption of key derivation methods, the owner needs to maintain only a few secrets. In this mechanism, the data can be updated only by the original owner through authentication way. At the same stage users with various access rights need to read the information in an efficient and secure manner. Both E-governmental data and users dynamics should be properly processed to preserve the performance and safety of the outsourced storage system.

System architecture: The design of the created ITA is made out of generator PCs, N cryptographic speeding up agents associated with the typical framework transport of the gateway and disseminated transfer speed arbitrator as appeared in Fig. 1. We think about heterogeneous quickening agents, i.e., quickening agents executing distinctive cryptographic calculations and permitting diverse preparing speeds. CPU-memory correspondence is performed on a quicker transport as in most current PCs. The system card is additionally associated with the quicker CPU transport. Just cryptography-related activities are offloaded to the accelerator (s). This implies all the IPSec header handling is finished by the CPU.

Assumptions: Our calculation depends on two principal suppositions: the first is that the handling time for packets is known (in any event roughly) ahead of time. This is valid for symmetric-key cryptographic calculations which are regularly utilized inside the IPSec setting: their processing time just relies upon the quantity of information blocks to be handled. The main special case is for the product execution of these calculations. For this situation the calculation time may fluctuate contingent upon the current CPU load. The subsequent supposition that will be every bundle can be processed freely from the others (i.e., there are no information conditions between various parcels). "This comes from IPSec specifications is that each packet must carry any data required for its processing"[13]. In Devargas[9] it is explained how to obtain "data independency among packets for AES". Our methodology completely abuses these presumptions to accomplish high security and QoS.

Description of the ITA: The principle objective of our ITA is to make sure about information transmission in varied networked systems and giving better execution and upgrading adaptability of information transmission by actualizing the most grounded security methodology and examining different security calculations. The principle highlights of the ITA:

When ITA is executed in a firewall or gateway, it gives solid security that can be applied to all traffic crossing the edge. Traffic inside a workgroup or organization doesn't acquire the overhead of security related preparing.

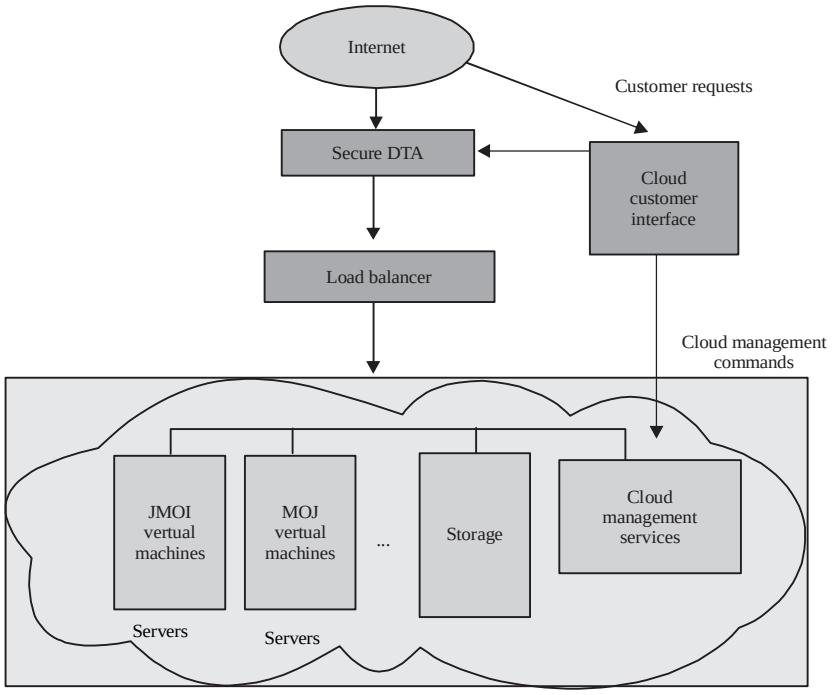

Fig. 1: Secure information transmission algorithm based on distributed bandwidth negotiator

ITA in a firewall is impervious to sidestep if all the outside traffic must utilize IP and the firewall is the main methods for entrance from the Internet into the association.

ITA as it researches the IPsec is underneath the vehicle layer (TCP, UDP) as is straight forward to application. There is no compelling reason to change programming on a client or server framework when it is executed in the firewall or gateway. ITA can be straightforward to end-clients. There is no compelling reason to prepare clients on security components, issue keying material on a for every client premise or disavow keying material when clients leave the association.

DTA can give security to singular clients if necessary. This is valuable for offsite laborers and for setting up a safe virtual sub arrange inside an association for touchy application. ITA can give a superior presentation and improving adaptability of information transmission.

The primary thought hidden the created ITA is to get the packets produced by the host PCs to be processed on the gateway (i.e., both of the speeding up agents or the CPU) which can give the briefest handling time. The created ITA forms every bundle as follows:

DTA, executed in a firewall or gateway has a Malicious Packet Detection System (MPDS) which will examine all the approaching packets and will choose to deny or pass the bundles through the gateway.

For the passed bundles from MPDS, speeding up agents will have the option to play out the cryptographic algorithm required by the considered packets is chosen. The principle objective of this examination is to give the more secure way to information transmission through the system, thus, ITA will explore the IPsec as the future standard security convention with Advanced Encryption Security (AES) which was at that point improved and picked by National Institute of Security and Technology in USA as the more secure encryption algorithm.

SECURE INFORMATION TRANSMISSION ALGORITHM WITH LOAD BALANCING AND CONGESTION CONTROL ALGORITHM

This Information Transmission Algorithm (ITA) assumes distributed Cloud Customer Interface (CCI) architecture as depicted in Fig. 1. A CCI is located in each of the LANs interconnected by the public network backbone: CCI is responsible for regulating traffic going into the public network. Suppose a host in public cloud has a flow of traffic that needs to request a service from the governmental cloud, the requesting host in public cloud would first make a request to the CCI by sending the amount of requested bandwidth to CCI. CCI would run the CAC algorithm (to be described below) based on real-time measurements made on the existing traffic at the cloud management services unit. If an admit decision is made, the requesting host starts sending traffic and the

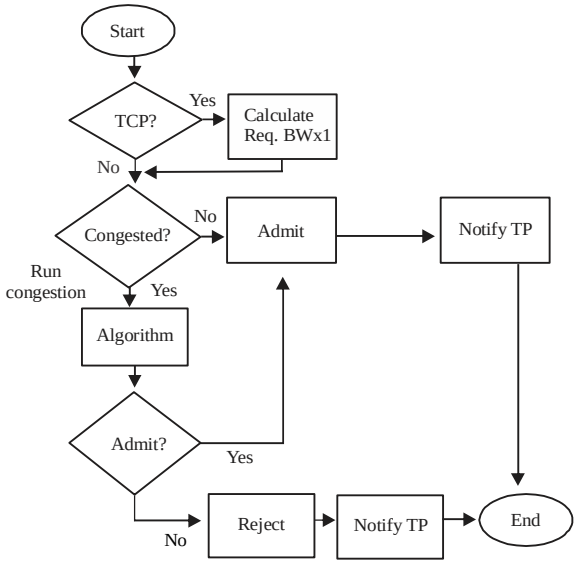

Fig. 2: Secure ITA

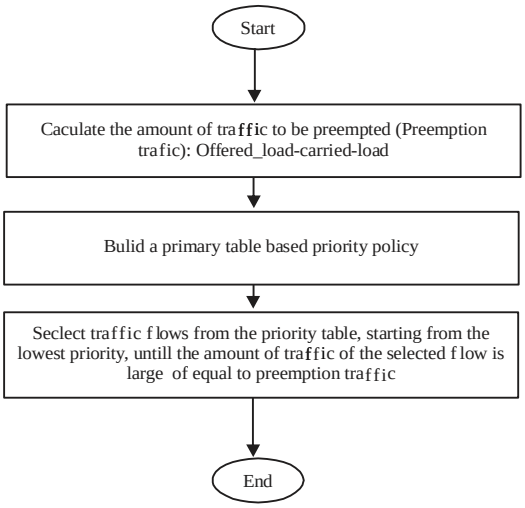

Fig. 3: Congestion control algorithm

load balancer is also informed to police the traffic. On the off chance that a reject choice is made, the mentioning host is informed about the choice. Moreover, "load balancer is educated to keep the dismissed stream from going into the open system"[14]. In order for the source to quickly make an admission/congesting decision, we believe the most valuable piece of information is the amount of carried traffic, i.e., the measure of traffic that is effectively sent through the WAN spine.. Therefore, at Governmental cloud, a measurement device measures the amount carried traffic. Such estimations are done on a for every Differentiated Services Code Point (DSCP) premise. The measurements are periodically sent back to public cloud which are used for the CCA and congestion algorithm. Assume because of clog in the open system, the transfer speed of a connection along the way in the open system out of nowhere diminishes to the degree that the connection data transmission is not at this point ready to help the measure of offered traffic. After "congested" state is declared by the cloud management services unit in governmental cloud and the CCI at public cloud is notified, the congestion algorithm is triggered and a fraction of the ongoing traffic flows are preempted. Then both the affected hosts and Load Balancer are notified by CCI. Assurance of the traffic streams to be appropriated upon clog or blockage is in light of the conveyed traffic estimations, per call mentioned data transfer capacity and a lot of predefined strategy (for example a strategy dependent on MLPP portrayed in Developed draft Strawman DSCP planning for GIG venture IP systems (n. d.)). Contrasted with the ordinary Bandwidth Merchant (BB, for example, the one depicted in Soltwisch, etc. which BB is accepted to have global knowledge about the network, this CCA utilizes a distributed architecture. Namely, each CCI makes admission and congestion decision solely based on the feedback from the destination and there is no other inter CCI information exchanged. In addition, CCI is consulted only when a call needs to traverse through the public network. If a call originated from public cloud does not need to go through the public network, CCI will not be consulted. The natty gritty depiction of this calculation is appeared in Fig. 2 embraced from (IPSec Developers Forum, n. d.). For UDP stream, the mentioned data transfer capacity is thought to be the encoding pace of the codec.

For TCP streams, the mentioned data transfer capacity is determined as record size/speed of administration necessity. The outcome is then sent to PSM where a cracked container calculation is utilized to direct the traffic. An elective method to decide the mentioned transmission capacity for TCP streams would be to deterministically dole out a fixed worth. We also note that the congestion algorithm is run as part of the data transmission algorithm. Suppose a high priority flow (e.g., a flash overwrite stream) demands for affirmation and the blocked banner is on lower need streams may should be appropriated to oblige the higher need call as commanded by the congestion policy. When the "congested" flag is set by the measurement device, the congestion algorithm is triggered to preempt existing flows congestion algorithm is shown in Fig. 3 in which two examples of congestion policy are presented. We note that the congestion policy can be set by the network operator dynamically, according to the need of the underlying mission.

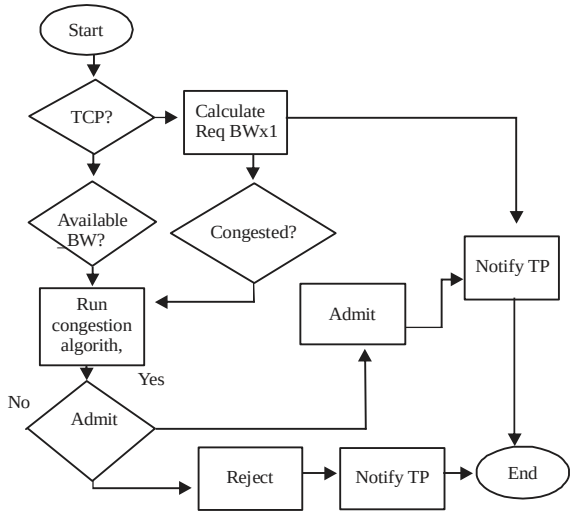

Fig. 4: CCA when available bandwidth can be obtained through bandwidth estimation techniques

Via cautiously watching (Fig. 2), we note that the information transmission calculation shows a solid "responsive" nature, for example, traffic will be conceded until blocked state is proclaimed. In the event that the "accessible transfer speed" can be resolved through transfer speed estimation methods, the information transmission calculation can be made progressively "proactive" to be specific, traffic streams are dismissed before blockage is watched. In a buddy paper, amazing transmission capacity estimation procedures are introduced with the end goal that the bottleneck connect transfer speed (characterized as the connection with the littlest measure of data transfer capacity along the way) and accessible transmission capacity (characterized as how much bandwidth "headroom" along the way for new traffic) are evaluated. They would then be able to be utilized in the information transmission as appeared in Fig. 4. Our investigation demonstrated that utilizing data transfer capacity estimation; blockage shirking can be adequately accomplished.

We used the same components of the model in Fig. 1 to validate the ITA but with implementing information transmission algorithm/congestion algorithm and without data transmission/congestion algorithm to study the behavior of the system in both experiments.

CONCLUSION

In this research paper, we introduced an algorithm to enhance and upgrade the security, privacy and confidentiality of information for those governmental requests that need a high degree of secrecy and confidentiality as well as an algorithm for managing electronic service requests in the Jordanian E-government to avoid congestion, distribute requests and load in such a way to prevent congestion, infinite postponement and circular waiting.

REFERENCES

01. Alhaj, A., S. Aljawarneh, S. Masadeh and E. Abu-Taieh, 2013. A secure data transmission mechanism for cloud outsourced data. Int. J. Cloud Appl. Comput. (IJCAC.), 3: 34-43.
02. Aljawarneh, S., 2013. Cloud Security Engineering: Avoiding Security Threats the Right Way. In: Cloud Computing Advancements in Design, Implementation and Technologies, Aljawarneh, S. (Ed.)., IGI Global, Pennsylvania, pp: 147-153.
03. Aljawarneh, S.A., R.A. Moftah and A.M. Maatuk, 2016. Investigations of automatic methods for detecting the polymorphic worms signatures. Future Gener. Comput. Syst., 60: 67-77.
04. Awan, M.A., 2008. Dubai E-government: An evaluation of G2B websites. J. Internet Commerce, 6: 115-129.
05. Al-Omari, H., 2006. E-government architecture in Jordan: A comparative analysis. J. Comput. Sci., 2: 846-852.
06. Barnes, S.J. and R. Vidgen, 2003. Measuring web site quality improvements: A case study of the forum on strategic management knowledge exchange. Ind. Manage. Data Syst., 103: 297-309.
07. UNDE. and SADPADM., 2008. UN E-Government Survey 2008: From E-Government to Connected Governance. United Nations, New York, USA., ISBN:978-92-1-123174-8, Pages: 225.
08. Kotler, P. and G. Armstrong, 1994. Marketing Management: Analysis, Planning, Implementation and Control. 8th Edn., Prentice Hall, New York.
09. Devargas, M., 1993. Network Security. NCC Blackwell, Manchester, UK.,.
10. Aljawarneh, S., M. Dababneh, H. Hosseny and E. Alwadi, 2010. A web client authentication system using smart card for E-systems: Initial testing and evaluation. Proceedings of the 2010 4th International Conference on Digital Society, February 10-16, 2010, IEEE, St. Maarten, pp: 192-197.
11. Raghuram, S.S. and C. Chakrabarti, 2000. A programmable processor for cryptography. Proceedings of the 2000 IEEE International Symposium on Circuits and Systems (ISCAS) Vol. 5, May 28-31, 2000, IEEE, Geneva, Switzerland, pp: 685-688.

12. Wang, W., Z. Li, R. Owens and B. Bhargava, 2009. Secure and efficient access to outsourced data. Proceedings of the 2009 ACM Workshop on Cloud Computing Security, November 9-13, 2009, ACM, Chicago, Illinois, ISBN: 978-1-60558-784-4, pp: 55-66.
13. Anderson, R.J., 2001. Security Engineering: A Guide to building Dependable Distributed Systems. 1st Edn., John Willey, UK., ISBN-10: 0471389226, pp: 640.
14. Dasarathy, B., S. Gadgil, R., Vaidyanathan, K. Parmeswaran, B. Coan, M. Conarty and V. Bhanot, 2005. Network qos assurance in a multi-layer adaptive resource management scheme for mission-critical applications using the corba middleware framework. Proceedings of the 11th IEEE Real Time and Embedded Technology and Applications Symposium, March 7-10, 2005, IEEE, San Francisco, California, pp: 246-255.