SCIENCE PROCEEDINGS SERIES

http://readersinsight.net/SPS

LIGHTWEIGHT AUTHENTICATION TECHNIQUE FOR SECURE COMMUNICATION OF EDGE/FOG DATA-CENTERS

Muktar Yahuza*

Departement of Computer System and Technology
University Malaya
Malaysia
mukyahuz@gmail.com

Yamani Idna Bin Idris

Departement of Computer System and Technology
University Malaya
Malaysia
yamani@um.edu.my

Ainuddin Wahid Bin Abdul Wahab

Departement of Computer System and Technology
University Malaya
Malaysia
ainuddin@um.edu.my

Mahdi A. Musa

Departement of Computer Science
Yobe State University Damaturu
Nigeria
mahdiamusa@gmail.com

Adamu Abdullahi Garba

Departement of Software Engineering
University Technologi Malaysia
Malaysia
adamugaidam@gmail.com

***Corrosponding author's Email:** mukyahuz@gmail.com , ainuddin@um.edu.my*

Peer-review under responsibility of 4th Asia International Multidisciplinary Conference 2020 Scientific Committee
http://connectingasia.org/scientific-committee/

SCIENCE PROCEEDINGS SERIES

http://readersinsight.net/SPS

Abstract

Edge computing has significantly enhanced the capabilities of cloud computing. Edge data-centres are used for storing data of the end-user devices. Secure communication between the legitimate edge data-centres during the load balancing process has attracted industrial and academic researchers. Recently, Puthal et al. have proposed a technique for authenticating edge datacenters to enable secure load balancing. However, the resource-constraint nature of the edge data-centres is ignored. The scheme is characterized by complex computation and memory intensive cryptographic protocol. It is also vulnerable to key escrow attack because the secret key used for encrypting and decrypting of the communicated messages is been created by the trusted cloud datacenter. Additionally, the key sharing phase of their algorithm is complex. Therefore, to address the highlighted challenges, this paper proposed a lightweight key escrow-less authentication algorithm that will ensure secure communication of resource-constrained edge data-centres during the load balancing process. The security capability of the proposed scheme has been formally evaluated using the automatic cryptographic analytical tool ProVerif. The relatively low computation and communication costs of the proposed scheme compared to the benchmark schemes proved that it is lightweight, thus suitable for resource-constrained edge datacenters.

Research Objectives

The edge data-centres, which are the key components of an edge network, are resource-constraint, characterized by limited memory, and low processing capacity (1). In an edge network, vital, and real-time data are being communicated between the participating EDC_s through an insecure communication channel. Therefore, the aim of this research is to develop a lightweight authentication scheme that will ensure mutual authenticity and integrity of the participating EDC_s for the privacy and security of the communicating data to be determined. Considering the resource-constraint features of the EDC_s, used of conventional cryptographic protocols is eliminated for developing the authentication protocols due to large number of keys involved, and high costs of communication and computation required.

After thorough investigation of Puthal et al technique for ensuring secure communication of edge data-centres during the load-balancing process, some drawback where found. Therefore in this paper, a lightweight authentication free from all the drawbacks of Puthal et al technique is proposed. The security of the proposed technique was systematically evaluated using ProVerif tool and also using informal methods as descriptive. Besides, the lightweight aspect of the proposed scheme was measured by contrasting the scheme's computation and communication cost with the selected bench-marking schemes.

SCIENCE PROCEEDINGS SERIES

http://readersinsight.net/SPS

Methodology

i. Initialization Phase

In this stage, all the parameters required for establishment of authentication between the genuine Edge Datacenters is selected by Key generation centre (KGC). Then KGS securely send all the selected parameters to the genuine edge datacenters (EDCs) including its public key, while keeping its secret key private.

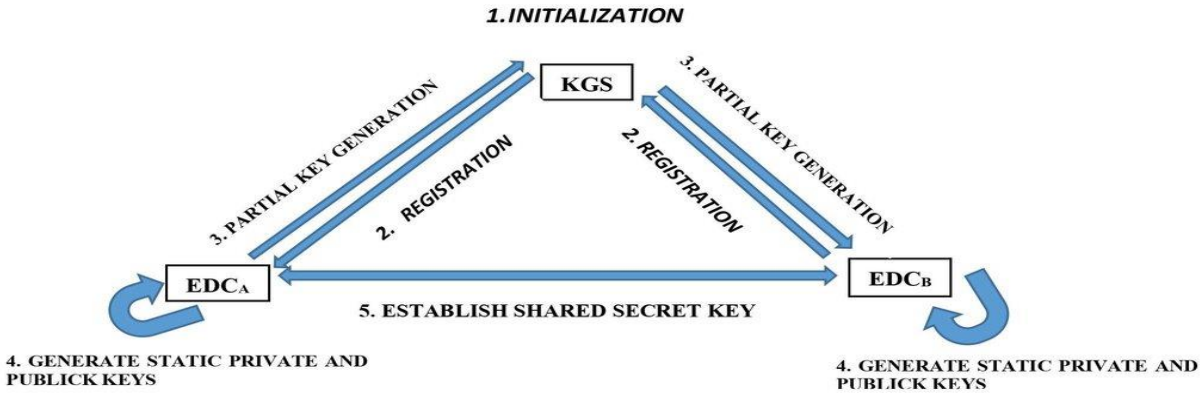

Fig.1: The Methodology

ii. Registration Phase

EDC_x that want to participate in the load balancing register itself with the KGS

iii. Partial Private Key Generation Phase

When KGC recive the registration request, it generates a partial private key (Y_x, U_x) to the EDC_x.

iv. Static Private Key Generation Phase

When EDC_x receive (Y_x, U_x) from KGS, it computes its static private key as $Sx = Lx + Yx$, and equivalent static public key as $Px = Sx * G$. Therefore any genuine EDC in the Fog/Edge network will verify the public key as $Sx * G = Ux + H_1[IDx \,||\, Ux] * P_{KGS}$. This will prevent any adversary from assuming the public key of EDC_x.

v. Shared Secret Session Key Establishment (Authentication) Phase

In this phase, two EDCs, e.g. EDC_A, and EDC_B that want to undergo load balancing will, first of all, authenticate one another by agreeing on a common shared secret session key $SSSK_{AB}$

SCIENCE PROCEEDINGS SERIES

http://readersinsight.net/SPS

Results

The proposed scheme is proved to be secure against all the possible attacks under , a well-accepted Canetti-Krawczyk (CK) adversarial mode.The security strength of the proposed scheme is formally investigated using the automated protocol verifier tool called ProVerif is employed. The advantage of using this tool as compared to other similar tools is that it has many features which enable it to handle many different cryptographic primitives (2). Most importantly, the tool is capable of modelling an infinite amount of parallel session (3). The result of the analysis is depicted in figure 2. The results of the query, not attacker indicating true, shows that the ephemeral secrets, private keys, as well as the shared secret session key, are not compromised in any way by the adversary. Moreover, the query **inj-event** result indicating true signifies that both $EDC_{A,}$ and, EDC_B achieve mutual authentication.

When compared with the benchmarking schemes, the proposed scheme is having appropriate communication cost as well as robust to several attacks. Additionally, better communication cost is provided by the proposed scheme as compared with the benchmarking schemes.

Findings

This research paper first analyzes the technique of Puthal et al (4), and has been found that the technique is not lightweight, and is vulnerable to key-escrow attack. Secondly, an authentication technique free from all the problems identified from Puthal et al (4) is proposed. The findings showed that the technique proposed would withstand all the attacks under the Canetti-Krawczyk adversarial model. It was shown that the proposed scheme outperforms most of the schemes interms of costs of computation and communication. Therefore, the proposed scheme established a balance between lightweight feature and security efficiency.

Acknowledgement

This research is partially funded by the University of Malaya Impact Oriented Interdisciplinary Research Grant (IIRG008A, B, C-19IISS), and Ministry of Education-Fundamental research Grant scheme (MOE-FRGS (FP072-2019A))

References

[1] Hong C-H, Varghese B. Resource management in fog/edge computing: a survey on architectures, infrastructure, and algorithms. ACM Computing Surveys (CSUR). 2019;52(5):1-37.

SCIENCE PROCEEDINGS SERIES

http://readersinsight.net/SPS

[2] Mahmood K, Chaudhry SA, Naqvi H, Kumari S, Li X, Sangaiah AK. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Generation Computer Systems. 2018;81:557-65.

[3] Blanchet B, Smyth B, Cheval V, Sylvestre M. Proverif 1.86 pl3: Automatic cryptographic protocol verifier, user manual and tutorial. 2012.

[4] Puthal D, Ranjan R, Nanda A, Nanda P, Jayaraman PP, Zomaya AY. Secure authentication and load balancing of distributed edge datacenters. J Journal of Parallel Distributed Computing 2019;124:60-9.

Author's Biography

MUKTAR YAHUZA *Received the B.Eng. degree in Computer Engineering from Bayero University Kano, Nigeria in 2010, and MSc in Computer Information and Engineering from International Islamic University Malaysia (IIUM) in 2015. He is a lecturer at Yobe State University Damaturu Nigeria. He is currently undergoing the PhD degree in Computer Science at University Malaya, Malaysia.*

His area of research include Smart Environment Authentication, Information Security, and, Image processing.

MOHD YAMANI IDNA BIN IDRIS *Received the B.E. MSc, and PhD degrees in Electrical Engineering from the University of Malaya, Kuala Lumpur Malaysia.*

He is currently an Associate Professor with the Department of Computer Systems, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia. He is the author of a book, more than 110 articles in reputable Journals, and more than 20 inventions. His research interests include Information Security, Embedded Systems (System on Chip, FPGA), Image Processing and Computer Vision, Digital Forensics, Surveillance Systems, Digital Signal Processing (Speech Processing, and Bio-Signals), and Wireless Sensor Network.

AINUDDIN WAHID BIN ABDUL WAHAB *Received the BSc, and MSc degrees in Computer Science from the University of Malaya, Kuala Lumpur Malaysia, and the PhD degree in Multimedia Network from Surrey University, UK.*

He is currently working as an Associate Professor, and Deputy Dean (Undergraduate) with Department of Computer Systems, Faculty of Computer Science and

SCIENCE PROCEEDINGS SERIES

http://readersinsight.net/SPS

Information Technology, University of Malaya, Malaysia. He published more than 90 articles in reputable Journals. His area of expertise include Information and Network Security, Information hiding, Digital Forensics, and Sensor Network. He is an Associate Editor of Elsevier Journal of Information security and Applications (JISA).

MAHDI A. MUSA *Received the BEng degree in Electrical Engineering from Bayero University Kano, MSc and PhD degrees in Computer Science at Faculty of Computer science and information system University Technology Malaysia.*

He is currently working as the Head of Department of Computer Science, Faculty of Science, Yobe State University Damaturu Nigeria. He published more than 20 articles in reputable Journals. His area of expertise include innovative solutions for "knowledge-based" information systems that span several areas applying ontology and knowledge management for interoperating information systems, e-learning and M-learning.

ADAMU ABDULLAHI GARBA *Is a Ph.D. Student at Universiti Teknologi Malaysia, and an Assistant lecturer at Yobe State University Damaturu Nigeria. He acquired his first degree at the University of East London in Software Engineering in 2013 and Master in Computer Science at Universiti Teknologi Malaysia in 2015. His current research interest is information security, cybersecurity, and database management. He is a member of Information Assurance and Security Research Group (IASRG), Department of Computing Faculty of Engineering Univerisiti Teknology Malaysia (UTM).*