Advances and Applications in Mathematical Sciences
Volume 20, Issue 11, September 2021, Pages 2689-2692
© 2021 Mili Publications

UNINTENTIONAL OUTFLOW OF CONFIDENTIAL DATA SEVERE SECURITY ORGANIZATIONS IN DIGITAL AREA

M. S. V. V. RAMESH and M. S. R. S. PRASAD

Assistant Professor
Department of Computer Science and Engineering
Pragati Engineering College
Affiliated to JNTUK
Surampalem, India

Ideal Institute of Technology
Affiliated to JNTUK
Kakinada, A.P., India
E-mail: rameshmerla@gmail.com
prasadmerla@gmail.com

Abstract

We produce LIME, one for charged with low frequency across more than one entities. We present a standard proof progeny formulate activity (LIME) that results drift transversely a couple of entities. In several instances, tag of the leaker is observed due to rhetorical techniques. The proposed methods will discover the simplified non-repudiation and loyalty assumptions of the prototype. Then estimated measures will be spread at intervals of two entities. Generally, the LIME approach is more suitable for radio band, to turn into a key walk vis-à-vis achieving liability voluntarily. The very important feature about the prototype is it enforces answerability explicitly.

I. Introduction

The internal servers and public serves needs security for the sensitive data [1]. To provide the security, the automated procedure is demanded in now a days for providing the security from the hackers. The servers auditing

2010 Mathematics Subject Classification: 62-07.

Keywords: accountability; fingerprinting; oblivious transfer; watermarking; information leakage; data lineage; public key cryptosystems.

Received October 12, 2020; Accepted November 4, 2020

process is also demanded for identifying the problems in the network. The security of the network majorly focuses on the identification of vulnerabilities [2]. These vulnerabilities will make the malfunctioning of the network and its database. The capacity of the network is found to be enhanced with millimeter wave based communication [3]. It includes the opportunistic relay. This relay is used for connection and secrecy outage probability. The security for the digital includes the coverage of leakage of sensitive information [4]. For this, the data lineage approach is introduced to provide the security. An accountable data transfer protocol is needed further for the development of the process. The theft of sensitive information leads to Data ex-filtration [5]. The existing sandbox approaches are failed to provide the security for the networks. The role based privilege isolation protocol is found to be prominent for the data security. The security for the RFID based networks requires additional measures for providing the security [6]. The Confidential Synchronized Anti-Tag Cloning approach is found to be efficient for RFID based networks. It involves the estimation of Synchronous Secret measures. The security environment for the network includes the encryption mechanism [7]. Among various encryption techniques, ElGamal technique is found to be efficient. It is found to be prominent for intrusion detection system. The security for Internet of Things (IoT) based networks is demanded in now a days [8]. The security should be provided between machines for communication.

II. Methodology

The architecture of the proposed system is shown in Figure 1.

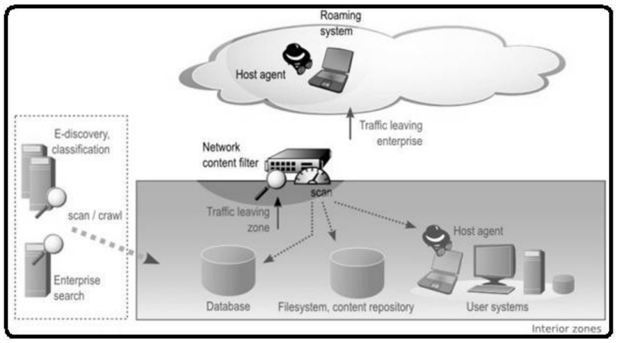

Figure 1. System Architecture.

The security of the network by using LIME is shown in Equation (1).

$$\sum_{i}^{M} P(i) \log \frac{P(i)}{Q(i)}. \tag{1}$$

The approach uses the KL regularizer for anomaly contribution.

III. Results and Discussions

The proposed method is compared with the existing methods and the results are shown in Figure 2. The results indicate the efficacy of the proposed method.

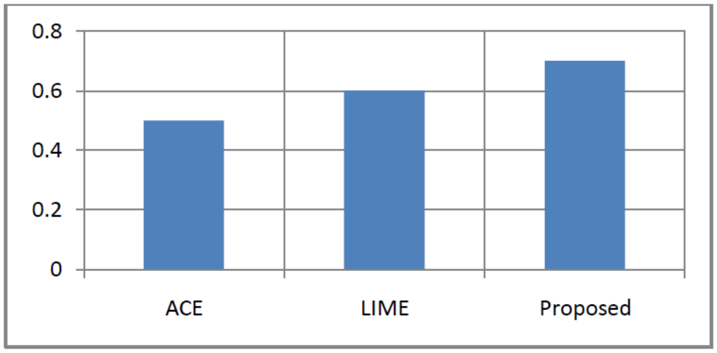

Figure 2. Comparison of Proposed and existing methods.

From the results, it is evident the proposed method is having efficient performance measure than the existing ACE and LIME methods.

IV. Conclusion

We produce LIME, one for charged with low frequency across more than one entities. We present a standard proof progeny formulate activity (LIME) that results drift transversely a couple of entities. In several instances, tag of the leaker is observed due to rhetorical techniques. The proposed methods will discover the simplified non-repudiation and loyalty assumptions of the prototype. Then estimated measures will be spread at intervals of two entities. Generally, the LIME approach is more suitable for radio band, to turn into a key walk vis-à-vis achieving liability voluntarily. The very important feature about the prototype is it enforces answerability explicitly.

The existing ACE and LIME methods are suffers with problem of sensitive information leakage. To overcome this problem, the present paper proposes a novel approach based on LIME for enhancing the performance of the network. The results indicate the efficiency of the proposed method.

References

[1] S. Patra, N. C. Naveen and O. Prabhakar, An automated approach for mitigating server security issues, 2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT), Bangalore (2016), 1075-1079 doi: 10.1109/RTEICT.2016.7807996.

[2] B. Kumar and M. Hamed Said Al Hasani, Database security-Risks and control methods, 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI), Wuhan, 2016, pp. 334-340, doi: 10.1109/CCI.2016.7778937.

[3] S. Wang, K. Huang, X. Xu and S. Zhang, On the Reliability and Security Performance of Opportunistic Relay Selection in Millimeter Wave Networks, 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 2018, pp. 1-6, doi: 10.1109/VTCFall.2018.8690612.

[4] M. Backes, N. Grimm and A. Kate, Data Lineage in Malicious Environments, in IEEE Transactions on Dependable and Secure Computing 13(2) (2016), 178-191, 1 March-April 2016, doi: 10.1109/TDSC.2015.2399296.

[5] B. Das, L. Maddali and H. Vani Nallagonda, Role-based privilege isolation: A novel authorization model for Android smart devices, 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 220-225, doi: 10.1109/ICITST.2015.7412093.

[6] B. Patel, G. Ramesh, S. Karna and A. Razaque, Confidential Synchronized Anti-Tag Cloning for securing Radio Frequency Identification communication, 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, 2016, pp. 1-6, doi: 10.1109/LISAT.2016.7494154.

[7] K. E. A. Negm, Design, implementation and testing of mobile agent protection mechanism for MANETS, The 3rd ACS/IEEE International Conference on Computer Systems and Applications, 2005, Cairo, 2005, pp. 98, doi: 10.1109/AICCSA.2005.1387089.

[8] S. Chowdhary, S. Som, V. Tuli and S. K. Khatri, Security solutions for physical layer of IoT, 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, 2017, pp. 579-583, doi: 10.1109/ICTUS.2017.8286075.