Applying AI Concepts for Identity and Access Management in Cloud Environments

Leandro R. Maciel and Vibhu Dhakal
NYU Tandon School of Engineering
New York University
lrm371@nyu.edu and vd2099@nyu.edu

***Abstract*—Virtualization of computers and network functions is an inexorable part our society's future. The recent unfortunate pandemic situation further accelerates the need for remote operations, artificial intelligence and digital employees (DEs). One of the greatest challenges of this digital transformation is managing digital identities and access control for cloud users, both humans and machines (including DEs). This short paper brings Artificial Intelligence (AI) concepts to the task of the Identity and Access Management (IAM) ubiquitous need. The approach is preliminarily a forensic behavioral analysis of employee's access to a specific application (in this case, a portal for cloud orchestration), to later apply the knowledge obtained by this cybersecurity software, to control real time the access of users (humans or DEs). The result is expected to be an additional IAM tool, joining forces with MFA (Multi Factor Authentication), CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), and similar IAM techniques.**

***Index Terms*— *Identity and Access Management, IAM, Cloud Computing, Security as a Service, Artificial Intelligence, AI*.**

I. Introduction

THE problem we are trying to solve is how to increase the efficiency of a Multi Factor Authentication (MFA) controlling access to cloud resources. Authentication is currently based on "what one knows" (password, etc.), "what one is" (biometric), and "what one has" (smartphone, token, etc.), including a combination of these three authentication processes. A successful approach is the Two Factor Authentication (TFA, or 2FA), combining in sequence a first authentication via "what one knows" (password), and subsequently a second based on "what one has" (smartphone or a token) [1]. By applying AI concepts, i.e., the collection and intelligently processing information from previous system usage, the user identification could be obtained based on observed behavior. If successful, there will be no need to send any additional interactive authentication. If unsuccessful, a 2FA steps could be used to assure accuracy in the authentication process. Regarding the paper structure, Section II describes the related work and possible improvements. In Section III, a use case is presented. Section IV includes the proposed solution with the respective metrics to validate the approach. Section V drills into the data obtained by the developed code over the cloud orchestration portal, and the comparison with defined metrics. A conclusion is presented in section VI, where future work is suggested for additional automation in this IAM area.

Paper submitted for review on December 13th, 2020, as part of the Information Security & Privacy CS-GY 6813 Fall 2020 course deliverable.

Leandro R. Maciel and Vibhu Dhakal are students in the Master of Science in Cybersecurity at NYU, Cyber Fellow at NYU.

II. Related Research

Current solutions available for MFA require evolution, as consequence of the Digital Transformation [2], [3]. With more remote users, DEs (Digital Employees), and a fast-growing number of IoT (Internet of Things) devices, an authentication process for virtual assets (cloud) needs to be more efficient, and faster. Three-factor authentication has been suggested, using facial recognition as the intermediary biometric step [4]. But it would not apply for DEs or IoTs. Recent data analytics tools using the concept of User and Entity Behavior Analytics (UEBA), have provided initial empirical positive results [5]. On a special note, BeyondCorp, a zero-trust centralized policy enforcement front end access control, based on information about a device, its state, and its associated user, has been successfully implemented by Google [6].

The concept of Behavior Based Continuous Authentication (BBCA) has gotten traction and reliable results when applied to humans, specially related to mobile users (e.g., smartphones) [7]. This encouraging positive results on humans could be expanded for a continuous authentication of DEs and IoTs as well. So, differently from existing publications, this research studies the specific application of BBCA to a cloud orchestration portal (COP), to authenticate humans, DEs and IoTs, culminating with a possible coexistence with CAPTCHA, other biometric authentication tools and the two-factor or multi-factor authentication.

III. Motivating Example

The typical credit card usage blocking issue, when a financial institution waits for a SMS confirmation, or an email for validating a simple web transaction, are usability issues that could be avoided by intelligent and continuous authentication systems. As digital transformation requires more and more remote access to virtual assets in the cloud, a use case is presented here, where a forensic analysis of user behavior is implemented, applied to a portal for cloud orchestration. A subsequent step is achieved by applying the resulting user collected behavior, a user's typical event access list, into a reference database for future comparison. Deviation from, or compliance to this target will provide criteria for continuous authentication for humans, DEs and IoTs.

IV. Hypothesis and Sample Metrics

By adding an intermediate AI BBCA layer, between the two typical FAs (e.g., 1st FA password and 2nd FA SMS), and removing the second FA, one could efficiently improve the speed of authentication. Additionally, one could incorporate DEs and IoTs "behaviors", increase usability and significantly reduce the cost of operation (e.g., reducing time, the need of a SMS, or the cost of token devices. One last authentication step, e.g., the use of SMS, could be used only as a safety net, in case the algorithm is unable to identify the user from the AI based continuous authentication. This provides robustness to the envisioned system, as in Figure 1.

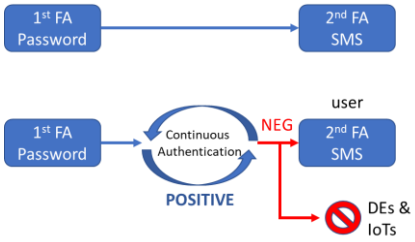

Fig. 1. Continuous authentication using AI for user behavior identification.

The metric used here is a "stability" concept, i.e., how fast a user achieves a clearly defined profile, or converging to a typical event list. In the case of a COP, a user (human, DEs or IoT device), accesses into the portal and executes events. Sample of event includes, logging in, creating a virtual machine (VM), optimizing VMs, changing credentials, creating reports, etc. After a stability is achieved, and a template is created, future metrics to validate authentication success should be a typical statistical analysis of binary classification: the F1-score, considering false positives (fp) and false negatives (fn) [8].

V. Empirical Evidences / Discussion on Results

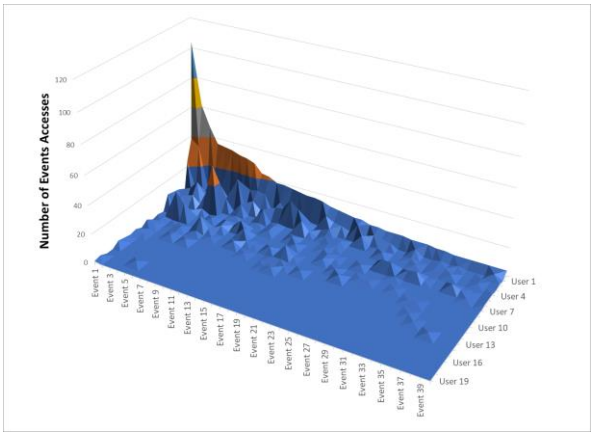

Figure 2. Empirical Evidence: associating users, events and # of accesses.

The first evidence obtained was the confirmation that a typical user gravitates to a specific list of events. Not all users execute the same commands, although some are basically common (such as login). Figure 2 shows the result from an experiment of tracking the activities in the COP for 2 months, showing 19 users, top 39 events, and the number of accessed events. There is a clear user separation by the behavior, i.e., which event is being accessed. For instance, User 1 is very active while User 19 probably just logged in to see a report. The next question was how fast could we achieve a typical event list per user. Figure 3 shows a "stability" metric comparing 3 users. As seen before, User 1 is quite active and uses the COP extensively, while User 3 only uses a small subset of the COP and rapidly converged to the list.

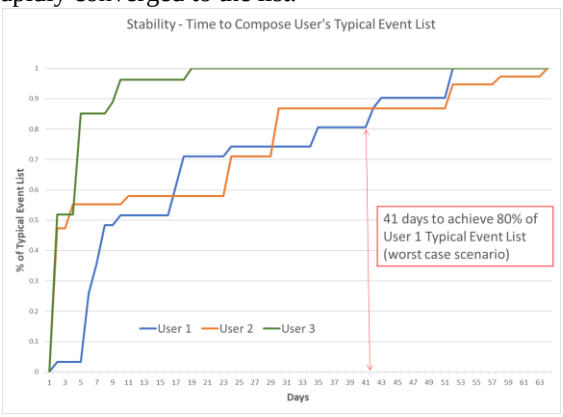

Figure 3. Stability – Time to create Reference / Typical Event List per User.

VI. Conclusion and Future Work

This paper presented the feasibility of reducing the need for MFA, while increasing security, by using BBCA applied to a cloud orchestration portal. The code implemented considers user event accesses, previously collected, to create a reference, then identify any user deviation to the norm, triggering an additional factor authentication, if needed. Future work is envisioned not only mapping user behavior based on event activity, but also creating a template for user requester IP, triggering MFA when detecting abnormal user IP addresses (unusual country origin).

VII. References

[1] A. Derhab, M. Belaoued, M. Guerroumi, and F. A. Khan, "Two-Factor Mutual Authentication Offloading for Mobile Cloud Computing," IEEE Access - Digital Object Identifier 10.1109/ACCESS.2020.2971024, February 2020.

[2] N. Naik and P. Jenkins, "A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards," 4th IEEE International Conference on Mobile Cloud Computing, Service and Engineering, 2016.

[3] G. Dreo, M. Golling, W. Hommel and F. Tietze, "ICEMAN: An Architecture for Secure Federated Inter-Cloud Identity Management," 5th International Workshop on Management of the Future Internet (ManFI), IFIP/IEEE IM, 2013.

[4] W. Kennedy, A. Olmsted, "Three Factor Authentication," The 12th International Conference of Internet Technology and Secured Transactions (ICITST), 2017.

[5] B. Tang, Q.J. Hu, D. Lin, "Reducing False Positives Of User-to-Entity First-Access Alerts for User Behavior Analytics," IEEE DOI 10.1109/ICDMW, 2017.

[6] R. Ward and B. Beyer, "BeyondCorp: A New Approach to Enterprise Security,' https://www.usenix.org, ;login: issue: December 2014, Vol. 39, No. 6.

[7] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective," IEEE Internet of Things Journal, VOL. 7, NO. 9, September 2020.

[8] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. Nyang "AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors," IEEE IoT Journal, VOL. 7, NO. 6, June 2020.