Prototype for Testing Context-Aware Authentication for Cloud Environments

Claudio Augusto N. Ferraz[1], Edgard Costa Oliveira[1], Ari M Mariano[1], Altino J M Moraes[2]
Postgraduate in Applied Computing, University of Brasília, UNB, Brasília, Brazil[1]
Doctorate in Production Engineering, Paulista University, UNIP, Brazil[2]

Abstract

Access to data in pervasive or ubiquitous environments by people and organizations still uses traditional, static or inappropriate methods. With the adoption of cloud computing, the concern of governments and proven companies to prevent digital fraud and data leakage becomes even more important, new laws establish the need to strengthen the protection of personal data held by organizations. Thus, it is recommended that these organizations carry out risk management in Cloud Computing considering the control and management of identities and access to data and information. Identity and Access Management - IAM - is a set of technologies and policies to address risks of improper access. One of the IAM technologies is context-sensitive authentication, which is an adaptive control technology that uses dynamic standards to determine the legitimacy of access. This article proposes the use of context-sensitive authentication as an Identity and Access Management technology to provide greater protection in accessing data in a cloud environment and also demonstrate the functioning of this technology through the construction of a prototype. The prototype will use context authentication to validate accesses through attributes that form an access profile to be validated by a given application.

1. Introduction

Information and data entered into organizations' digital systems and services must be protected against fraud and identity and access attacks that affect the confidentiality, integrity and availability of that information, especially sensitive data when information assets are migrated to the computing environment. in the cloud. On the other hand, cases of digital fraud and information leakage that affect any type of organization in the digital world are growing exponentially. Cybercrime crimes are proliferating in the digital world on a large scale and are increasingly sophisticated, as they constantly seek to exploit vulnerabilities in systems, technological architectures, protocols and digital services [1]. In a world that increasingly depends on a digital identity and services, in which many of the services of private companies or the government are only being offered on a digital platform, the need to worry about the security of data and information becomes exponential. In this context, the largest companies in the world, including technology, have already suffered from the action of digital criminals who access and hijack information using it illegally.

This reality is no different in the government that handles and stores personal and confidential information from companies and citizens, and when making services available in the digital world, you must ensure that these hacker actions do not compromise the reliability and availability of government digital services.

Information and data embedded in organizations digital systems and services must be protected against fraud and attacks. In order to offer digital services, the government and private companies also start to use cloud computing, which increases the challenge of protecting sensitive or confidential data. Recent legislation has emerged as a way of establishing guidelines and targets for dealing with risks and enforcing security controls, such as the General Data Protection Law (LGPD). With the adoption by the Federal Government of Brazil of the General Data Protection Law (LGPD), Law No. 13.709 of August 14, 2018 [2], which will come into force in August 2020, and which is very similar to GDPR (General Data Protection Regulation) [3] in force in Europe since May 25, 2018, it seeks to bring greater rigor to the way private companies and government agencies deal with citizens' privacy and data protection issues. The new rules will affect all activities involving the use of personal data by organizations, which have until 2020 to adapt. The rules seek to protect data from vulnerabilities and leaks of data and information.

Identity management and access control are solutions of great importance to prevent non-legitimate access, creating increasingly effective controls for the protection of information assets, both of which are part of a set of technologies and processes aimed at protecting identity and accesses, which is called Identity and Access Management (IAM). Identity and Access Management refers to the “technologies, processes, policies and support infrastructures necessary for the implementation, control and maintenance of digital identities and access to its resources” [4]. The IAM solution combines policies and technologies to address risks such as improper access, illegitimate identities and excessive privileges. These are solutions that hinder digital fraud by strengthening access technologies and new types of verification of user behavior or access context when trying to authenticate themselves to use a particular digital service.

Context-sensitive or behavior-based authentication is a technology that transparently authenticates the user from their access context or behavioral profile, it has a dynamic operation to adapt to changes in the access profile in the authentication process of users and establishes an additional layer of security, which can be used with other authentication mechanisms.

Data protection initiatives by companies and citizens and the mitigation of information security risks are extremely important for the security of the digital systems and services platform and for the digital transformation and reducing the bureaucracy of digital organizations processes.

2. Risk Management for Cloud Environments

A well-designed Risk Management model is crucial to ensure that information is at the same time available, protected and secure. Business processes and procedures need to take security into account, and information security managers need to adjust their security policies and procedures to meet business needs. An example of a cloud computing risk that needs to be managed is third party access to sensitive information, as it creates a risk of compromising confidential information.

Although cloud computing reduces the overall scope of security and does not require customers to manage part of the computing stack in a shared responsibility model, this is a good opportunity for new types of approaches and the adoption of new methods to protect information. The cloud will require a different approach to security - the security habits and designs of the local storage structure do not work well for information stored in the cloud because it is another environment with other Information and Communications Security policies and technologies. Organizations should not assume that using a cloud service means that everything they do within that cloud will be secure. Security requirements should be given greater attention with the use of cloud computing, as in addition to the traditional security controls of local infrastructure, cloud service providers and their customers must be more concerned with internal and external access control and the leakage of information shared and available in a cloud environment.

The National Institute of Standards and Technology (NIST) [5] points out that cloud computing refers to a practical model for enabling network access to a shared set of configurable on-demand computing resources (eg, networks, servers, storage, applications and services) that can be quickly provisioned and released with minimal management effort or interaction with the service provider. According to ISACA [6] third party access to confidential information creates a risk of compromising that information. In cloud computing, this can compromise intellectual property protection and trade secrets. One of the biggest challenges for governments in adopting cloud computing and for Digital Government is to protect sensitive, restricted or sensitive information from service systems and portals against digital fraud and information leakage [7]. According to [8] computational security presents itself as an indispensable resource to ensure access in Cloud Computing environments, and emphasizes the protection of privacy, since sensitive data is now in the custody of third parties. In this context, identity management grows in importance as services need to use authentication and authorization to control user access. The process of establishing a user identity is known as identification and authentication. The goal is to have only authorized users accessing a computer system, network or specific service. In the Identity and Access Management (IAM) solution, user behavior is monitored and analyzed against established access rights to identify excessive privileges or abnormal access. This is true for all types of users and accounts, including privileged users and service accounts. The below capacity model, published by Gartner [4] for Online Fraud Detection (OFD) solutions, which are technologies that work against fraud prevention, points to Behavior Analysis as one of the main factors to combat fraud and information hijacking.

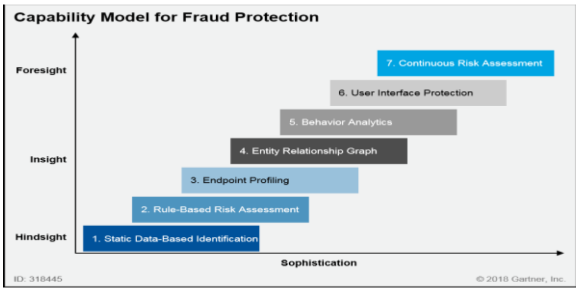

Capability Model for Fraud Protection
Foresight
Insight
Hindsight
7. Continuous Risk Assessment
6. User Interface Protection
5. Behavior Analytics
4. Entity Relationship Graph
3. Endpoint Profiling
2. Rule-Based Risk Assessment
1. Static Data-Based Identification
Sophistication
ID: 318445
© 2018 Gartner, Inc.

Figure 1. Capacity model for OFD solutions [4]

Capacity model technologies more accurately detect identity attacks such as identity fraud. In addition, there is a shift away from spot fraud detection methods (eg, at enrollment) to a continuous risk assessment model based on identifiable precursor activities and non-transactional attributes of customer interaction.

As techniques become more sophisticated, methods emerge that detect historical patterns of fraud and try to prevent these patterns from becoming recurring. The trend is toward methods that provide insight and action-oriented intelligence about the risk of each customer interaction [9].

3. IAM Technologies

A range of solutions can be adopted to ensure the security of digital identities and network access, from software to policies to be followed by users, such as IAM technologies to address the risks of improper access and excessive privileges. IAM is an essential function for protecting information privacy, enhancing the user experience, enabling accountability and controlling access to an organization's assets. Identity management refers to the people, processes, and technology needed to manage the entire lifecycle of digital identities and profiles. Access management, also known as user permission management, refers to the processes and technology used to control access to a specific information asset provided by a specific identity. User permissions are sets of attributes that specify the access rights and privileges of an authenticated identity [10].

Identity and Access Management is a framework developed for business processes that ensures greater control for the registration and security of digital or electronic identities. The control offered by this structure allows the integration between technologies and policies to support access, especially for critical data. The protection offered by the IAM occurs through different authentication systems used together or in isolation: single sign-on, multifactor, a layer of protection and access management, added to a data governance process, which does not allow them to be shared at all, unless they receive authorization.

IAM uses some technologies such as Single Sign-On, which is a process that allows users to access multiple applications that require authentication by passing their credentials only once, and Federation that allows an organization to manage its users' identity and access to resources from partner organizations, but the main technology covered in this article is authentication.

3.1 Authentication

Authentication is the process of verifying the credentials of an entity that attempts to access a protected resource. Authentication must be secure, reliable and manageable. Authentication systems must have the ability to use the transaction risk definition as a guideline and provide adaptive authentication based on the transaction risk level. Adaptive authentication provides control based on the characteristics and behaviors of a dynamic access profile. Authentication is the process of verifying the identity or other attributes claimed by an entity or verifying the source of the submitted data. The entity can be a user, process, or device. Authentication happens every time we use our computers. Much of the authentication is transparent to the user and handled through computational communication processes without the user even realizing what is happening [10]. The most basic authentication approach is single factor authentication. Single-factor authentication is usually based on a reusable static password (something the user knows) in combination with a user ID. Passwords are a shared secret, known to the user and the system [10]. Single factor authentication, which is the case for user and password, is simple and although it has improved over time it is still a form of weak authentication, as the user needs to remember the password at all times and often write down the password itself, in addition to being able to be discovered through digital attacks, such as the brute force in which an algorithm tests the combinations until identifying the password and also the Social Engineering, where fraudsters ask users for their access credentials by means that they look legitimate.

The security of 2-Step Verification is based on your layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker can discover the user's password, it will be useless if he or she does not have the additional authentication method either. This works by requiring two or more authentication methods. In the figure below we have a graph showing on the horizontal axis the strength of the factor or combination of authentication factors and on the vertical axis the types of authentication: single, double or combined three factor authentication. We realize that the more factors combined, the greater the strength of authentication.

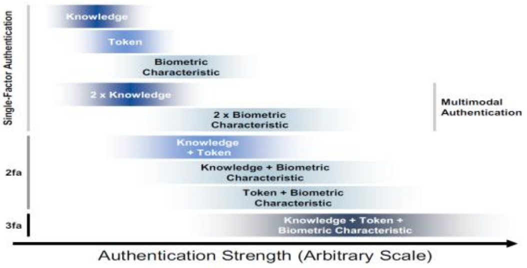

Single-Factor Authentication
Knowledge
Token
Biometric Characteristic
2 x Knowledge
2 x Biometric Characteristic
Multimodal Authentication
2fa
Knowledge + Token
Knowledge + Biometric Characteristic
Token + Biometric Characteristic
3fa
Knowledge + Token + Biometric Characteristic
Authentication Strength (Arbitrary Scale)

Figure 2. Authentication Strength [11]

Authentication approaches that depend on more than one factor are more difficult to compromise than single-factor approaches. Multi-factor authentication approaches combine something that a user knows, something that a user is, or something that a user owns. For example, a bank terminal transaction requires multifactor authentication: something the user has (ie, the card) combined with something the user knows (ie, his personal identification number - PIN). Multifactorial authentication, also known as strong authentication, can use several techniques to verify an identity.

Biometrics, as a multifactorial authentication technique, measures and analyzes the unique characteristics of each individual's human body for authentication purposes [10].

According to [12] authentication can be biometric using fingerprint and other body features that make it unique, biometrics can also be used on the behavioral aspect that uses, for example, the characteristics of how the individual uses the mouse or types on the keyboard.

Physical biometric authentication is static in nature and based on an individual's physical characteristics such as the face, fingerprint, iris and retina patterns. This type of authentication is very precise and difficult to compromise, but it requires the use of devices with sensors, scanners and readers of physical characteristics, specific software for collecting, transporting and managing credentials and a base for storing the physical characteristics of individuals. Behavioral biometrics is the measurement and recording of human behavioral patterns to verify and authenticate an individual computer user either in real time or retrospectively. Rather than focusing on the outcome of an activity, behavioral biometrics cares how a user conducts the specified activity. It does not check if the user name and password are entered correctly, for example, but how a user accesses: he is typing quickly or slowly, how he changes between system windows using the tab key or the mouse, how he uses the mouse and the keyboard.

On Time Password (OTP) are one-time passwords on a hardware device-based system. OTP systems create passwords that are valid for single use or for use within a specific time period [10]. The most important advantage that is given by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who is able to capture an OTP that has already been used to log in to a service or transaction will not be able to use it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems is not vulnerable on all of them, if the password for one of them is obtained by the attacker. However, OTPs are sent over the Internet to users' devices, and if passwords are captured by an attacker, access could be by an illegitimate user, this type of attack is often referred to as a man-in-the-middle attack, intercepts the information as it is being transmitted for unauthorized use.

3.2 Context-Aware Authentication

The emerging mobile computing paradigm makes it possible to access resources from anywhere, anytime. But at the same time that this ubiquitous access provides its benefits, it creates particular challenges to provide security to participating entities. Such challenges are not adequately addressed by traditional security approaches [13]. Traditional authentication mechanisms are ineffective in meeting the needs of highly dynamic environments such as mobile and pervasive environments [14]. Also, according to Babu and Venkataram [15], the effectiveness of most authentication mechanisms for mobile computing depends on the strength of the identifiers used for user authentication.

According to [13] context-aware authentication, which uses context-shifting to enable the adaptation of security mechanisms based on the current situation, is essential for providing effective security in pervasive environments.

Context-aware authentication utilizes a kind of digital identity of the individual through the correlation of behavioral properties or characteristics that form a profile of that individual. Contextual authentication can be used in conjunction with other authentication technologies as it is an additional layer or level for the security system. This type of technology works as if it were a person's digital DNA. This user profile can be formed by the correlation of various behavioral characteristics, geolocation and hardware used by the individual accessing a particular service or system.

Contextual or behavioral authentication has many advantages [16], including the ability to be continuously verified without user knowledge and to operate without additional hardware. For example, use of apps [17, 18] and location tracking can be employed for users with continuous authentication. Multifactor authentication, which requires two or more authentication factors, such as password, token, or requesting user characteristic, may be difficult because the use of some of these factors, which involve physical or static tokens, which are considered only as a peer point. inbound and do not perform continuous authentication, are susceptible to theft or loss, and do not consider providing continuous authentication for the entire access session. In addition to individual analysis of each of the above factors, a cross-analysis can be performed by correlating various factors and comparing them with the user's authentication activity history. These correlations are different combinations involving access device, geolocation, browser, operating system used, logical addresses, and time range, these characteristics create the user's behavioral access profile. The figure below shows the overall architecture of a context-based authentication system based on device attributes such as: Global Positioning System (GPS), timezone, installed applications, running processes and tasks, operating system description and version [19].

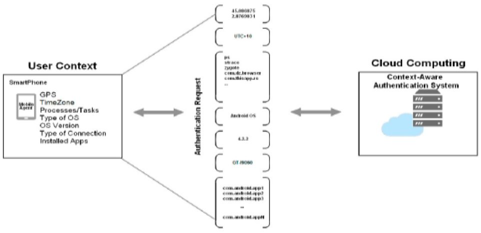


Figure 3. Context-Aware Authentication Architecture [19]

Behavior or context authentication analyzes the context in which authentication occurs and assesses the risk of an attempted identity theft and fraud. This analysis can be performed without affecting the normal user experience. It can enrich any authentication process in which a user name, password, tokens or other authentication factors are used. Therefore, it is especially useful in environments where it may not be possible to use stronger methods, for example, for usability reasons (as usually occurs in online shopping scenarios) or because the cost of implementing stronger methods (such as hardware OTP - One Time Password) that generate disposable passwords for use in a single access, or the cost of implementing large-scale biometric devices, can be prohibitive costs in certain scenarios, such as that of a system in a cloud environment that is accessed by users from different parts of the globe.

The system stores detailed information about all context factors of authentication processes. Also, when an anomalous situation is detected, the system generates an event that is logged in the audit system. This event can be converted to an alert or configured to enable an additional authentication factor, such as the knowledge-based factor to verify that the user owns the credentials. Thus, context analysis detects anomalies in authentication processes, increases the level of security provided by passwords or other factors combined, reduces the risk of identity theft or digital fraud, and offers a greater degree of confidence in protecting resources.

Authentication by context or behavior, which has as its main characteristic to be adaptive, works as an additional layer of security that manages from dynamic standards to validate the legitimacy of the access. Because it is adaptive it can work very well in cloud environments, which are eminently pervasive, which are characterized by ubiquitous computing and dynamic access, where users are predominantly mobile and can access applications from various locations around the globe. With the growth of cloud computing and internet businesses, this pervasive scenario is the most current. This technology is transparent to the user, as it automatically detects profile information, updates it, and compares it with the account profile information. It is also difficult to compromise, because in case of attempted fraud the system will be able to block accesses considered abnormal or suspicious. If combined with the authorization process, it becomes efficient in dealing with the risks of excessive privileges, as it will continuously check the users access rights in that particular login session to the system. As a result, authentication by context or behavior proved to be the most appropriate to combat attempts by digital frauds that can lead to loss of confidential data and the organization's image.

4. Prototype

This study implemented a prototype designed through a computational application routine based on Authentication by Context or Behavior. For this purpose, an access validation application was built based on some characteristics of this access profile, such as: source logical address range, browser type and operating system used during access. When comparing the elements that make up the access context, that is, the information of the IP address, browser and operating system used, that make up the access profile of that account, the application can allow or deny access, or even take some action for validation this access. For the prototype to be implemented, some requirements had to be met for the control mechanism to be effective. To contextualize the functioning of the application we describe an authentication architecture based on behavior or context.

Context Authentication solutions often have the authentication, validation, and challenge subsystems [20]. The authentication subsystem performs access control and validates user access from a known profile that is updated when the subsystem correlates factors as access account behavior evolves. The validation subsystem compares the access characteristics against the stored profile base to validate or not the access. The challenge subsystem generates acknowledgments when the validation subsystem considers access as suspect.

In the developed prototype, the access program takes care of verifying access by user and password and collects the input data to compare with the access profile, to validate this profile and consequently the access. The construction of a profile base is desirable so that its update is dynamic and can serve a pervasive computing environment. In the prototype, access is validated in a static way and compares the stored information with the access request information.

The prototype has access control and registered user accounts. Each account must have a profile and context base as per the validation controls provided below:

A. IP range
B. Operating system used for access
C. Browser used by access

The above attributes have been selected as they are commonly used and provide unique characteristics when combining the three factors, but attributes such as timezone, most accessed applications, unique device identifier where the application gathers device information can be used. access, making this digital identifier unique, among other attributes. The authentication system queries a base of IP addresses and a base or behavioral or context profile information to validate access. The application simulates this behavior with a pre-registered username and password that is compared with the authentication data entry to validate the first step of access. The validation subsystem must compare access characteristics to the stored profile for access to be released. If access to that user account is considered suspicious, the system should verify the type of access (account privilege) and trigger the challenge subsystem to apply the challenge to the degree of privilege of the access account. The prototype compares the source IP, operating system, and browser type attributes, individually or correlated, with the information stored by the application for each system account. The challenge subsystem must send the challenge to the user and if the challenge is answered correctly then access will be allowed. If the challenge is not answered or answered incorrectly then access should be denied. In the case of the prototype the system will send a challenge composed of questions if trying to access more than one authentication factor does not match the registered data of that account. Computer simulation now considers access as suspect and uses the challenge system to validate access. In addition to the user and password factor, the prototype will make available other factors of user attributes that can be analyzed from the login records of access attempts, in this case study, only the three factors (IP address range, operating system and type browser) will be considered and may be correlated for access validation.

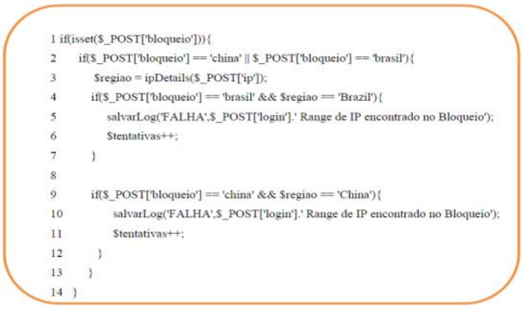
The prototype provides access logs with records of actions performed by access attempts. Through these logs it should be possible to audit access attempts and possible indications of accounts that may be being used fraudulently.

Authentication levels can determine the levels of control and measures to be taken at the time of the access request. According to [15], all operations performed in a pervasive environment cannot be classified into a single category. Therefore, the nature of operations must be involved in order to categorize authentication levels.

The profile type or privilege type determined the action and the level of that action. If access is considered suspicious, a challenge may be sent to the access requestor and the level of access requested will also determine the level of the challenge. The challenge level ranges from high to low and is determined by the types of questions sent to the access requester. For the application the authentication level was related to the number of input factors that differ from the stored access profile. From an input factor, in addition to username and password, the prototype submit the challenge. Whatever the input attribute, IP address, browser type, operating system, or browser other than the profile base, access is considered suspect and the challenge system is triggered. The prototype was developed in the PHP language (a recursive acronym for PHP: Hypertext Preprocessor) which is a commonly used open source scripting language especially suited for web development. The user must enter the prototype with login credentials (login and password) and, for implementation and testing reasons, additional fields have been added to validate the proposed template, such as the IP address range and country of origin of that address range IP. The application automatically identifies the source IP address by querying a website's IP address base that references the IP block entered for a particular country or region. Valid IP addresses on the World Wide Web allow us to identify the area and country of access because each block of valid IP addresses is registered for a particular country, region, or autonomous system that may be from a company or university.

The fields for validating access are presented on the data entry screen, such as the user and password. The application automatically detects which IP address (IP address - Internet Protocol), operating system and browser type of the device on which it is running. In the case of validation by IP address originating in a certain country, the database of the site https://ipapi.com/ is used, which from the IP addresses provided by the application that consumes the service, returns the country of origin to the application. of the IP address entered as input. For the experiment we used the IP address ranges from China and Brazil to perform the simulation.

The application will perform a scan by the IP address detected on the machine where it is running and the user can select the range of IP addresses from Brazil or China to verify access compliance. This verification is static for the experiment, but in a more complex and robust system in a production environment the control must be based on dynamic access profiles, so that the base is dynamic and constantly updated in order to effectively analyze the accesses. a large system user base. The prototype provides a demonstration of how this functionality can be useful for access reliability, as it becomes one of the authentication factors that can correlate with other factors for building a profile or "electronic identity" for that account or user. The application validates the IP per country, in case the prototype is restricted to the IPs of Brazil and China, collecting the IP from the source device and comparing it with the IP block of the two countries. The code below demonstrates the code that performs the factor comparison and verification, ie whether the source IP belongs to the Brazil or China block. If access is from a device in the Brazil IP range and the special validation option "Block Brazil IPs" is selected, the range will be in the block scope and access will be denied or sent the challenge.

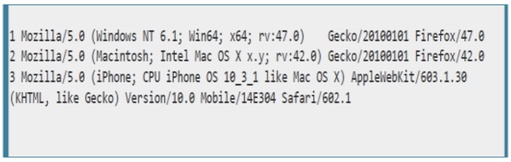


```
if(isset($_POST['bloqueio'])){
    if($_POST['bloqueio'] == 'china' || $_POST['bloqueio'] == 'brasil'){
      $regiao = ipDetails($_POST['ip']);
      if($_POST['bloqueio'] == 'brasil' && $regiao == 'Brazil'){
          salvarLog('FALHA',$_POST['login'].' Range de IP encontrado no Bloqueio');
          $tentativas++;
      }

      if($_POST['bloqueio'] == 'china' && $regiao == 'China'){
          salvarLog('FALHA',$_POST['login'].' Range de IP encontrado no Bloqueio');
          $tentativas++;
      }
    }
}
```

Figure 5. IP blocking function

The prototype uses information from the browser and operating system used to access the system for the purpose of composing the digital profile of the account or user. To perform this validation the application uses the USER AGENT feature of browsers. This feature provides a string information string ranging from browser type and version to operating system type. User Agent is an HTTP (Hyper Transfer Protocol) header that is sent by browsers to an application and serves as a unique identifying factor for that browser, regardless of type (Mozilla, Chrome, Internet Explorer, Safari, ...). It contains information about your web browser name, operating system, device type, and many other useful information.



```
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)    Gecko/20100101 Firefox/47.0
Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0
Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_1 like Mac OS X) AppleWebKit/603.1.30
(KHTML, like Gecko) Version/10.0 Mobile/14E304 Safari/602.1
```

Figure 6. User agent

In the figure above the first User Agent identifies a Mozilla browser on a 64-bit Windows operating system. The following User Agent identifies Mozilla and the Mac operating system and the third User Agent demonstrates an IPhone with Mac OS system and Mozila Firefox browser. The application is executed for access validation, first it performs the validation of the simple access that already exists in the system, which is the username and password. If this first validation succeeds, the application can perform validation by correlating between one and up to three factors, in case the validation of the source IP address block between IPs from Brazil and China, validate access from the browser and the system, access device, either just one of these factors or the correlation of two or three of them. The code below is an excerpt from the implementation of the challenge and compares the entries provided by the user to confirm the legitimacy of access, in this case the person registration and name of the mother's birth city, using the POST function to capture input data. In case of inconsistent information, access will be denied by calling the program "block.php" and the lock message will be displayed on the screen. If any of the three parameters are not met during the scan, IP, operating system, or browser, the prototype will perform a challenge to confirm access, but if more than one of these parameters is not met, the prototype will immediately block access, because by the business rule implemented this type of violation will be considered an illegitimate access. This challenge consists of sending questions from a predefined register when creating the access account.

The application presented access and lock logs as appropriate. Based on the defined requirements, the processing of the information in LOG format is stored in a physical file. Thus, all access history and treatment can be stored and auditable. When the application is run it creates a daily log file with the results of the login attempts, where it tells if the access was successful or failed. In case the login credentials are entered correctly and the option "Block Brazil IPs" is selected, as the access device is within the Brazil address range and there is a difference in the IP attribute the challenge is triggered. The responses to the challenge were incorrect and so access was blocked.

When entering the correct access credentials and selecting "Browser" the challenge is triggered, since the configurations of the browsers of the access device and the one stored in the prototype are different.

In this case, the browser version of the access device is different from the version stored in the prototype account profile, so access was denied.

5. Results

The prototype used as an experiment demonstrated that contextual authentication fulfills the function of preventing improper access and serious consequences such as information leakage and digital fraud. Validation of the results was possible due to the result of the application log and the tests performed with various use cases. Although the application does not function dynamically as expected from a context-aware application in a production environment, it has provided satisfactory results that indicate the use of context or behavior authentication, regardless of whether it is an experiment and works with static data that simulate the behavior in production. Through the logs generated by the application were denied access denials when one of the input data for access validation was different from the attributes previously registered in the application that make up the user's access profile, thus simulating a profile base of a context authentication application in production. Accesses were also validated and allowed where the access credentials coincided with the attributes previously registered in the application. Through logging and testing it was possible to verify that when one of the context factors was different from the attributes registered in the application, a question and answer challenge was sent to the user and according to the accuracy of the answer in relation to the pre-registered base the access was allowed, otherwise it was blocked. The operation of the application has shown that from attributes that form a particular access account profile, access requests can be analyzed, allowed, blocked or faced with a transaction considered suspicious can pose challenges to confirm the legitimacy of access. The application was developed to meet these requirements and after performing the access simulations it was evidenced through transaction logs and tests that when entering with selected attributes on the screen: source IP address range, operating system or browser, the application compared input data with predetermined parameters related to that account to classify access as legitimate or suspicious. The application granted access by positively validating the input information and in case of inconsistency between input data and profile attributes, access was considered suspicious. In order to validate access, a challenge was sent to the requester from a registration in the application itself, if the answers showed compliance with the profile attributes, access was allowed, otherwise access was blocked.

Thus one of the technologies used by the Identity and Access Management solution has been applied computationally through access simulations, confirmations, locks, and challenge challenges to users in an experiment and simulation environment that demonstrates the greatest protection against unauthorized access, fraud and information leakage that this type of solution can bring in access to applications in cloud computing environment.

6. References

[1] Norton Cyber Crime Report: The Human Impact. Symantec. 2019. Available at: https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Human%20Impact-A4_Aug18.pdf

[2] Brasil: Lei no 13.709, de 14 de agosto de 2018. Lei geral de proteção aos dados., ago 2018. http://www.planalto.gov.br/ ccivil_03/ _Ato2015-2018/2018/Lei/

[3] EU, UNIÃO EUROPÉIA: *Gdpr - general data protection regulation, eu.* https://eur-lex.europa.eu/eli/reg/2016/679/oj. 17

[4] Care, Jonathan. Phillips, Tricia. *Market Guide for Online Fraud Detection*. Gartner, jan 2018.

[5] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, "*Cloud computing synopsis and recommendations,*" NIST special publication, vol. 800, p. 146, 2011. [Online]. Available in: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

[6] ISACA, Emerging Technology – *"Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives."* – ISACA, Illions, USA – Oct, 2009. Available in: <http://www.isaca.org>.

[7] Portal UOL. Data leakage grows and is already 2nd largest digital attack on federal government. Available in: https://www.bol.uol.com.br/noticias/2019/06/16/vazamento-de-dados-cresce-e-ja-e-2-maior-ataque-digital-ao-governo-federal.htm

[8] Neto, L. A. B. *A Shibboleht SimpleSAMLphp Federated Identity Integration Engine for Cloud applications*. Federal University of Maranhão. 2014.

[9] Deepak H. Sharma, Dr. C. A. Dhote, Manish M. Potey. "*Identity and Access Management as Security-as-a-Service from Clouds*" 7th International Conference on Communication, Computing and Virtualization 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050916002489

[10] Osmanoglu, Erlem. *Identity and Access Management Business Performance Through Connected Intelligence*, Elsevier, 2014

[11] Allan, A. *Defining Authentication Strength Is Not as Easy*. Gartner, March 2018. Available at: https://www.gartner.com/guest/purchase/registration?resId=1796018&srcId=1-3478922230

[12] Saini, B. S.; Kaur, N.; Bhatia, K. S. Authenticating Mobile Phone User using Keystroke Dynamics. International Journal of Computer Sciences and Engineering. 2018.

[13] Johnson, G. *Towards shrink-wrapped security: A taxonomy of security-relevant context*. In Proceedings of the 7th Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2009, pages 1–2. IEEE Computer Society. 2009.

[14] Malek, B., Miri, A., and Karmouch, A. (2008). A framework for context-aware authentication. In Proceedings of the 4th IET International Conference on Intelligent Environments, 2008, pages 1–8. 2009.

[15] Babu, B. and Venkataram, P. *A dynamic authentication scheme for mobile transactions*.

2009.International Journal of Network Security, 8:59–74.

[16] Saevanee, H.; Clarke, N.L.; Furnell, S.M. *Multi-Modal Behavioural Biometric Authentication for Mobile Devices.* IFIP Adv. Inf. Commun. Technol. 2012, 465–474.

[17] Ashibani, Y.; Mahmoud, Q.H. *A Behavior Profiling Model for User Authentication in IoT Networks Based on App Usage Patterns*. In Proceedings of the 44th Annual Conference of the IEEE Industrial Electronics Society (IECON),Washington, DC, USA, 21–23 October 2018; pp. 2841–2846.

[18] Hghghgh Ashibani, Y.; Mahmoud, Q.H. *A User Authentication Model for IoT Networks Based on App Traffic Patterns*. In Proceedings of the 9th Annual IEEE Information Technology; Electronics and Mobile Communication Conference (IEEE IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 1589–1595.

[19] Benzekkia, K. Fergouguia. A.E. ElAlaoui, A.E. *A Context-Aware Authentication System for Mobile Cloud Computing.* Procedia Computer Science 127 (2018) 379–387. 2018.

[20] Rocha, Cristiano Cortez da *et al.*: *Uma arquitetura para autenticação sensível ao contexto baseada em definições comportamentais*. 2012.

7. Acknowledgements

We would like to thank the Graduate Program in Applied Computing (PPCA) at the University of Brasília (UNB), Brasília, Brazil.