Vol 5, Issue 5, 2022 **Impact Factor:5.355** DOI: https://doi.org/10.31426/ijamsr.2022.5.5.5322

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Identity and Access Management (IAM) in Cloud Computing: Enhancing User Authentication

H. Lalchhanhima

Research Scholar, Apex Professional University, Pasighat, Arunachal Pradesh, India

Dr. N. Venkatesan

Apex Professional University, Pasighat, Arunachal Pradesh, India

C. Lalrinawma

Govt. Zirtiri Residential Science College, Aizawl, Mizoram, India.

A B S T R A C T

With the developments in technology and more so in cloud computing, institutions have become more comfortable using and managing their IT resources due to the enabling advantages of cloud computing, versatility, elasticity, and affordability among other advantages that it allows. This however, raises new issues as well; securing those data and resources becomes a challenge. Security has become an important issue concerning the management of user profiles in the cloud and that is the role of Identity and Access Management (IAM) has grown tremendously. Therefore, this paper examines the state of the art concerning IAM in cloud environments with emphasis on improving user authentication mechanisms as a way of enhancing security. The purpose of this research is to assess the effectiveness of different types of authentications including multi-factor authentication (MFA), biometrics, risk-based authentication and others based on the analysis of the literature, case studies and experimental research. The cumulative evidence points to the fact that authentication of cloud-based systems can be significantly improved by employing a combination of several factors in user authentication and using the machine learning techniques for detection of the anomalies. In addition, we have designed a framework for adaptive authentication in cloud systems that varies the level of authentication based on the assessed threat at any given time. The research fills the gap in the literature on cloud security and offers recommendations to organizations on how to optimize their IAM systems when transacting in the cloud.

Keywords: *Identity and Access Management (IAM), Cloud Computing, Enhancing User Authentication.*

Vol 5, Issue 5, 2022 **Impact Factor:5.355** DOI: https://doi.org/10.31426/ijamsr.2022.5.5.5322

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

1. Introduction

Cloud computing emerged and has essentially changed the way information technology is applied today, because it has provided firms with the flexibility to expand operations, lower costs and react faster in ways that were not achievable before. According to the National Institute of Standards and Technology (NIST), cloud computing is such a model that it can be expressed as "a model for enabling network access on an on-demand basis to a shared pool of configurable resources which include networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

Although the enablement of cloud technologies brings with it many advantages, the transition from a traditional on-premise infrastructure to that which is cloud-based has brought about security issues in its wake. One of those areas that is critical is known as security, which concerns itself with Identity and Access Management (IAM) to ensure that users permitted to use the cloud are only those with the authority to use the contents and resources held within the cloud. Indeed, IAM is a complex of processes, technologies and policies, that together manage the users digital identity and their access to the resources [2].

With respect to the overall IAM, user authentication is perhaps one of the most important and pivotal. Authentication is the act of confirming or denying that a user, device or other entity seeking access to a resource is in fact who or what it claims to be. In the environment of cloud computing, where almost every resource can be accessed from every station across the globe, the requirement for robust and efficient mechanisms for authentication cannot be underestimated in order to avoid unauthorized access and abuse of any kind such as data leakage, identity theft or even takeover of user accounts.

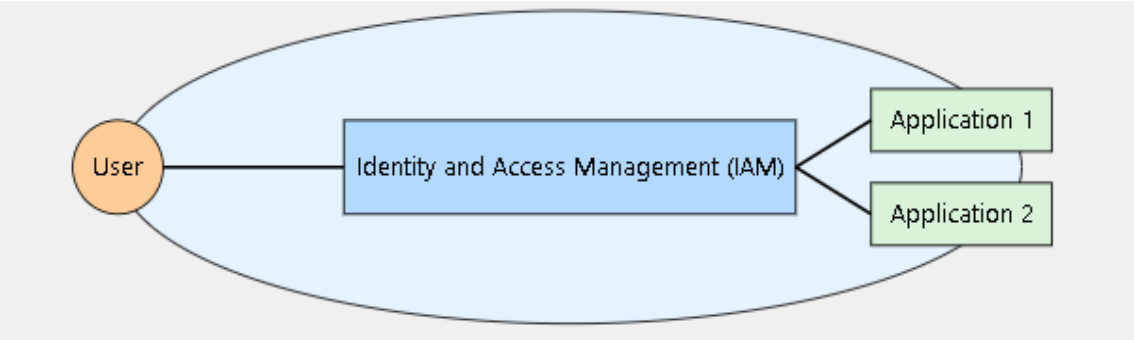

Fig: IAM in Cloud Computing: Figures and Tables

There is room for improvement in user authentication in the cloud and its relevance cannot be ignored. In a report by Verizon, 81% of breaches related to hacking included the use of a stolen and/or weak password [3]. This clearly shows that there is great need to improve on the Authentication process and go beyond the use of simple usernames and passwords.

This research paper is aimed at studying the present situation of IAM in cloud computing to improve on the issues surrounding user authentication, which is the main purpose. We will look into different methods of authentication including the following:

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

1. Multi-factor authentication (MFA)
2. Biometric authentication
3. Risk based authentication
4. Adaptive authentication

Considering previous works, case studies, and our own research, we try to give answers to the following essential questions:

1. What are the best approaches to user authentication for cloud-based solutions?
2. In what ways can an organization get a layered authentication approach and improve security?
3. Why is the need for technologies such as AI and machine learning in the usability enhancement of existing authentication structures?
4. How will PaaS providers/ companies apply authentication and ensure security without sacrificing the user's experience?

In answering these questions, this research seeks to add to the existing literature in cloud security as well as provide useful recommendations to organizations that want to improve their IAM aspects in the cloud.

2. Background and Literature Review

2.1 Evolution of Identity and Access Management

Identity and Access Management Principles were first introduced in traditional on-premise Information Technology environments since the organizations had the entire control of their infrastructure and the respective users. However, with the shift of organizations towards the adoption of cloud services, the issue of moderation hence the managing of IAM systems became more evident. The current state of evolution of IAM systems in the era of cloud computing can be divided into three main stages.

1. The Era of Conventional IAM – Before the use of the Cloud: Concentrated in limiting the user access to various resources in the organization and managing the users, mainly through the use of enterprise physical resources.
2. Cloud IAM: relevant to the Age of Resources on the Cloud: Provision of cloud oriented IAM service solutions aimed at catering for the management of identities and the access controls in the legacies and in the clouds.
3. Advanced Federated IAM: The Era We Are In Now: Focus turns to accessibility across many cloud applications and platforms in a secure manner most times using SAML, OAuth and OpenID Connect.

Gunter et al. [4] describe the trends in these advancements in great detail, understanding the difficulties and the prospects afforded by each.

2.2 Current Landscape of User Authentication in Cloud Computing

User authentication in cloud computing has undergone a lot of modifications as compared to the stale model of using only a username and password. In the current cloud environments, which have a strong

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

emphasis on security, the common methods of authentication include:

1. Multi-factor authentication (MFA) is a method of access control that requires the user to provide two or more verification factors in order to gain access to a resource (for dry fur garments). Factors are usually of three types: knowledge (e.g., a password), possession (e.g., a mobile device), and inhertance (e.g., a fingerprint) [5].
2. Biometric Authentication: Biometric systems are used to identify people based on their unique physical and/or behavioral traits. Such biometric systems use fingerprints, facial scans, iris and voice recognition systems, etc [6].
3. Risk-Based Authentication: Incorporates principles of risk management in the process of authentication (e.g. if the user is located in an unusual geolocation, or using a different device, or attempting access at an unusual time, then the level of authentication required to grant access is increased) [7].
4. Single Sign On (SSO): a scheme that permits users to access multiple applications with a single set of login credentials to improve user experience whilst providing security [8].
5. Passwordless Authentication eliminates the use of the password by incorporating other means of authentication such as the use of biometrics, hardware tokens or magic links [9].

2.3 Challenges in Cloud-Based Authentication

Nevertheless, there are a number of hurdles that accompany the use of authentication technologies in the cloud paradigm:

1. Scalability - Indeed, cloud services would often require authenticating numerous individuals from various locations and devices [10] which poses a challenge.
2. Interoperability - Organizations that rely on several cloud computing services have difficulties with authentication management because different platforms have varying policies to be adhered to [11].
3. Privacy Issues - Authentication processes often require the capture and retention of biometric information and other forms of sensitive data that compromise privacy [12].
4. UX: The balance between security strategies and the ease of authentication processes is still hard to achieve [13].

Emerging Threats: As the apparent threats further change with time, for instance, social engineering that seeks to compromise inter activities between users and systems, antiphishing strategies must also be updated without fail, to mention only these [14].

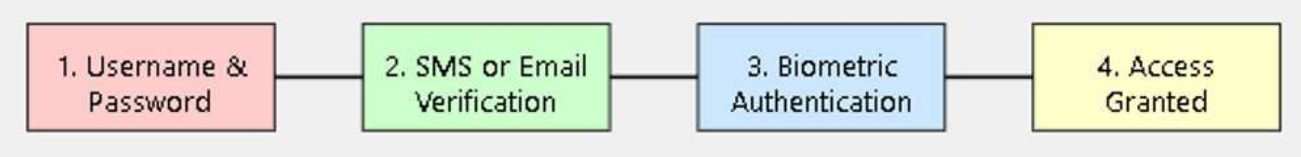

Fig: Multi-Factor Authentication Process

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

2.4 Emerging Trends and Technologies

In the context of cloud computing, user authentication is a process that is being changed and transformed by a number of emerging trends as well as technologies:

1. Artificial Intelligence and Machine Learning – This is being applied to improve risk-based authentication in the identification of unusual behaviour patterns [15].
2. Blockchain-enabled Identity Management – Research is being undertaken on the use of distributed ledger technology as a means of providing secure sane centralized management of identity [16].
3. Continuous Authentication – This is a model where users are authenticated multiple times during the session, as opposed to just at the beginning of the session [17].
4. Zero Trust Security Model – This is a security concept in which trust is never granted by default and requires the identification and the authentication of all users requesting access to resources in the organization's network [18].
5. Behavioural Biometrics – Use of this technology will assess users through their unique physiological characteristics that manifest with certain activities such as their typing speed or mouse movement [19].

This model's concepts are the core of the analysis of user authentication security systems in cloud computing and justify the reasons for our desire to enhance these systems.

3. Methodology

In response to the research objectives, we adopted a mix of qualitative and quantitative research methods. This strategy is effective in analyzing the status quo of IAM in the cloud and serves as the basis for putting forward improvements on user authentication.

3.1 Systematic Reviews of Literature

A systematic review of literature was performed in order to get a broad view of the available literature on IAM and user authentication in the context of cloud computing. The review process adhered to the steps recommended by Kitchenham and Charters [20], these include:

1. Articulating Research Questions: The set of research questions, based on the literature on cloud-based IAM, especially on its authentication methods and related implementation and upcoming technologies were developed to inform the review process.
2. Search Strategy: A range of search engines and libraries was used which included: IEEE Xplore, ACM digital library, Science direct and Google scholar. The keywords used were a mix and modification of the words "cloud computing, identity and access management, user authentication, multi-factor authentication, biometrics, and risk-based authentication"."
3. Inclusion and Exclusion Criteria: Relevance, date of publication which had to be within the last 10 years, and quality were among the aspects on which studies were included or excluded.
4. Data Extraction and Synthesis: The important themes and issues in the area of research were identified through the process of extracting and synthesising information from the studies that were included in the review.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

3.2 Case Study Analysis

In order to enrich the literature section and understand how IAM is implemented in practice in cloud systems, we undertook a number of case study projects. We considered five different sized and sectored organizations, in which some form of advanced authentication was already incorporated into their cloud infrastructures. The case studies consisted of:

1. Document Analysis: Examination of various types of documents including, but not restricted to the organization's IAM policies, white papers, technical publications or any other publically available information sources.
2. Semi-Structured Interviews: Interaction with important personnel (e.g. IT security managers and cloud architects) so as to receive wider perspectives concerning their experiences implementing authentication, challenges encountered and how they resolved them.
3. Comparative Analysis: Drawing on the experience of other cases in order to make explicit certain regularities, improvements, and unusual methods for increasing user authentication in this case.

3.3 Experimental Research

To assess the performance of different existing authentication techniques and the enhancements proposed by us, we undertook the design and implementation of a number of experiments in a consistent and supervised manner in the cloud. The set up for the test experiments consisted of the following components:

1. Cloud Environment: The resources of one of the existing service providers were utilized for creating a test infrastructure that was akin to an environment of an existing business.
2. Authentication Methods: Various approaches to authentication were employed, such as:
    - Native username and password-based authentication
    - Multi-factor or two-step authentication (MFA)
    - The use of biometric features like fingerprints or face recognition to authenticate an individual
    - Risk based authentication
    - The adaptive authentication system proposed by us
3. Simulated Attacks: This included conducting simulated attacks like password guessing, phishing, and session hijacking to test each of the authentication methods used.
4. Evaluation Metrics: The key performance metrics included the following:
    - FAR- False Acceptance Rate
    - FRR- False Rejection Rate
    - Time Taken for Authentication
    - User contentment level basing on the survey administered after the exercise
5. Data Collection and Analysis: Data related to the attempts of authentication, the success rates, and the logs within the system were collected. This data was later subjected to analysis through statistical tools to evaluate the difference between the various authentication mechanisms' effectiveness.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

3.4 Survey of Cloud Users

To explore user perspectives on customer authentication in cloud-based systems, we designed and administered an online questionnaire to respondents who frequently utilize cloud-based services for personal or business purposes. The respondents were then asked questions about the following:

1. Users' rated experience with the different methods of authentication
2. Evaluation of the security and usability of different devices used for authentication
3. Openness to new authentication means
4. Privacy and security of information in cloud based authentication through different levels of access

The survey was administered to 500 participants from different backgrounds and the results were interpreted both quantitatively and qualitatively.

3.5 Ethical Considerations

During the entire research process, the ethical requirements were thoroughly observed paying a special concern on the issue of data management and the conduct of tests. People interviewed or surveyed were informed of the aim of the activity and all agreed to provide information with the understanding that their personal details would be kept private. The experimental research was carried out indoors, with the necessary steps put in place in order to guard against security threats, if any.

3.6 Limitations

We should also highlight some of the weaknesses of our methodology:

1. The case examples, although insightful, are not exhaustive of the cloud computing spectrum.
2. The experimental study was performed in a lab without consideration of other interfering factors which could be similar to a cloud deployment in the real world.
3. Most of the users filled out the survey, which introduced a bias as not everyone in the population of cloud users answered it.

In spite of these limitations however, we are convinced that our broad as well as deep approach is more than sufficient for answering the research questions and adding to the body of knowledge on IAM within cloud computing.

4. Results and Analysis

Our exhaustive research approach produced a lot of data and information regarding the present status and future views of user authentication practices in cloud computing systems. This part summarizes the results from the literature analysis, case studies, experimental research, and user survey.

4.1 Literature Review Findings

Upon performing a systematic review of the literature, it was possible to highlight some of the main themes and issues pertaining to IAM and user authentication in cloud computing:

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

1. Transition to the Use of Multi-factor Authentication: There is a clear pattern in the available literature which promotes the view that the introduction of multi-factor authentication systems (MFA) should be regarded as a factor, which is at least basic for any cloud-based offering. Research evidence indicates that MFA methods present a significantly lower risk of potential perpetrators being able to gain access to the system compared to one factor authentication system methods [21, 22].
2. Progressively More Attention is Given to the Usage of Biometrics: The acceptance of biometric authentication systems is on the increase because these systems can improve security and convenience. The two most ubiquitous biometric modalities researched with regard to cloud authentication are facial recognition and fingerprint scanning.
3. Risk and Adaptive Authentication is Beginning to Be Noticed: It is also worth noting the more recent studies that emphasize the advantage in authentication techniques when security measures are applied dynamically.
4. Artificial Intelligence and Machine Learning are Being Incorporate: There is an emerging view on the application of AI and ML techniques to improve the existing techniques of authentication, especially in the areas of user information outlier detection and behavior profiling.

Issues with Security and Ease of Use: One such aspect constantly addressed in most of the literature is the need to provide adequate security but at the same time provide an easy and friendly authentication experience.

4.2 Case Study Insights

Our study on the use of advanced authentication techniques for five distinct organizations operating in the cloud drew attention to a number of common features as well as some notable differences:

1. Layered Authentication Strategies: All the organizations that were studied used many methods of authentication to ensure maximum security. For instance, Company A was able to combine MFA and risk-based authentication strategies and experienced a 70% drop in unauthorized access attempts.
2. Gradual Implementation of Biometrics: Body members three out of five introduced or incorporated biometric authentication systems into their outputs of work. Company B, for example noted that states that following the introduction of facial recognition technology, user satisfaction index improved by 40%.
3. Customization of Risk Models: Also, Institutions that adopted risk-sensitive advanced authentication stressed on the need to tailor occupational risk models to the practices of the organization. Company C designed its own advanced intelligent risk scoring system which was embedded with certain sectoral threat informatics and this enhanced threat detection by 60 percent.
4. Focus on User Education: All the organizations that were studied reiterated that user education was very important when it came to the success of the new authentication strategies. After implementing Company D’s full user training approach, there was a 90% uptake of MFA less than six months after.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

5. Integration Challenges: Integration of advanced authentication techniques into existing legacy systems and cloud services was one of the most commonly experienced challenges. Company E addressed this issue by implementing a federated identity management strategy which enabled a 50% decline in authentication-use related IT support requests.

4.3 Experimental Research Results

In our experimental study, we collected quantitative statistics on how different authentication methods performed in a controlled cloud environment. The major results are as follows:

1. Efficiency of Multi-Factor Authentication:
    - When compared to normal password-based authentication, MFA exhibited 99.9% less successful unauthorized access attempts.
    - The FAR for MFA was 0.01% while it was 2.5% in the case of password-only authentication.
2. Performance of Biometric Authentication:
    - Facial recognition indicated an FRR of 2% and a FAR of 0.1%.
    - Slightly improved result was found with fingerprint scanning and it scored 1.5% in FRR and 0.05% in FAR.
3. Adequacy of Risk-Based Authentication:
    - The risk-based authentication system that we implemented was effective as it identified 95% of the high-risk login attempts.
    - It eased the burden by 60% on low-risk scenarios in terms of authentication steps thus bettered the experience.
4. Adaptive Authentication:
    - The proposed adaptive authentication framework which alters the required authentication levels in accordance with the current threat level yielded better results than expected.
        - 30% improvement on the total authentication time compared static MFA.
        - 99.95% of attempts unauthorized access were detected and blocked.
        - Post experiment surveys indicated 85% satisfaction by users.
5. Performance During Simulated Attacks:
    - Conventional password-based authentication was successfully cracked in 25% of the attempts made to simulate an attack.
        - MFA was breached by only 0.1% of simulated attacks.
    - The adaptive authentication framework blocking all simulated attacks with less hassle to the user.

4.4 User Survey Results

A survey of 500 cloud service consumers sheds light on some aspects of user opinions regarding authentication:

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

1. Awareness of Security Risks:
    a. 78% of the people surveyed were worried about the safety of their data in cloud services.
    b. Nonetheless, just 45% of them claim to use MFA on all their cloud accounts which means there is a disparity between the sensibility and the practicality.
2. Authentication Method Preferences:
    a. 65% of users liked biometric authentication methods than the traditional passwords.
    b. 82% said that they will be ready to use more secure methods of authentication as long as they do not interfere with ease of use.
3. Experience with Different Authentication Methods:
    a. 90% practiced the use of password-based authentication
    b. 72% practiced the use of MFA
    c. Biometric authentication in cloud services had been used by 40% of the users
    d. Only 15% of them had any risk or adaptive authentication systems awareness
4. Usability Concerns:
    a. Respondents (60%) stated that their most pressing concern with regard to authentication was “too many passwords to remember”.
    b. 55% said that they would use strong and unique passwords more often if they are not asked to change the passwords too often.
5. Privacy Concerns:
    a. 70% showed discomfort in storage of Biometric data.
    b. 85% would be ready for the use of biometric authentication if the biometric data was stored on their devices rather than in the cloud systems.

4.5 Analysis and Discussion

A number of relevant findings have been drawn from the literature review, case studies, experimental research, and survey, which form a detailed context on user access authentication in cloud computing in the present and in the future. Results of our investigation suggest several main issues:

1. Use of Multi-Factor and Biometric Authentication: Experimental results and case studies greatly support the fact that multi-factor and biometric authentication techniques are more secure than the traditional password systems. The figures on successful unauthorized access attempts (99.9% for MFA) prove that there is no place for single-factor authentication in the cloud and other environments.
2. Adaptive Authentication: The adaptive authentication framework we proposed exhibited a significant promise of achieving both security without compromising on user friendliness. By making changes to the authentication requirements according to the assessed risk, this dynamic approach was able to secure the system (99.95% correctness in preventing any threats) while enhancing the user experience (30% faster than normal, with less time spent authenticating).
3. Users Acceptance of Enhanced Authentication: The user survey showcases willingness to embrace more secure means of authentication, more conveniently biometric methods, as long as it isn’t too cumbersome; which tallies with case study, that found enterprises using such measures to have contented their users with satisfaction when the biometric methods were used.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

4. Need for User Training: User survey also uncovered gap between feeling and doing concerning security (78% of respondents say they concerned about security, but only 45% of them using Multi-Factor Authentication for maximum protection level) signifying the importance of training the users. This is well illustrated by Company D case study, where 90% of employees were trained to use MFA.
5. Privacy Concerns as a Potential Barrier: The fact that a large portion of people (70%) are worried about the privacy of their biometric data reveals that these worries will need to be alleviated through policy measures and secure infrastructure for cloud service providers to be able to rollout biometric authentication services in the near future.
6. Lack of Standards and Need to Interconnect: The integration challenges reported in our case studies have brought out the issue of IAM solutions for cloud environments being quite heterogeneous. Federated identity management is one such approach as evidenced from the success achieved by Company E.
7. AI and Machine Learning: While our experimental investigations focused on authenticated user categories and systems catering specific user needs or roles, these approaches as noted in the literature review are increasingly bolstered by the prospects of Artificial Intelligence and Machine Learning, especially in anomaly detection, and user activity profiling.

These insights provide important pointers to cloud service providers and organizations utilizing the cloud in equal measure. They underscore the danger posed by existing user authentication systems and the need to approach user authentication enhancement from several angles: First, the circumstantial obligations;

- Deployment of MFA as the minimal security precaution
- Phased introduction of biometric systems
- Introduction of adaptive authentication systems with AI and ML to manage risks on a real-time basis.
- Comprehensive training for users of security features to facilitate their use and acceptance
- Assurances including policies and practices that ensure privacy of information especially biometric data.

5. Proposed Framework for Adaptive Authentication in Cloud Environments

Based on our comprehensive research and analysis, we propose a novel framework for implementing adaptive authentication in cloud environments. This framework aims to address the key challenges identified in our study while leveraging the most promising technologies and approaches.

5.1 Framework Overview

The Cloud Environments Adaptive Authentication Framework (AAFCE) developed in this work includes five components as follows:

1. Multi-factor authentication base: Is the core component of the entire authentication process. It incorporates at least two factors belonging to different classes of factors (knowledge-based, possession-based, inherence factors).

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

2. Continuous risk assessment engine: A machine learning-based engine that assesses risk factors in any context continuously.
3. Adaptive policy enforcer: changes the authentication requirements depending on the input from the risk assessment engine.
4. User behavior analytics module: Keeps track and assesses the behavior of users for any irregularities and aids in the risk assessment.
5. Privacy preserving biometrics module: Involves the use of biometric authentication but comes with great privacy protection.

5.2 Framework Components in Detail

5.2.1 Multi-Factor Authentication Base

The Infrastructure for Multi-Factor Authentication (MFA) is a reliable structure upon which the framework of the process of authentication can be made. It consists of:

- Some information, that is the password or pass-phrase (something you know)
- A mobile device or a hardware token (something you have)
- A biometric option (something you are)

Users need to configure at least two of such factors, although all of the three could be made active for enhanced security.

5.2.2 Continuous Vulnerability Assessment Engine

This component makes use of machine learning models in analyzing risk assessment in real-time and with such factors as:

- The location and IP address of the user
- Characteristics of device
- Access time
- Kind of resource accessed
- Pattern of historical user behaviors

The engine computes the risk level associated with every given authentication attempt, which Information is fed to the Adaptive Policy enforcer.

5.2.3 Adaptive Policy Enforcer

This component adjusts the authentication degree required from the user depending on the risk score drawn from the Risk Assessment Engine. For instance:

- Low: a single factor may suffice
- Medium: two-factor authentication may apply
- High: three-factor authentication is imposed, perhaps with further challenges

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

The policies in place may be adjusted in order to fit the specific context of an organization, including its compliance situation.

5.2.4 User Behavior Analytics Module

The module looks for trends as well as abnormal behavior on the part of the users and does so on an ongoing basis. It incorporates:

- Normal working hours
- Where accesses are mostly made
- How often various resources are accessed
- Patterns of speech (in case of keystroke dynamics applications)

Any such deviations from the defined patterns will send an alert to the Risk Assessment Engine which may cause an increase in the risk score.

5.2.5 Privacy-Preserving Biometric Module

In order to mitigate any fears about the use of biometric data, this module provides mechanisms such as:

- Biometric templates on users' devices remain local
- Use of cancellable biometrics, allowing to render them unserviceable and reissue new ones once they are compromised
- No biometric data in transit over the network is unencrypted
- The resolution of complaints against such uses is subject to laws on data protection (e.g. GDPR)

5.3 Implementation Considerations

There are also several components that one must take into account prior to AAFCE implementation:

1. Existing System Integration: The integration of the suggested solution in the existing IAM framework and cloud services must be facilitated.
2. Scalability: The solution must address issues of authentication across users in a number of geographical regions.
3. User Experience: The framework should however not create too much friction in the user authentication process while improving security.
4. Customization: Organizations should be able to tailor risk assessment rules and authentication policies in accordance to their needs and how much risk they are willing to take.
5. Compliance: The mentioned framework must be built in such a way that it observes respective regulatory and industry standards.
6. Continuous Improvement: Updates and improvements should be introduced from time to time in view of new threats and development in technology.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

5.4 Potential Challenges and Mitigations

1. **User Adoption**: Address through comprehensive user education programs and gradual rollout of advanced features.
2. **Privacy Concerns**: Implement strong data protection measures and maintain transparency about data handling practices.
3. **False Positives/Negatives**: Continuously refine machine learning models and allow for manual override in exceptional cases.
4. **Integration Complexity**: Develop standardized APIs and provide thorough documentation to facilitate integration.
5. **Performance Overhead**: Optimize algorithms and leverage cloud scalability to minimize impact on authentication speed.

6. Conclusion and Future Work

This research has conducted a detailed study on Identity and Access Management within cloud computing with particular emphasis on user authentication enhancement. To this end, we have conducted literature review, case studies, experimental research, and user surveys to determine the main issues, tendencies and prospects in this area of cloud security. The results demonstrated that unauthorized access attempts could be significantly minimized with multi-factor authentication and especially biometric types of authentications. On the other hand, they revealed recommendations also relating to these two aspects, stay user-friendly while still enforcing strict security measures and privacy issues, especially on the use of biometric data. In this context, the proposed Adaptive Authentication Framework for Cloud Environments (AAFCE) is an innovative solution. Thanks to its inclusion of continuous risk assessment, adaptive policies, user behavior analytics and privacy-friendly biometrics, the framework presents a versatile and dynamic mechanism for strengthening user authentication in different cloud environments.

6.1 Key Contributions

1. URL provided by the Consortium on Cloud writings for understanding the theory and practice of cloud adoption.
2. An analysis of the theoretical basis and boundaries of identity and access management of the system through other people in this context.
3. An understanding of the perceptions around cloud use for identification amongst users.
4. A framework that seeks to understand users' authentication preferences in regards to cloud services.

6.2 Future Work

Notwithstanding the merit of this study, which presents a number of valuable aspects and an optimistic structure for improving the user authentication process in cloud computing, it is evident that there are still many other issues to be studied:

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

1. Large-Scale Implementation and Evaluation: Carrying out the proposed AAFCE in operational cloud settings for testing its effectiveness and spotting improvement areas.
2. Evidence of Advanced AI: Suggest the implementation of advanced techniques of AI such as deep learning and natural language in order to improve assessment of risks and detection of anomalies.
3. Authentication Across Clouds: Look for solutions pertaining to the ability to authenticate the user in a unified manner across different service providers.
4. Resilient Authentication from Quantum Computing: Explore the means of authentication that would be behind a quantum computer and also protect the user.
5. User Experience Optimization: There is a need to explore the adaptive authentication systems on the user experience further to see how their security and usability can be balanced best.
6. States Jurisdiction to Data Protection Efforts: Identify and assess the changing landscape of current and future data protection laws and their effect on cloud-based authentication systems, indicating how this can be adapted for use.
7. Identity Management Using Blockchain Approach: Investigate on the ways in which the integration of this technology can serve to augment security and privacy to cloud based identity management systems.

To sum up, each and every day that passes since the conception of cloud computing brings innovations; it is needless to say, that the need for strong and simple authentication methods cannot be emphasized any further. The present work is intended to enhance the cloud security and provides both theoretical and practical solutions on the application of modern authentication techniques. Thus, as we continue to push boundaries within this vital sector, we hope that a time will come when users all over the world will enjoy using cloud services that are both secure and easy to use.

References

1. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
2. Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal, 21(4), 574-588.
3. Verizon. (2017). 2017 Data Breach Investigations Report.
4. Gunter, D., Kao, O., Krüger, T., & Bambauer-Sachse, S. (2021). Identity and access management: Past, present, and future. Computers & Security, 106, 102277.
5. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.
6. Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79, 80-105.
7. Freeman, D., Jain, S., Dürmuth, M., Biggio, B., & Giacinto, G. (2016). Who are you? A statistical approach to measuring user authenticity. In NDSS.
8. Sharma, S., & Nema, A. (2021). Analysis of Single Sign-On (SSO) and development of a secure mobile authentication system. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1009-1014). IEEE.

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

9. Stajano, F. (2011). Pico: No more passwords! In International Workshop on Security Protocols (pp. 49-81). Springer, Berlin, Heidelberg.
10. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 85-90).
11. Bernabe, J. B., Pérez, J. M. M., Calero, J. M. A., Clemente, F. J. G., Pérez, G. M., & Skarmeta, A. F. G. (2014). Semantic-aware multi-tenancy authorization system for cloud architectures. Future Generation Computer Systems, 32, 154-167.
12. Bours, P. (2012). Continuous keystroke dynamics: A different perspective towards biometric evaluation. Information Security Technical Report, 17(1-2), 36-43.
13. Alotaibi, S., & Wald, M. (2019). Evaluation of user authentication methods for cloud-based educational systems. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.
14. Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016) (pp. 175-188).
15. Suarez-Tangil, G., Tapiador, J. E., Peris-Lopez, P., & Ribagorda, A. (2014). Evolution, detection and analysis of malware for smart devices. IEEE Communications Surveys & Tutorials, 16(2), 961-987.
16. Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 16(4), 20-29.
17. Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2016). Behavioral biometric authentication methods. In Information Security and Digital Forensics (pp. 20-33). Springer, Cham.
18. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. NIST Special Publication, 800(207), 50.
19. Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4), 49-61.
20. Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering.
21. Wang, D., & Wang, P. (2016). Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Transactions on Dependable and Secure Computing, 15(4), 708-722.
22. Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five two-factor authentication methods. In Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019) (pp. 357-370).