International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 6, Issue 9, ISSN No. 2455-2143, Pages 249-255
Published Online January 2022 in IJEAST (http://www.ijeast.com)

A STUDY ON SECURITY SERVICES AND THREATS IN CLOUD COMPUTING

Sumit Kumar, Prof. Dr.Preeti Rai
Gyan Ganga Institute of Technology Sciences

Summary: **Digitalization has infiltrated all sides of modern culture today. One of the most important aspects of making this procedure secure is authentication. Cyber criminals are putting in a lot of effort to break into existing network channels and launch destructive assaults. When it comes to businesses, information is a valuable resource. The question here is how to safeguard crucial information. This takes into account a variety of features of a society that is commonly referred to as hyper connected, such as online communication, purchasing, access rights control, and so on. We shall cover the ideas of MFA and KBA, or Multi-Factor Authentication and Knowledge Based Authentication, in this study article. The goal of MFA and KBA is to be utilised for human-to-machine interactions, providing an easy-to-use and secure validation mechanism while gaining access to the service. We will also look into the existing and evolving factor suppliers (sensors) that are used to authenticate a user in this study. This is a critical tool for safeguarding data against malicious insiders and outsiders. The basic purpose of access management is to give authorised users access to a service while simultaneously preventing unauthorised users from accessing it. To ensure access management, a variety of strategies can be used. In this paper, we will cover various strategies for ensuring enterprise-ready access management, with a particular emphasis on multifactor authentication. We'll also discuss how knowledge-based authentication fits into multi-factor authentication and how it may help businesses protect their data from cyber-attacks. Finally, we'll talk about the future of MFA and KBA.**

Keywords: **Cyber security, evolution, vision, SFA, 2FA, MFA, data breach, KBA.**

I. INTRODUCTION

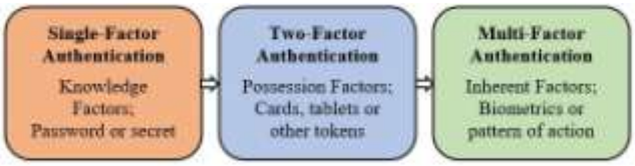
The constant rise in smart device usage, as well as the associated networking features, has an impact on mobile networks all around the world. Authentication is the key to keeping the transfer of such a large amount of data safe in such a tightly knit setting.

Authentication is frequently described as a technique through which the system computes the values sent by the user and compares them to the existing value. This is also known as the user identification process. It is a critical precaution against unwanted access to a computer or other sensitive application, whether offline or online.

Initially, only one factor was employed to authenticate the person. Because of its user friendliness and simplicity, Single-Factor Authentication (SFA) was widely adopted. It's possible, for example, to use a password or a PIN to verify a user's identity. This is, without a doubt, the most basic level of authentication. By changing the password, one automatically compromises the account. An unauthorised person could also try to get access using social engineering techniques such as the rainbow table or the dictionary assault. When employing this method of authentication, the minimal requirement of password sophistication is usually taken into account. Considering all of the risks connected with single-factor authentication, the SFA was deemed a weak form of protection. Furthermore, validation within a single element was not known to be trustworthy in providing appropriate protection due to a range of security threats. Two-Factor Authentication (2F) was designed to address the drawbacks of SFA by combining username/password with a personal ownership factor, such as a card or phone number. Factor groups are now categorised into three types as a result of the introduction of this new type of authentication:

1. SOMETHING YOU KNOW: As the name suggests, it is something that user already knows. That can be anything such as a password or any “secret”.
2. SOMETHING YOU HAVE: This is related to what user possesses that includes tablets, cards, tokens, etc.
3. SOMETHING YOU ARE: This is the Biometric factor, and can also be explained as the physical aspect of the individual. For example, thumb impression, facial recognition etc.

Multi-Factor Authentication (MFA) quickly became famous because of the extra layer of security that it offered using multiple types of credentials. Using MFA offered seamless protection of hardware as well as other important facilities against unauthorized access. For the most part, MFA is focused on biometrics, in which people are instantly identified on the basis of their behavioral and biological characteristics. As users were expected to show proof of their identification, which is dependent on two or three different factors, this move provided an enhanced degree of security.


Single-Factor Authentication
Knowledge Factors; Password or secret
Two-Factor Authentication
Possession Factors; Cards, tablets or other tokens
Multi-Factor Authentication
Inherent Factors; Biometrics or pattern of action

FigureA.The Evolution of Authentication Methods

MFA is now needed to be utilised in instances where protection standards are higher than usual. According to SC Data UK, 68 percent of European citizens desire to adopt biometrics as their primary means of transaction verification. Take a look at your everyday cash withdrawal routine. Here, the operator must present a physical token, such as a card, followed by a PIN code. This method might simply be made more complex by adding the second channel. In a more fascinating case, it may be accomplished using facial recognition techniques. In addition, according to a new survey, thirty (30) percent of firms intended to implement the MFA resolution in 2017, with fifty-one (51) percent saying that they are now utilising MFA and 38 percent stating that they are using it in "certain parts" of their operations. These figures show that multi-factor authentication is the right move forward in the evolution of authentication. MFA has three uses: business applications such as e-commerce, ATMs, and so on. Applications from the government and investigative applications Currently, MFA is a critical vector for: the authentication of the user's identity and the electronic computer (or its system); the authentication of the user's identity and the electronic computer (or its system; and the authentication of the user's identity and the electronic computer (or its system). Confirmation of infrastructure links; Validation is required for connected IoT devices such as tablets, smart watches, and phones. The MFA approach should be as simple as possible, including features such as:

1. Consumers must first register and then validate with the SP (Service Provider); 2. When accessing the service, the customer must provide an SFA with the finger print or token authorised by the service provider; 3. User authentication is done by logging in and signing using the matching credentials provided in the user portal until the device approves it (or social login). The management framework will allow secondary authentication factors for added security. When the customer has successfully completed the checks, the framework automatically grants access to the portal.
2. Verification (secondary level) is carried out on its own, based on biometric authentication or other methods (MFA). In other words, if the (MFA) fails, the operator will just have to supply an additional code or the token.

II. POTENTIAL SOURCES OF MFA

Currently, a large number of sensors are used in authentication mechanisms, allowing a user to be identified. In this section of the paper, we address the MFA-appropriate variables, what types of sensors are available on the market, and their associated challenges. Additionally, we will also talk about the steps to be taken in immediate future.

2.1 Protection Using Passcodes:

The traditional method to validate an operator stands by requesting password or a Personal identification number (PIN) code. Information factor historically reflects the hidden pass-phrase. To authenticate the user, it only takes a basic input system (atleast one button).

2.2 Authentication Via Token:

A physical token, such as a passport, which is suggested as a second factor party, should then be added to the password. A costumer can use a mobile, smart watch, etc., which are more difficult to use from the hardware perspective.

2.3 Biometric Using Voice:

Majority of current electrical devices now comes consisting of a mic which gives allowance to speech recognition which can be used as MFA factor. Unfortunately, down side of using speech recognition as method of authentication is that it might allow agencies to recognize speakers as well as imitate their voices.

2.4 Face Recognition:

At start of the development of face recognition method, the technology used image analysis which was quite easy to clone by supplying a picture to the system. The next stage was to enable three-dimensional identification of the face, by requesting the user to turn the head in a particular way during the authentication process. Lastly, development of the device has come upto the point where it is understanding the user's individual expressions.

2.5 Iris Recognition Technique:

The methods for iris detection have been on the market for more than 20 years. When studying the color pattern of an individual’s eye, this technique doesnot enable the consumer to be close to the capture system. Another enticing method is retina examination.

2.6 Recognition Via Hands:

To authenticate the individual, certain programs employ the study of the actual form of a hand. Pegs were being deployed for this purpose but the usability of such methodology was quite low.

2.7 Recognition Of Veins:

Fingerprint scanners provided the option to read even the finger's vein. To obtain and archive the movement of the whole hand,more complex systems use palm print recognition.

2.8 Finger Print Authenticaton:

The majority of mobile phone vendors are now moving to use finger prints canners as the main authentication mechanism. This approach is intuitive but is very simple to produce, primarily since our fingerprints can be acquired from nearly everything we touch.

2.9 Authentication Using Thermal Image:

In this case, thermals ensors are used to recreate the unique thermal picture of the blood supply of one's body in the vicinity.

2.10 GPS Based Authentication:

A special case of position-based authentication is the use of the spatial location of the device and customer. Because of the transmission properties, the GPS signal may easily be jammed or deemed defective; it is thus advised to use a minimum of (2) Sources of location, such as Global positioning system (GPS) and the wireless network ID.

III. CHALLENGES ENCOUNTERED

For the implementation of secure identification and multi-factor authentication, user acceptance is a vital feature. Considering, it's very important to track a deliberate and detailed method when implementing and executing MFA solutions.

3.1 Compatibiity:

Three viewpoints could describe the key usability problems that arise in the authentication process. Availability of the task: time to register and time for device authentication. Effectiveness of the task: attempts to login for authentication and User personal opinion.

INCORPORATION:
In spite of all the usability problems being implemented, integration raises more concerns together within technical in addition human view points. Majority solutions of MFA in relation to the market are hard ware-based.

2.11 Protection:

A digital infrastructure consisting of essential elements, such as sensors and computing un its is any MFA platform. Both of these are usually vulnerable at completely different levels to a range of threats, reaching from repetition of attempts toward enemy outbreaks. Protection is therefore critical instrument for privacy towards being allowed also protected. During transmission between the sensor and the computation device, sensitive data breach is a possibility. Such robbery can occur primarily because of transmission which is un safe through the input device respectfully to the data base also there is a potential for an attempt. Danger isalso associated with attacks in relation to the locations. The global positioning system (GPS) signals might be in clined to the location locking and feeding incorrect information to the receiver so that an in accurate time or location is measured. For cellular- and WLAN-based location services, related strategies can be applied. The MFA architecture should provide comparatively high "throughput" ratios, representing a system's capacity to satisfy its operators' expectations in regards attempts of inputs amounts per time extent. A penetration assessment panel may also be sponsored by the MFA security platform to determine the possible vulner abilities.

3.2 Durability:

Even if the protection and privacy issues are thoroughly addressed, from the very beginning of their journey, biometric devices, mainly finger printing, have fall en short of achieving the "robustness" criterion. This was primarily due to operational experiments being carried out instead of field tests in the laboratory setting.

IV. KNOWLEDGE BASED AUTHENTICATION

Knowledge Based Authentication is another strong measure to prove that the person who is providing the authentication information is truly that person. As its name clearly states KBA uses the knowledge possessed by the individual.
These four requirements should comply with a successful KBA query:

- The question should be appropriate for a large segment of the population.
- Easy answer.
- The answer to the argument should be one.
- Difficult retrieval of answer.

It is categorized into three forms with notice able differences:
a) Static KBA, b) Dynamic KBA, c)Enhanced KBA

a) Static KBA

Static KBA can be explained is shape of set of secrets that are pre agreed and that allows operators in picking safety questions also to deliver answers to which remain logged by the organization to be accessed later. Organizations are moving away from this method because questions are too generic and can be easily hacked.

b) Dynamic KBA

These are referred to as "out of the wallet" questions that are not pre-defined but created using a variety of data sources in real time.

c) Enhanced Dynamic KBA

Enhanced dynamic KBA goes one step further and makes the authentication process more secure, as it uses proprietary data stored behind firewalls and creates authorized question for relevant users, ensuring end to end authentication.

4.1 KBA CHALLENGES

Fig. 2 specifies the difficulties of KBA, it talks about fundamental issues, security and ease of use, however it incorporate the attributes that are separated into six categories. The Challenge of security contains safety problems, accessible individual information, and the confidentiality.

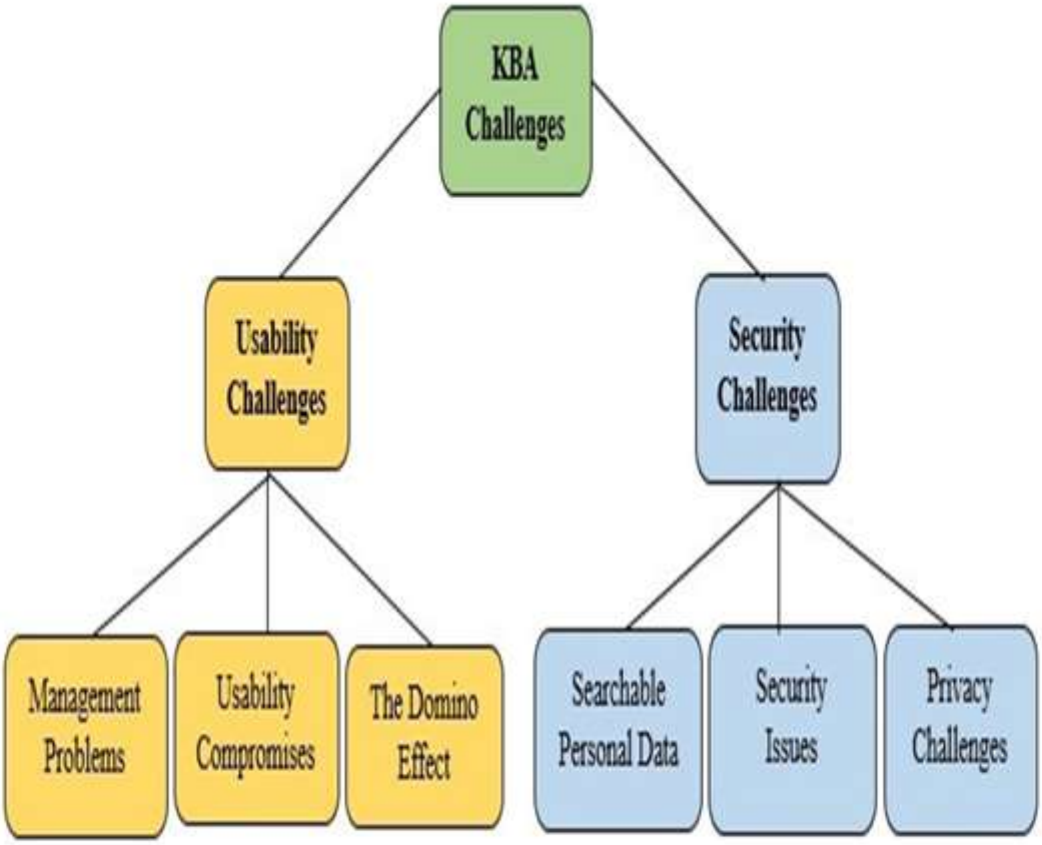


Figure2. ThechallengesofKBA

4.1.1 Security/ Confidentially Challenge

It is by which individual information is saved, indifferent domains. This classifies into three sections: attack types, searching about individuals' data or recognition, and confidentiality in regards to the client account.

Confidential/ Security challenge is classified into further types:

4.1.1.1 Search able personal

It becomes simple for users when the password they use is same across multiple social networks, but such scenario is considered a challenge due to login circulation and redundancy. That may be activated by simple guessing or attacks.

4.1.1.2 Security/Confidentially Issues

Many kinds are present if we talk about threats and hacking that include a false account or data theft. Security's biggest obstacle is guessing passwords for the account. There are numerous online and offline methods for guessing passwords that are being used. Inclusion of CAPTCHA in programs is the popular solution to avoid guessing when online.

The offline technique needs no computing resources, but it is based on guessing passwords multiple times while lettering them in such way that it is known to be repetitive.

4.1.1.3 Privacy/Confidentiality challenges

In order to ensure privacy, policies and regulations are often devised the aim of which is to regulate access to consumer data.

Thus, to diffuse attacks, a need in creating security enquiries that shall be neither confidential to operators norbiased against individual users.

4.1.2 Usability Challenge

Due to the convenience of using the same password indifferent domains and programs, accessibility is considered a key difficulty in handling user accounts. Yet it is a challenge that en dangers personal protection and secrecy.

4.1.2.1 Problems Related to management

It consists many issues, like organizational security many people whom,owing similarity of passwords and verification concerns, wish to use the system. They don't comprise of values that are default, texts, also companies consist of fast retrieval strategies for unexpected out breaks.

4.1.2.2 Usableness compromises

Opportunity to question usableness offers some capacity for the individual. Audio and Graphical trials somehow be acquired. Use of the similar key is a concern for user accounts on many platforms. Users are targeted by attackers without the user's knowledge by guessing user identities and passwords. Such password guessing has many policies to mitigate the difficulty of memorability of passwords.

4.1.2.3 The domino effects

A group of identical events are introduced as a result of this accumulative impact. It's a sequence of dominoes crashing, also best described as mechanical influence.

V. ACCESS MANAGEMENT TECHNIQUES

5.1 Centralization

An enterprise primary technique towards data breach is to deploy a solution to centralize views, controls and authority over user's identities. Any organization's network primary comprises of applications, databases, portals, data traffic flows, recommended measure to keep an eye on all the moving parts.

5.2 Role Based Access Control

The purpose of this type of access control is to restrict user's permission to their roles inside the infrastructure for example, an old employee of a firm should not have access to digital financial account. Any enterprise for most security measure should be to assign clear and designated roles to users. RBAC helps in facilitating, Cyber Security Visibility, Business Processes, Identity Security is also of immense importance not to grant relaxations to users outside their roles, temporary privileges should expire in under a certain timeline.

5.3 Zero Trust Identity Security

In corporation of multiple check point to get your identity authenticated and is called zero trust identity security. In a nutshell, any organization should never trust anyone under any circumstances. They should not allow anyone to get connected to your database and network. It should first undergo a series of steps to authenticate.

5.4 Principle of Least Privilege

This technique parallels RBAC as they both work to limit privilege being granted to users. This highlights that users should only be granted those permissions which are necessary for their specific job or role.

5.5 Automated On boarding

Automated on boarding process ensures that the users get started just with the right permissions.

5.5 Orphaned Account Detection and Removal

Failure in the process of employees off boarding results in management failures and allows the cyber criminals to use these accounts as gateways to breach into the system and result in cyber-attack.

Techniques should be implemented to mandate and automate the process of off boarding to make sure that nor phaned accounts have slip pass identity security.

5.7 MFA

Single factor authorization hasn't proven to be reliable barrier various vulner abilities. Cyber criminals can easily guess password-based logins systems or applications etc. Moreover, user's repetitively using username passwords for multiple sites for their ease has made it easier for cybers cams.

5.8 KBA

Asking the right questions with the right data is not enough to refine the KBA tool for reliable, efficient and stable identity authentication. Although various research suggest consuming a graphical or image authentication mechanism, yet Textual KBA is still a widely used authentication method. The method has its own downside which makes it challenging to protect against attackers. Therefore, there is no single sustain able model that fits all organizations' needs.

VI. CONCLUSION

The protection of data is crucial to maintain critical operational information for a company. The use of additional resources like MFA has been utilized to establish control over data. Not only does Multi Factor Authentication (MFA) add an additional step when authenticating users but also adds another layer of assurance and security. Logging of MFA attempts can be viewed and used in security analyst work. Knowledge Based Authentication (KBA), even with all enhancements and improvements remains an imperfect authentication method if independently introduced. KBA may be used as a wide spectrum approach to authentication if used as a component in Multi Factor Authentication (MFA). Hackers will still be able to get their hands on the data, but further effort is required than searching up public information or collecting aggregated data. In contextual based systems, KBA can be used as a contingency approach when users fail to meet the requirements for other forms of authentication.

VII. REFERENCES

[1]. Atat, R.; Liu, L.; Wu, J.; Li, G.; Ye, C.; Yang, Y.; Yi, Y. Big Data Meet Cyber-Physical Systems: A Panoramic Survey. IEEE Access2018, 6, 73603–73636. [Cross Ref]

[2]. Akinrolabu, O.; New, S.; Martin, A. Assessing the Security Risks of Multicloud SaaS Applications: A Real-World Case Study. In Proceedings of the 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 21–23 June 2019; pp. 81–88.

[3]. Akinrolabu, O.; Nurse, J.R.; Martin, A.; New, S. Cyber risk assessment in cloud provider environments: Current models andfuture needs. Comput. Secur. 2019, 87, 101600. [CrossRef]

[4]. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Comput. Sci. Rev.2019, 33, 1–48. [CrossRef]

[5]. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Integration of block chain and cloud of things: Architecture, applications and challenges. IEEE Commun. Surv. Tutor. 2020, 22, 2521–2549. [Cross Ref]

[6]. Singh, M.M.; Ching, K.W.; Manaf, A.A. A novel out-of-band biometrics authentication scheme for wearable devices. Int. J.Comput. Appl. 2018, 42, 589–601. [CrossRef]

[7]. Vehniä, V.J. Implementing Azure Active Directory Integration with an Existing Cloud Service. Master's Thesis, University ofVAASA, Vaasa, Finland, 2020.

[8]. Arunarani, A.R.; Manjula, D.; Sugumaran, V. Task scheduling techniques in cloud computing: A literature survey. Future Gener.Comput. Syst. 2019, 91, 407–415. [Cross Ref]

[9]. Bhagyoday, R.; Kamani, C.; Bhojani, D.; Parmar, V. Comprehensive Study of E-Health Security in Cloud Computing. Int. Res. J.Eng. Technol. (IRJET) 2019, 1216–1228.

[10]. Bendiab, G.; Shiaeles, S.; Boucherkha, S.; Ghita, B. FCMDT: A novel fuzzy cognitive maps dynamic trust model for cloud federatedidentity management. Comput. Secur. 2019, 86, 270–290. [CrossRef]

[11]. Yıldırım, M.; Mackie, I. Encouraging users to improve password security and memorability. Int. J. Inf. Secur. 2019, 18, 741–759.[CrossRef]

[12]. Pilar, D.R.; Jaeger, A.; Gomes, C.F.A.; Stein, L.M. Passwords Usage and Human Memory Limitations: A Survey across Age andEducational Background. PLoS ONE 2012, 7, e51067. [CrossRef] [PubMed]

[13]. Cheng, H.; Rong, C.; Qian, M.; Wang, W. Accountable Privacy-Preserving Mechanism for Cloud Computing Based on IdentityBased Encryption. IEEE Access 2018, 6, 37869–37882. [CrossRef]

[14]. Jegadeesan, S.; Azees, M.; Kumar, P.M.; Manogaran, G.; Chilamkurti, N.; Varatharajan, R.; Hsu, C.-H. An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications.Sustain. Cities Soc. 2019, 49, 101522. [CrossRef]

[15]. Faheem, M.; Akram, U.; Khan, I.; Naqeeb, S.; Shahzad, A.; Ullah, A.; Mushtaq, M.F. Cloud Computing Environment and Security

[16]. Challenges: A Review. Int. J. Adv. Comput. Sci. Appl. 2017, 8, 183–195. [CrossRef]

[17]. Veerabathiran, V.K.; Mani, D.; Kuppusamy, S.; Subramaniam, B.; Velayutham, P.; Sengan, S.; Krishnamoorthy, S. Improving secured ID-based authentication for cloud computing through novel hybrid fuzzy-based homomorphic proxy re-encryption. Soft Comput. 2020, 24, 18893–18908. [CrossRef]

[18]. Varghese, B.; Buyya, R. Next generation cloud computing: New trends and research directions.

Futur. Gener. Comput. Syst. 2018,79, 849–861. [CrossRef]

[19]. Roy, S.; Chatterjee, S.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Vasilakos, A.V. On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services. IEEE Access 2017, 5, 25808–25825.