future internet

MDPI

Article

A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure

Soumya Prakash Otta [1,*], Subhrakanta Panda [1], Maanak Gupta [2] and Chittaranjan Hota [1]

[1] Department of Computer Science and Information Systems, Birla Institute of Technology and Science-Pilani, Hyderabad Campus, Secunderabad 500078, India

[2] Department of Computer Science, College of Engineering, Tennessee Tech University, Cookeville, TN 38505, USA

* Correspondence: p2016300@hyderabad.bits-pilani.ac.in

Abstract: The unauthorized usage of various services and resources in cloud computing is something that must be protected against. Authentication and access control are the most significant concerns in cloud computing. Several researchers in this field suggest numerous approaches to enhance cloud authentication towards robustness. User names and associated passwords have been a common practice for long as Single Factor Authentication. However, advancements in the speed of computing and the usage of simple methods, starting from the Brute Force technique to the implementation of advanced and efficient crytographic algorithms, have posed several threats and vulnerabilities for authentication systems, leading to the degradation of their effectiveness. Multi-factor authentication has emerged as a robust means of securing the cloud using simultaneous and multiple means of authentication factors. This employs multiple levels of cascaded authentication checks. This paper covers an extensive and systematic survey of various factors towards their adoption and suitability for authentication for multi-factor authentication mechanisms. The inference drawn from the survey is in terms of arriving at a unique authentication factor that does not require any additional, specialized hardware or software for multi-factor authentication. Such authentication also uses the distinct biometric characteristics of the concerned user in the process. This arrangement augments the secured and robust user authentication process. The mechanism is also assessed as an effective means against impersonation attacks.

Keywords: access control; authentication management; authorization management; biometrics; cloud computing; cloud IAM; multi-factor authentication; user identity

check for updates

Citation: Otta, S.P.; Panda, S.; Gupta, M.; Hota, C. A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. Future Internet **2023**, 15, 146. https://doi.org/10.3390/fi15040146

Academic Editors: Mazdak Zamani, Rohit Tanwar, Behrang Samadi, Touraj Khodadadi, Claude Chaudet and Paolo Bellavista

Received: 26 February 2023
Revised: 26 March 2023
Accepted: 28 March 2023
Published: 10 April 2023

1. Introduction

The US Census Bureau reports that the number of employees who worked mostly from home increased three folds between 2019 and 2021, from around 9 million to about 27 million. The COVID-19 pandemic is regarded as the main reason for such an increase [1]. The reaction to the pandemic has spurred hybrid work and the cloud-based digitization of corporate operations, both of which present new security issues [2]. It is a fact that various components tightly integrate into the currently used advanced Information Technology (IT)-enabled ecosystem. In a system like this, the constituent components' functionalities are interdependent. Hence, their associated risk, threat, and vulnerability are also interdependent. The need for and the problems relating to the requirements of virtually unlimited IT resources are increasing daily. Cloud computing addresses such a need for vast and high-speed information processing. According to Boonkrong [3], users are vulnerable to various security issues, including access control, while accessing the system in an integrated and cloudified environment. A generic approach cannot address the associated risks, threats, and vulnerabilities in a heterogeneous environment like the cloud. Instead, specialized approaches can ensure safe and secure utilization of the cloud's IT infrastructure and cyber systems. A typical access control mechanism is required to access and use such a system.

Safe and secure accessing of a system of this nature needs a control mechanism consisting of four definite steps: identification, authentication, authorization, and auditing [4,5].

1.1. Research Background

The identification process confirms the identity legitimacy of the concerned user from the designated user name. Authentication is a definite and essential requirement of the security model to control access. The authentication process determines authorization and access permission for resources with a Boolean result method [6]. The user is prompted to input an attribute x. The system computes F(x) before comparing it with a stored corresponding value of y for the respective user following Equation (1).

$$F(x) = y \tag{1}$$

where x = Input credential, y = Verifiable parameter, and F = System function of Authentication.

The two processes, namely, identification and authorization [7–11] work hand in hand to confirm user identity. Next in the sequence is the process of authorization, which is responsible for handling restrictions and limitations or access rights for resources. The auditing process keeps track of user access for entering the system and when and what resources the identified and authenticated user has attempted to access in the form of the access log file. Considering the authentication process in more detail, it is the process responsible for validating and confirming the user's identity. A claim for ownership over a user identity may not always be true regarding Boolean results [12]. Hence, to confirm user legitimacy and further grant access permissions to the resources, evidence for confirmation of legitimacy needs to be provided and proven. The associated evidence for proof of corresponding user name (User ID) in the authentication process is termed a 'credential'.

From the historical point of view, the first known example of unauthorized access is the accidental disclosure of secret phrases used by thieves for secured gate opening and closing of hidden storage for stolen valuables, committed by Ali Baba. Similarly, in the technical community, the password was used for the first time at MIT to control access to time-shared computers among the students and faculty. Since then, many technological advancements have taken place in this direction, using user credentials for authentication. After many developments, user authentication to a system is done using either of the four commonly known ways. They are something the 'user knows' (proof-of-knowledge), 'user has' (proof-of-ownership), 'user is' (proof-of-characteristic), or 'where the user is' (proof-of-location). Any of the mentioned things are called an authentication factor [13] as depicted in Figure 1.

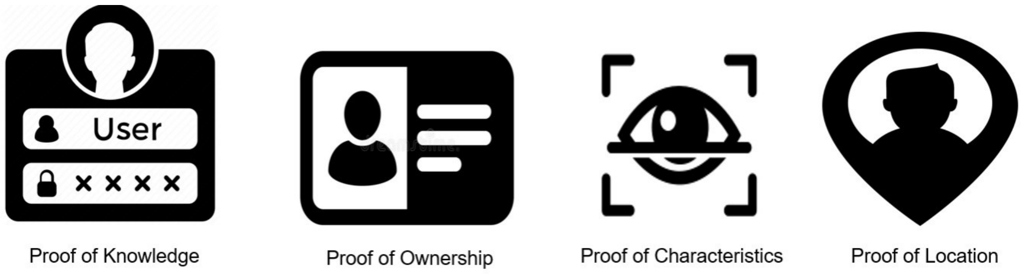

Figure 1. Fundamental Authentication Factors.

The 'user knows' a password or code that can be used as evidence for user authenticity, which is most likely to be forgotten by the user and requires safe storage for referral if not remembered. The 'user has' a hardware key or software key, which can be produced as evidence for proof. However, the same physical entity may be lost or stolen and, hence, requires a safe and secured storage and referral mechanism. Similarly, 'user is' refers to the user having a unique biometric in terms of fingerprint or retina image that can be used as evidence. Located in a logical or geographical boundary, the user may provide proof of 'where the user is' as evidence of user legitimacy. However, the accuracy of the corresponding location factor is directly dependent on the accuracy of the location detection mechanism as well as the accuracy of the Global Positioning System (GPS). The requirement for mobility and computing has led to the cloudification of lightweight and resource-constrained devices in the ecosystem. Wang et al. [14] have described the four different authentication categories and generalized the authentication model using them. However, for user convenience, a password is the most common, well-established, and widely used method for authentication [15].

With the historical and technological genesis of the usage of passwords for authentication, the domain of IT over the years has seen many advancements in terms of speed of processing, size of storage, and high throughput networks. The advent of high-speed computing and the usage of algorithms like Brute Force have weakened authentication processes using the conventional means of a username and password. In turn, this has resulted in many data breaches, compromising volumes of critical information globally. Frequent re-occurrences of such incidents put a question mark on the system of usage of the user ID and password. It also highlights the weaknesses associated with providing a robust protection mechanism against unauthorized authentication leading to undesired access to restricted and protected data. The Identity Theft Resources Centre (ITRC), in its annual report for the year 2020 [16], has listed out the root causes of identity theft and its implications, showing that 38% of data breach occurrences are due to improper cloud security configuration. It also revealed that 36% of data breaches could have occurred due to pissing attacks and related disclosure of user credentials. Upon analysis of the National Vulnerability Database (NVD) (updated up to Dec 2022) with the Common Vulnerability Scoring System (CVSS) in accordance to the Cloud Security Alliance, The Treacherous 12 [17] as well as Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 [18], it was observed that insufficient Identity and Access Management (IAM), as well as IAM, contribute cloud vulnerability by 23.6% and 45.3%, respectively, as depicted in Figure 2.

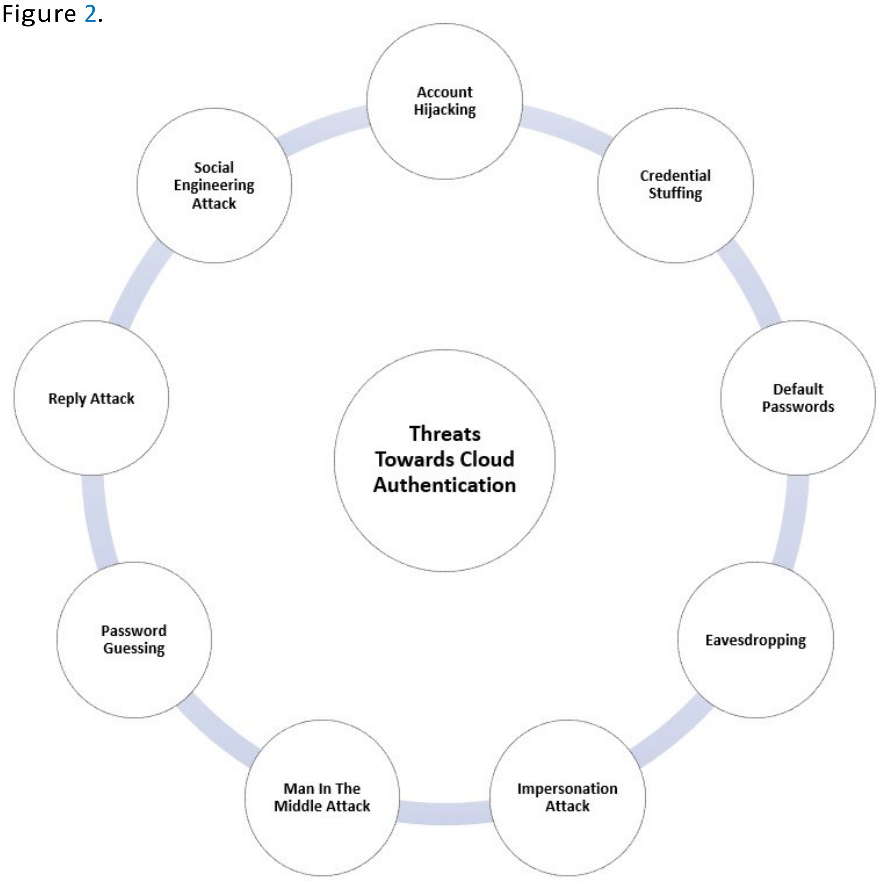

Figure 2. Contributors Towards Cloud Vulnerability.

1.2. Research Motivation

The user authentication process has the sole aim of establishing user identity by means of verification of credentials of genuine users of the system. Single Factor Authentication (SFA) was popular due to its simplicity and user-friendliness [15,19]. Mujeye [20] observed that combining two or more strong authentication measures could increase the difficulty level for guessing and breaking the SFA type of authentication. Accordingly, to increase the degree of difficulty for the attacker, researchers developed the idea of using more than one factor in a cascading manner or using one factor within another factor of authentication. Such developments gave rise to the authentication method commonly known as Multi-Factor Authentication (MFA) [21,22]. Though the overhead associated with processing more than one credential or factor check was initially relatively high, the advancement of technology and processing speed has been leveraged with newer-generation IT devices. However, based upon the type and categories of factors adopted for MFA, in almost all cases, the system requires special purpose or additional hardware equipment and software drivers associated with their fundamental functioning. Though additional checks for authentication are frustrating for the users, the same overhead is worth the value for secure user authentication and further to the entitled IT resources. Saleem et al. [23] have conducted a detailed survey on user convenience vis-à-vis difficulty with the introduction of MFA. Otta et al. [24,25] have carried out extensive analysis on Authentication Management and Authorization Management with respect to Security As A Service, covering human users of the cloud network [26].

1.3. Outline and Contribution of Work

Biological characteristics provide uniqueness to the user. This could be used as a potential means to tackle a known threat to any authentication system called an impersonation attack, where a false user tries to act as a true user. Many surveys have been conducted covering factors of authentication. However, to the best of our knowledge and available literature, for the first time, this research work makes an effort to bring out the fact that, with no additional requirements other than the factory fitted System Accessories, biometric uniqueness of users can be used as a factor of authentication.

The broad guiding factors considered for the progress of this work are listed below, which are derived from the technological shortfalls associated with the adoption of authentication factors towards MFA and which signify the notable contributions of this research:

1. It best utilizes only the Original Equipment Manufacturer (OEM)-fitted hardware and software without requiring additional or specialized Hardware and Software.
2. Systematic analysis is conducted of various factors used for authentication in the light of multiple threats and vulnerabilities concerning user authentication for cloud environment.
3. Systematic analysis is also conducted of available methods and means to be used to identify and make the best use of the least complex solution or combination of solutions towards implementing an efficient MFA for a Multi-Cloud scenario.

The organization of the rest of the paper is as follows: After introducing this topic in Section 1, Section 2 describes the aspects of the authentication process along with Cloud Authentication mechanisms. Section 3 dwells upon the various factors of authentication. Section 4 presents an extensive analysis of security aspects associated with authentication in light of facial recognition. Section 5 concludes the paper along with a brief insight into the future scope of this research work.

2. Authentication Process

Authentication is required to verify a user's identity and prevent unauthorized individuals from accessing the system [27,28]. It differs from identification, which is the first step in confirming a user's identity by requesting credentials. The second stage in the authentication process is authorization, which establishes the user's credentials with the system.

The NIST 800-63-B [29] provides recommendations on the types of authentication processes as well as the authenticator types. This process has been deliberated upon in detail by Otta et al. [25] for the cloud environment.

2.1. Traditional Authentication

It is an established fact that user verification is possible through four authentication types used for this purpose. However, Cloud Service Providers (CSPs) can combine these types to provide a more secure authentication method [30]. CSPs choose the different types based on their number of users, economic cost factors for the authentication process, a specific type or combination of their security requirements, and the cost of managing the authentication system storage of authentication credentials, to name a few [31]. The various types, along with their specific means of implementation desired for this work, are described as follows.

2.1.1. Proof-of-Knowledge

The knowledge, in this case, is best known as cognitive information because only a genuine user has access to the actual desired information for proof. This type of authentication has a prominent issue because it can be shared with others who can comfortably impersonate genuine users [32,33]. Another disadvantage is that it is simple to render it ineffective by employing various advanced guessing tools and technical methods such as Brute Force. This type of authentication also necessitates extensive character memorization and, as a result, is easily forgotten.

2.1.2. Proof-of-Ownership

This type of authentication is also known as authentication by ownership or authentication in possession. In this, the user has to be in possession of the device or object to strengthen the authentication process. In general, the owners of these objects must spend significant effort to ensure their safe custody. The replacement of lost, stolen, or damaged objects is expensive in this case and is thus regarded as a considerable weakness [34]. When used as standards, these objects have inherent flaws that expose them to other vulnerabilities like duplication, forgery, and manipulation [35].

2.1.3. Proof-of-Characteristic

This uses humanistic characteristics about a person to describe the user's uniqueness. It is commonly referred to as biometric authentication. Such authentication is linked to a person, so forging or stealing an identity is more difficult. Furthermore, this type of authentication cannot be lost or stolen [36]. High-security systems and sites widely use this type of authentication because it is difficult to compromise. Such authentication does not necessitate human intervention because the process automatically determines the user's identity [37]. Automated measurements compare the captured entity with the stored entity in real time. When compared to other types of authentications, this one is more robust.

2.1.4. Proof-of-Location

Such type of authentication records when and where the user logged in. This authentication process uses the user's location to determine their identity. This type of authentication commonly uses a GPS [38], IP address, cell tower ID, and so on. The majority of Location-Based Authentication (LBA) implementations essentially require the use of a location signature (LS), which is generated with the assistance of a location signature sensor (LSS) [39]. The location signature describes the person's physical location and the timestamp of the access request.

2.2. Cloud Authentication Mechanism

Four processes comprising the access control [40] mechanism are best described by identification, authentication, authorization, and accounting, as proposed by

Ahmad et al. [41]. Identification refers to uniquely defining and describing each user of the cloud system with an associated set of credentials. An individual must provide a credential for establishing their identity in an authentication process. Different systems may necessitate various forms of credentials. An individual is frequently required to produce a credential as a password in today's computer and communication networks. Some systems may even demand the individual to have more than one credential to be provided as proof of the user's genuineness [42]. The entire cloud authentication mechanism for users can be broadly categorized into three phases as described by Rangwani et al. [43], namely, (i) Registration, (ii) Log-in, and (iii) Verification. The authentication process can involve two parties, the Supplicant and the Authenticator. However, depending on the presence of a Responder that represents a trusted third party (TTP) [44], the authentication system could have three essential components [45]. After authentication, authorization is the next phase. Authorization is a process that deals with access restrictions and limitations on resources. Authorization explicitly specifies what each user may and may not do or access. In other words, authorization grants or restricts users' access to available resources. Accounting is the fourth component of access control [46]. Accounting keeps track of who enters the system, what they do, and at what time.

2.3. Threats towards Cloud Authentication

The system verifies the user's credentials and confirms the user's identity to authenticate the user. The system designers use several established methods to authenticate users of the system. Further access control measures for accessing system resources are enforced based on successful authentication [47]. The gravity of the situation has increased exponentially as nearly every system has been networked and connected to the internet. Passwords have traditionally been the most commonly used means of establishing identity and authorizing additional resources to the identified user. While the well-known and conventional methods give some convenience to users, they are also determined to be significantly susceptible variables that pose a significant threat to the system, user credentials, and system resources [48]. The following are some of the most well-known susceptibilities, triggering causes, and processes considering cloud authentication, as depicted in Figure 3:

1. Account hijacking: The process of an attacker stealing or hijacking a cloud account is known as cloud account hijacking. In identity theft schemes, cloud account hijacking is a typical strategy in which the attacker utilizes stolen account information to carry out illegal or unauthorized behavior. In reality, the attacker usually impersonates the account owner using stolen credentials to hijack a cloud account [49]. Attackers might use stolen credentials to access sensitive sections of cloud computing systems, jeopardizing their security, integrity, and availability.
2. Credential Stuffing: In several cases, hackers have posted hacked and compromised credentials on the dark web. For credential stuffing, the attacker searches the dark web for a password that has already been hacked. Then, an attempt is made to pene-trate the system using the already-compromised password as a credential. Similar efforts are made with other accounts of the same user who have passwords that have been hacked to access the system. When a person has numerous accounts in the system, it is usual practice to share a single password for convenience. Users' habits of not choosing separate passwords for multiple accounts and reusing a common password are exploited in this form of attack [50]. Organizations like the Open Web Application Security Project (OWASP) have proposed many techniques to combat credential-stuffing attacks. The most generally recommended methods include us-ing separate passwords for various user accounts and using the CAPTCHA system for authentication.
3. Default Passwords: A pre-installed and factory-configured password is known as a default password. The system administrator and users do not update the default password of the system being used for convenience and occasionally due to ignorance. The failure to consider this essential factor is seen as a matter of concern for rendering

the system vulnerable to cyber-attacks [51]. As a remedy, the system urges the system user to change the default password at initial use and with similar redirections for routine password changes with a pre-defined level of difficulty. Password policies such as a minimum length, a mix of upper- and lowercase alphabets, digits, and special characters are imposed on the user.

4. Eavesdropping: The attacker uses this approach to secretly listen to and sniff private conversations between two people without their consent or knowledge. It is thought to be more straightforward if the attacker controls the system's networking equipment and network traffic [52]. Suppose that non-secured HTTP and FTP-like service traffic is sniffed using the default networking port, and data traffic are studied. In that case, an attacker can quickly uncover the password and credentials from the analyzed network's plain-text data traffic using tools or software like Wireshark. However, employing encrypted services in conjunction with standard encryption techniques may alleviate this.
5. Impersonation Attack: In such an attack, an unauthorized user or wrong user makes an attempt to act as a genuine user by fraudulently acquiring the credentials of the actual user [53]. Such attacks could lead to serious data breaches in highly secured working environments like bank and defense sectors where highly sensitive, crucial information and applications are handled. This can be controlled by using biological uniqueness associated with the user.
6. Man-in-the-Middle Attacks: A man-in-the-middle attack can steal user credentials if the attacker can get inside the sender and the receiver. The attacker may now transmit and receive all data exchanges between the two computers. As a result, the attacker can pose as a sender to the recipient and vice versa [54]. The attacker has the power to modify and delete sections of the communications in transit in addition to sending and receiving messages. As a result, the attacker can collect sensitive information, such as the username and password, and use it for malicious purposes.
7. Password Guessing: Password guessing is a technique in which an adversary attempts to guess the username and password of a legitimate user and then authenticate it as being such. The attacker merely guesses probable passwords that the user will likely use in a password-guessing attack. A brute-force attack is generally an exhaustive search that an adversary can use to guess a password. It is an attack in which the attacker attempts to generate all potential password combinations and then authenticates to the system using the username and various password combinations [55]. The time it takes to carry out this assault is determined by the password's length. A dictionary attack is when an attacker tries each word in a dictionary as a password to breach a password-protected authentication system. A password dictionary attack is still classified as both a brute-force attack and a dictionary attack. Similarly, a password-spraying assault is a sort of attack that depends on a small number of frequently utilized passwords.
8. Replay Attacks: Another prominent method of attacking authentication methods is a replay attack. The replay attack involves a hacker copying a password or credential from one organization and utilizing it to authenticate with another. The goal is to mimic the user whose credentials or passwords have been copied. The attacker replicates the message or credentials and transmits them to an authenticator, hoping they will be validated successfully [56].
9. Social Engineering Attack: Using personal and interpersonal skills is common in social engineering approaches, although it is not always essential to apply information technology. When a user is subjected to a social engineering attack, the adversary tries to persuade them so that they are obliged to disclose certain information or even do a specific action [57]. In today's world, social engineering may take three primary forms: in-person social engineering, phone social engineering, and digital social engineering.

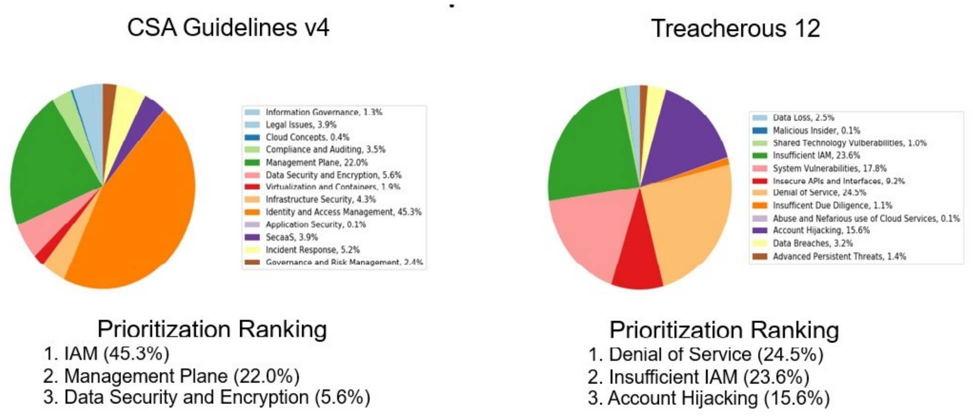

Figure 3. Threats towards Cloud Authentication.

Based on the facts mentioned above and their potential threat to the cloud in the matter of Confidentiality, Integrity, and Availability, several corrective measures are suggested as possible remedial measures. A summary of such corrective and restorative actions is described in Table 1.

Table 1. Threats to Cloud Authentication and their Remedial Measures

Potential Threat	Suggested Remedial Measures	Ref.
Account Hijacking	Use of MFA Use of One Time Password (OTP) Use of End-to-End Encryption	[21,49]
Credential Stuffing	Use of different passwords for different accounts Use of MFA	[23,50]
Default Passwords	Use of random and unique default passwords Prompting and forcing users for changing default passwords	[23,51]
Eavesdropping	Adopting strong and robust encryption mechanism	[25,52]
Impersonation Attack	Use of biometric means to uniquely identify the user Use of MFA	[53]
Man-in-the-Middle Attacks	Use of Virtual Private Network (VPN) Adopting strong and robust encryption mechanism	[25,54]
Password Guessing	Using long and strong passwords that are not obvious No reuse of same and already used password	[45,55]
Replay Attacks	Use of a strong and robust Challenge-Response means	[25,56]
Social Engineering Attack	Educating users on how to avoid being a victim of in-person, over-the-phone, and digital attacks such as phishing or e-mail attacks.	[25,57]

3. Factors of Authentication

When a user makes a genuine claim, they must furnish the desired information to demonstrate that they are who they claims to be. That desired information is an authentication factor. We dwell upon various factors as depicted in Figure 4 and analyze their strengths, weaknesses, and suitability for being used for a secured and robust authentication mechanism.

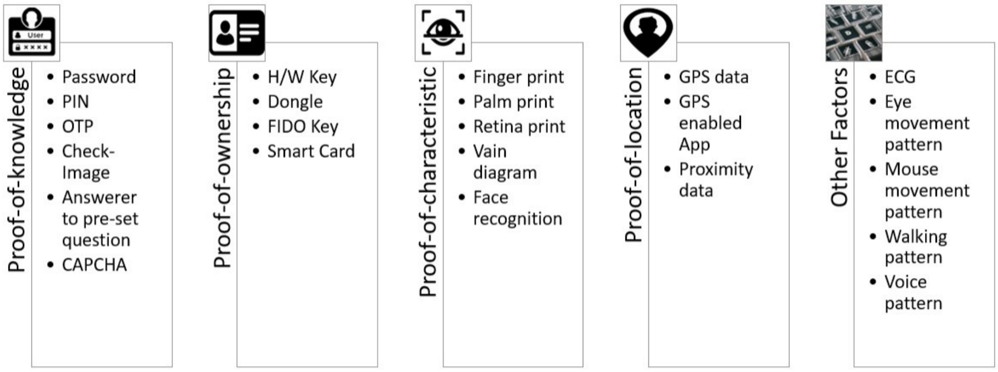

Figure 4. Various Authentication Factors.

3.1. Knowledge Factors

This refers to the verification of users' genuineness with the help of knowledge possessed by the user claiming to be genuine one. Passwords are the most commonly used means to verify a user using the knowledge factor. However, apart from forgetfulness by the human user, its safe storage and custody have always been a concern. A password is a combination of alphanumeric characters arranged in a designated sequence to act as a factor of authentication. Sometimes a specified set of some fixed number of numerical digits can be used as a Personal Identification Number (PIN) as a knowledge factor for authentication. It also uses means to accept and verify pre-stored answers submitted by users trying to authenticate into the system using the knowledge factor of the concerned user [58]. However, the related security aspect of storing the password or pre-stored answers is a concern for its storage in an unencrypted form. Moreover, the accessibility of such unencrypted storage space to users who could be unauthorized to have access to this part of storage is a notable vulnerability.

3.2. Ownership Factors

In this case, the user needs to own a device or specified object to prove genuineness in accessing the system resources. The most commonly used means in this category are photographic identity cards issued by a competent card issuing authority. An upgraded version of such a card may be a magnetic strip or chip-enabled smart card, which needs to be owned by the user to prove and establish identity to access the system. In addition, a hardware security key in the form of a dongle is one of the alternative objects that need to be owned by the user for system authentication [59]. However, the physical security of usage of such owned devices as an authentication factor is a concern since they are vulnerable to being lost or stolen and could potentially be mis-utilized by an unauthorized or malicious user.

3.3. Characteristic Factors

This factor primarily focuses on the user's unique physical and other biometric characteristics. Fingerprints, palm prints, hand geometry, face, iris, and retina are all common biometric means used as an authentication factor. Such biometric authentication procedures are divided into two parts. The first step is to register or enroll the biometric. The second step involves verification. A specialized sensing device captures biometric data during the registration process. Then the data is processed to extract and translate into a template database, from which an authentication procedure may be performed later. The authentication process starts with acquiring and processing the user's biometric data to extract and convert the person's biometric information. Biometric authentication compares a user's actual characteristics to stored data to see whether they are who they claim to be while accessing the system. Though it provides the mechanism for uniquely identifying users, it may require special hardware and corresponding software for its essential functioning [60]. The fact that human traits can change over time poses a problem for biometric authentication. These changes may result from aging, sickness, or an accident.

3.4. Location Factors

This authentication method uses the user's location to determine their identity. This sort of authentication often involves using a Global Positioning System (GPS), an IP address, and the location data of the service provider's point of presence (PoP). This authentication may also track where and when the user tries to log in. The majority of Location-Based Authentication (LBA) implementations require a location signature (LS), which is created using a location signature sensor (LSS) like a GPS. The person's actual location and the time that person seeks access are described in the location signature. After the LS has been produced, it is sent to the mechanism that verifies the user's identity. This form of authentication continues indefinitely. The LSS combines signature data with transmitted data, which the host confirms. The data from the LSS would be lost if the connection was at all hijacked [61].

3.5. Other Related Factors

With enhancements in IT-enabled speed and processing, some other means are also being adopted as a factor of authentication, especially means like the way a user speaks (voice), the way a user walks (gait), and even the way a user types (keystrokes). Hung et al. [62] have made a systematic analysis and comparison of various behavioral as well as physiological biometric factors.

4. Analysis of Authentication Factors

Several authentication techniques are in use for access control. Their strengths, weaknesses, offered opportunities, and associated threats have been deliberated upon in the SWOT analysis by Patel et al. [63]. However, a detailed analysis of authentication and corresponding factors is essential for the present work.

4.1. Comparison of Factors for Authentication

Depending on a particular type of factor or a set of factors used simultaneously, user verification can evolve as a simple but robust mechanism for user authentication. One or more factors listed in Table 2 can be used to authenticate users.

As a suggested method to mitigate the inherent weakness of password-based authentication, measures like biometric-based with multi-factor-based authentication are advised [64]. Based on the comparative analysis in Table 3 regarding various types of attack scenarios, it can be concluded that retina analysis and thermal image recognition are the least vulnerable to attacks; hence, they are the most secure approaches. However, they require specialized hardware and corresponding specialized software for their operation. On the other hand, despite being vulnerable to Spoofing attacks and Impersonation attacks, face recognition can use the standard web camera to deal with the attack scenario with a suitable solution involving a liveness aspect in place. This aspect is considered for progressing in our approach for the desired authentication mechanism.

Single-factor Authentication (SFA) depends on only one factor. Because of its convenience and user-friendliness, SFA is widely accepted by users. Among the various methods, the most common one employed is a username and password/PIN-based authentication. It is based on the knowledge factor (what-you-know). These password/PIN-based authentications have been considered weak as they are vulnerable to various attacks. Furthermore, malicious users can apply dictionary attacks [65], rainbow tables [66], or social engineering tactics to acquire access. When using this authentication method, a minimum password complexity need is usually considered. Users tend to have the same passwords over multiple websites, and a password leak from one can lead to security threats over all the user accounts on different service providers. Some notable drawbacks of this approach are as follows:

1. To access various services, users must remember the authentication factor. If one common password is used for several accounts, these programs may be affected if the password is compromised.
2. When many passwords are used, the burden of its remembrance, upkeep, and safekeeping for proof is on the users. Hence, password fatigue is evident when certain users only use one password for authentication.
3. If this factor is penetrated or compromised, the user will be unable to utilize the service until the problem is fixed. It causes a considerable delay in obtaining the desired service or information needed when it is required.
4. If a single element is compromised even without the user's knowledge, the result might be disastrous.

Table 2. Advantages and Limitations of Authentication Approaches.

Approach	Advantages	Limitations	Ref.
Face Recognition	Convenient, quick, and efficient	Large storage requirement, can create data vulnerability, compromised biometric is irrecoverable	[23,67,68]
Fingerprint Scanner	Ease of use, cost-effective	Scanners may fail, easy to replicate fingerprint, compromised biometric is irrecoverable	[61,69–71]
Geographical Location	Effective in case the user needs to be present at a particular location	GPS may not be accurate at some locations	[61,72]
Ocular-based Methods	Very efficient and difficult to spoof	Need high-quality camera and robust mathematical techniques, compromised biometric is irrecoverable and cannot be changed	[23,73,74]
OTPs	Extra layer of security, hard to crack, expires after defined time	User availability required, lack of power backup, network issue, vulnerable to man-in-the-middle attacks	[20,75,76]
SmartPhone Applications	Code regenerated in defined time gap, hence safe from attacks	User availability required, lack of power backup, network issue, invalid codes for clock de-synchronization between device and service	[21,77,78]
SmartCards	More secure using encryption technology	Card may get lost, the chip may be damaged, radio interface for two-way communication	[78–80]
Thermal Image Recognition	Efficient, can be used from a large distance	Different thermal image in case of fever	[23,81,82]
Vein Recognition	Efficient, accurate	Expensive, but still vulnerable to spoofing attacks at the current stage, compromised biometric is irrecoverable	[61,71,83]
Voice Recognition	Convenient, quick and efficient	False negative in the loud background, change in voice due to sickness; compromised biometric is irrecoverable	[61,84,85]

Table 3. Different authentication approaches and their vulnerability to various attacks.

Authentication Approach	Brute-Force Attack	Guess Attack	Phishing Attack	Spoofing Attack	Impersonation Attack	Ref.
Face Recognition	No	No	No	Yes	No	[23,67,68]
Fingerprint Scanner	No	No	No	Yes	No	[61,69–71]
Geographical Location	No	No	No	No	No	[61,72]
Ocular-based Methods	No	No	No	No (retina) & Yes (iris)	No	[23,73,74]
OTPs	No	No	Yes	No	Yes	[20,75,76]
Password/PIN	Yes	Yes	Yes	No	Yes	[14,70,71]
SmartPhone Applications	No	No	Yes	No	Yes	[21,77,78]
SmartCards	No	No	No	Yes	Yes	[78–80]
Thermal Image Recognition	No	No	No	No	No	[23,81,82]
Vein Recognition	No	No	No	Yes	No	[61,71,83]
Voice Recognition	No	No	No	Yes	No	[61,84,85]

4.2. Weakness of Single-Factor Authentication

In a recently conducted study by CyberNews, the investigation team [86] in 2021 analyzed the 15 billion passwords exposed in various database breaches. The study found that only around 2 billion of those passwords were unique. The ten most commonly used passwords are 123456, 123456789, qwerty, password, 12345, qwerty123, 1q2w3e, 12345678, 111111, and 1234567890. It signifies that even after knowing the threats associated with password security, people still prefer to use these easy-to-crack or easy-to-guess passwords. Even if people use difficult-to-guess or secure passwords, there are still chances of the passwords being compromised through phishing and spoofing attacks.

Due to the dependency on telecommunication and data networks, associated factors like OTP, CAPTCHA, PIN, and modern methods like RFID have definite vulnerabilities while functioning as an SFA. User characteristic factors like biometrics are potentially more stable due to their uniqueness associated with the corresponding user.

4.3. Emergence of Multi-Factor Authentication

Although any number of factors discussed above may be used as an authentication factor, only a few unique and practical factors are generally used for authentication in the scheme of MFA (using several factors simultaneously). Some are, undoubtedly, more powerful and complicated than others. All of them, however, are more secure and protected than password-only authentication.

MFA's purpose is to verify genuine users to safeguard sensitive information by offering a layered defense and making it more difficult for unauthorized persons to acquire access. The advantage of using MFA is that it provides a more secure approach to authenticating users. Any factor that has been compromised or exposed to a data breach is no longer usable; nevertheless, the system can continue to provide authentication services using the non-compromised authentication factors. To obtain access to a target system, attackers must overcome several obstacles [87].

The concept of MFA started with the physical verification of the user's identity card and verifying the user's photo with the corresponding authenticated photo present on the officially issued identity card. For example, when a person enters a bank, they are asked to show a photo ID. The person is then identified and authenticated based on their biometric parameters. That is, the bank matches the face of the person with the face on the ID card. It is a form of facial recognition and can be analogous to today's biometric authentication method. To generalize, this combined effect of more than one authentication factor and their unified and simultaneous utilization for user verification is represented in Equation (2).

$$F(x) = f1(x1) [\ f2(x2) \quad \begin{matrix} 1, & \text{if } f1(x1) [\ g1(y1), \text{TRUE} \\ 0, & \text{otherwise.} \end{matrix} \tag{2}$$

F(x) is the Multi-factor System Authentication Function over user x with a resultant Boolean Value. f1(x1) is the First Authentication Factor Function with input value x1; g1(y1) is the Second Authentication Factor Function with the input value y1; and so on, for its applicability to third and subsequent factors for authentication.

4.4. Related Research Conducted on MFA

Several researchers have explored the aspects associated with various factors for authentication. Multiple factors have also been employed simultaneously for MFA. Their efficacy and salient aspects are considered for the present research scope without requiring additional hardware or software other than the OEM-supplied and installed system components.

Dasgupta et al. [88] proposed an Adaptive-MFA approach. The system chooses the best authentication modalities among many based on the current scenario, like surrounding lighting or noise conditions. The modalities with which the authentication occurs are not fixed. Thus, the dynamic nature reduces the risk of various attacks on the system. It also ensures that the same factors are not used for authentication for two consecutive times, thus reducing the risk of attacks. The limitations of the above system include that it is very complex and requires ample storage space. Storing all factors is not suitable for versatile applications. This system uses lots of external hardware and degrades the user experience during the sign-up phase. Hence, this approach is also not ideal for the presently defined scope of research.

Aboaba et al. [89] proposed an approach based on smartcards and fingerprint biometrics taken together for MFA. The extracted feature from the fingerprint is applied to a fingerprint template and stored in an encrypted format in the smart card. The limitations are that fingerprints can be spoofed and cards can be stolen. This approach uses an external device not under the present scope and terms of reference.

Sciarretta et al. [90] proposed an approach based on the generation of OTPs. It deals with three entities—user, service provider, and identity provider. During the user registration phase, it builds a trusting relationship between the identity provider app and the service provider app. Then, after the activation, every time the user wants to log in, an OTP is created inside the application and sent to the identity provider along with user details. The identity provider verifies the details and checks the validity of the OTP. If everything is in order, it allows the user to sign in. This method is relatively secure as the transmission between the applications is cryptographically secure and it times the OTPs. The limitation is that it needs a phone to be available with the user each time. It requires an additional device to be there with the user, and this does not fit into our system as we intend to achieve this without using any external device.

Hammad et al. [91] proposed a solution using CNN based on a decision-level fusion of fingerprint and ECG. It uses internal fusion to fuse the crucial features of each biometric to improve accuracy. This authentication process is slow and requires high power consumption. The ECG machine is quite costly. Similarly, this method is unsuitable for our present scope since external devices are not solicited. This process is slow, and it hinders the user experience as well.

Zimmermann et al. [92] conducted a study on subjective user perceptions and objective features of the various authentication schemes. The password-based authentication is the most preferred scheme according to the users. It is easy to use and effortless because it is familiar to the users. However, it has a high cognitive load for the users, such as remembering the password. After the password, the fingerprint scheme (followed by face and iris recognition) is preferred in terms of preference, effort, security, and intention to use. The smartphone-based methods were least selected because of the high effort, more login time, and error-prone quality. It shows that user preference correlates with usability and not security and privacy.

AL Saleem et al. [23] proposed an MFA approach using a recall-based system. The user must select three images from different categories during the sign-up process. Then, every time the user logs in, they must choose those three images from a list of many images. As a third factor, the approach uses a PC ID so the user cannot log in from a different PC. The PC needs to be allowed by the admin beforehand. The advantage of this approach is that it adds a layer of security, is easy to use, and has low-cost requirements. This recall-based approach is somewhat similar to the knowledge-based approach and has the same disadvantages. The user needs to remember what image was selected during sign-up, which increases the cognitive load on the user and degrades the user experience. There is a trade-off between ease of use and achieving security. Hence, this approach does not fit into our system, wherein we want to accomplish both ease of use and security.

Sharma et al. [93] proposed a fingerprint-recognition-based approach. The fingerprint template stored in the database is in the form of a 3D spiral curve. Even if the database is compromised, it can not extract helpful information from the stored template. Once the template is compromised, it creates a new template for the same fingerprint by changing the key-set values. The only limitation is when the fingerprints are stolen from another source and the spoofed ones are used with this system. This system uses an external device and hinders the user experience, which does not suit our defined requirements.

Abdelkader et al. [94] utilized a chatbot capable of generating authentication challenges for the system. It is also in a situation to evaluate user responses, along with the necessary functionalities for the smooth operation of the framework system.

An extensive analysis of most of the prominent measures researched for MFA from 2016 to 2022 has been carried out. Table 4 presents a detailed analysis of the advantages and limitations of these mentioned methods. The cost factor associated with the implementation of MFA depends on the type of additional hardware and software required for MFA implementation. This is in addition to the cost of the system implementation or even the infrastructure being hired from a CSP [95]. This research considers our current requirement of not including any additional hardware or software for the functioning of MFA. Moreover, from these analytical results, it can be inferred that the Impersonation Attack scenario for authentication, in particular, Cloud Authentication, requires due deliberation and further research.

Table 4. Comparison of various MFA Approaches and Inherent Vulnerability.

Ref. (Year)	Advantages	Limitations	Inherent Vulnerability
[88] (2016)	(i) Dynamic and environment dependent to choose most suited modalities. (ii) Reduces predictability for the attacker. (iii) Positive experience regarding usability.	(i) Quite complex. (ii) Requires large storage. (iii) Registration is lengthy as multiple input of biometrics of the user is required for password creation.	Depends on a particular set of approaches selected at a time
[89] (2017)	The data is stored in the smartcard in an encrypted way.	(i) Card may be lost or stolen. (ii) Spoofed fingerprints from other sources may be used.	Spoofing attack
[90] (2018)	(i) Secured approach. (ii) Transmissions are encoded cryptographically. (iii) OTPs are timed.	(i) Requires downloading of different app. (ii) Unavailability of smartphone.	Phishing attack
[91] (2019)	The combination of the fingerprint with ECG is more secure as it provides the liveness factor.	Slow and requires high power consumption; costly.	NA
[92] (2020)	(i) Use of textual and figurative credentials. (ii) Use of human factors.	(i) More cognitive on the human brain. (ii) Special hardware for human-specific biometric verification	Guessing attack
[23] (2021)	(i) Cheap and secure in comparison to textual passwords. Anti-key-logger and anti-screen recorder	(i) Increases cognitive load of the user. (ii) A small approach, not suitable on a large scale. (iii) More time-consuming.	Phishing attack
[93] (2021)	Templates are such that attackers cannot access the original fingerprint details from them	Fingerprints may be stolen from other sources and spoofed	Spoofing attack
[94] (2022)	(i) Uses Autonomous Inquiry-based Authentication Chatbot (AIAC). (ii) Human Dynamics Insight And Metrics segment of the authentication framework is used.	(i) Chatbot needs sufficient training on user credential data. (ii) It incorporates a huge credential dataset depending on the number of registered users of the system.	(i) Impersonation attack. (ii) Central point of failure of the authentication process.

4.5. Face Recognition towards Potential MFA

The detailed comparative analysis mentioned above concludes that factors of authentication other than facial recognition entail the requirement of specialized and additional hardware as well as software. They may even require specialized user training for flawless utilization of the authentication factors. At the same time, using such specialized means as an authentication factor is liable to affecting the uninterrupted user experience in a logged-in user session. Considering the user's face to be utilized as a biometric authentication factor, it essentially requires three mutually related processes for facial recognition. The processes are:

1. Capturing of the image.
2. Detection of the face in the captured image.
3. Comparison of detected facial features with the registered user's stored credentials.

For capturing a simple image, a system-connected webcam is recommended to be used without asking for additional hardware components. However, the detection of the user's face in the captured image as well as recognition of the registered user's facial features need due deliberation to meet the need for robust authentication.

Capturing the face image of the user and the comparison of biometric features and the stored user's credentials is a relatively simpler process. In a cloud environment, the CSP serves multiple tenants, and each tenant could have multiple and huge numbers of users, leading to related complexity for user authentication. Similarly, in a multi-cloud infrastructure, inter-operability among multiple CSPs further complicates the user authentication and associated access control issues [96]. From the above-presented analysis and present survey, the potential of using face recognition towards MFA for cloud infrastructure is considered. A simple but effective face recognition mechanism with OEM-fitted web cameras of the system can be a potential means for MFA and also for tackling impersonation attacks.

4.6. Threats to MFA

At the same time, there are multiple threats envisaged in the implementation and adoption of Multi-Factor Authentication (MFA). The most prominent threats, which have a direct effect on the scope of the present research for threat modeling of MFA, are listed in Table 5.

Table 5. Prominent Threats to MFA Implementation.

Threat	Envisaged Effect
Biometric Spoofing	Biometric authentication mechanisms may be vulnerable to spoofing attacks, where attackers create fake biometric data to fool the authentication system.
Credential stuffing	Attackers may use stolen MFA credentials to gain access to other accounts belonging to the same user.
Denial of Service (DoS) attacks	Attackers may launch DoS attacks against the authentication system, preventing legitimate users from accessing their accounts.
Insider Threats	Employees or contractors with access to sensitive systems may abuse their privileges to bypass MFA or steal MFA credentials.
Malware	Malicious software such as keyloggers or screen capture tools may be used to steal MFA credentials from infected devices.
Man-in-the-middle attacks	Attackers may intercept communication between users and the authentication system, allowing them to steal MFA credentials.
Social Engineering	Attackers may attempt to trick users into divulging their MFA credentials through phishing attacks or other forms of social engineering.

5. Conclusions and Future Work

MFA is an effective means of increasing the difficulty for intruders to gain unauthorized access to the system. MFA ensures secured access to resources for interactions between users and cloud infrastructure by facilitating efficient, user-friendly, and trustworthy authentication whenever accessing a service. This paper presented a systematic approach to determine a factor, particularly biometric face recognition, without disturbing a logged-in user from ongoing work and without requiring additional hardware and software for the system.

Performance consistency and efficiency should be further experimentally established for various associated phases of MFA system functioning. This research effort aims to prevent impersonation attacks on the system since the uniqueness of the user's biometric facial characteristics is being considered as a factor of authentication [97] as a part of the MFA process. This is to avoid dependency on TTP and make use of a DLT-based storage.Having credentials with advanced cryptographic means, an MFA solution based on the Physically Unclonable Function (PUF) [98] would have an edge over the classical solutions. However, needing further exploration is the trade-off between performance and security of user authentication using state-of-the-art facial recognition based on Non-Convoluted Neural Network (Non-CNN) and Convoluted Neural Network (CNN) algorithms [99] against impersonation attacks. Such effort is expected to handle the potential spoofing attacks by means of a liveness check of the user and provide a means of secured user authentication for the cloud environment and multi-cloud infrastructure.

MFA is vulnerable to social engineering attacks and many researchers are continuously exploring the options for its detection and prevention. Similarly, a simple DoS attack, by blocking the second authentication channel, could also affect the system effectiveness. The usage of cryptography techniques coupled with suitable measures, such as Network Traffic Monitoring, Implementing Traffic Load Balance Functionality, Using of Content Delivery Networks Functionality, and especially Implementing Data-Rate Limiting Approach to and from suspected IP addresses, is a suggested way to tackle possible DoS attacks on MFA systems.

Author Contributions: Conceptualization, S.P.O. and S.P.; methodology, S.P.O., C.H. and M.G.; writing—original draft preparation, S.P.O.; validation, S.P., C.H. and M.G.; formal analysis, S.P.O.; investigation, S.P. and C.H.; writing—review and editing, M.G.; visualization, S.P.O.; supervision, S.P.O. and M.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank BITS Pilani (Hyderabad, India) and Tennessee Tech University (Tennessee, USA) for supporting this work.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

CNN	Convoluted Neural Network
CSP	Cloud Service Provider
LBA	Location-Based Authentication
MFA	Multi-Factor Authentication
PIN	Personal Identification Number
SFA	Single Factor Authentication
TTP	Trusted Third Party

References

1. Cybersecurity: Trends from 2022 and Predictions for 2023. Available online: https://www.infosecurity-magazine.com/blogs/trends-from-2022-predictions-for/ (accessed on 1 January 2023).
2. Top Trends in Cybersecurity 2022. Available online: https://www.gartner.com/doc/reprints?id=1-29OTFFPI&ct=220411&st=sb (accessed on 3 January 2023).

3. Boonkrong, S. Multi-factor Authentication. In Authentication and Access Control: Practical Cryptography Methods and Tools; Apress: Berkeley, CA, USA, 2021; pp. 133–162. [CrossRef]
4. Figueroa-Lorenzo, S.; Añorga, J.; Arrizabalaga, S. Methodological Performance Analysis Applied to a Novel IIoT Access Control System Based on Permissioned Blockchain. Inf. Process. Manag. **2021**, 58, 102558. [CrossRef]
5. Rawal, B.S.; Manogaran, G.; Peter, A. Manage the Identification and Authentication of People, Devices, and Services. Cybersecurity and Identity Access Management; Springer Nature: Singapore, 2023; pp. 149–157. [CrossRef]
6. Mihailescu, M.I.; Nita, S.L. A Searchable Encryption Scheme with Biometric Authentication and Authorization for Cloud Environments. Cryptography **2022**, 6, 8. [CrossRef]
7. Parikshit, N.; Shashikant, M.; Bhong, S.; Gitanjali, R. Authorization and Access Control, Authorization and Access Control; CRC Press: Boca Raton, FL, USA, 2022; pp. 19–31. [CrossRef]
8. Goel, A. Access Control and Authorization Techniques w.r.t. Client Applications. Data Intelligence and Cognitive Informatics; Springer: Berlin/Heidelberg, Germany, 2022; pp. 23–44. [CrossRef]
9. Gupta, M.; Awaysheh, F.; Benson, J.; Azab, M.; Patwa, F.; Sandhu, R. An Attribute-Based Access Control for Cloud-Enabled Industrial Smart Vehicles. IEEE Trans. Ind. Infor. **2021**, 17, 4288–4297. [CrossRef]
10. Gupta, M.; Sandhu, R. Towards Activity-Centric Access Control for Smart Collaborative Ecosystems. In Proceedings of the ACM Symposium on Access Control Models And Technologies (SACMAT), Trento, Italy, 7–9 June 2021. [CrossRef]
11. Michal, T.; Amr, S.; Aishwarya, S.; Michael, C.; Tomas, C. Systematic Review of Authentication and Authorization Advancements for the Internet of Things. Sensors **2022**, 22, 1361. [CrossRef]
12. Ettore, F. Maria, E.V. Generalities on Boolean and vectorial functions. In Boolean Functions for Cryptography and Coding Theory; Cambridge University Press: Cambridge, UK, 2020; pp. 27–75. [CrossRef]
13. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. Cryptography **2018**, 2, 1. [CrossRef]
14. Wang, C.; Wang, Y.; Chen, Y.; Liu, H.; Liu, J. User authentication on mobile devices: Approaches, threats and trends. Comput. Netw. **2020**, 170, 107118. [CrossRef]
15. Wang, D.; Zhang, X.; Zhang, Z.; Wang, P. Understanding security failures of multi-factor authentication schemes for multi-server environments. Comput. Secur. **2020**, 88, 101619. [CrossRef]
16. 2020 Annual Report. Identity Theft Resource Center. Available online: https://www.idtheftcenter.org/wp-content/uploads/2021/03/03.25.2020-2020-Annual-Report-FINAL-optimized.pdf (accessed on 22 December 2022).
17. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. Available online: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ (accessed on 22 December 2022).
18. The Treacherous Twelve' Cloud Computing Top Threats in 2016. Available online: https://cloudsecurityalliance.org/artifacts/the-treacherous-twelve-cloud-computing-top-threats-in-2016/ (accessed on 22 December 2022).
19. Ferrag, M.A.; Maglaras, L.; Derhab, A.; Janicke, H. Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. Telecommun. Syst. **2019**, 73, 317–348. [CrossRef]
20. Mujeye, S.; Levy, Y.; Mattord, H.; Li, W. Empirical results of an experimental study on the role of password strength and cognitive load on employee productivity. J. Appl. Knowl. Manag. **2016**, 4, 99–116. [CrossRef]
21. Sain, M.; Normurodov, O.; Hong, C.; Hui, K.L. A Survey on the Security in Cyber Physical System with Multi-Factor Authentication. In Proceedings of the 23rd International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 7–10 February 2021. [CrossRef]
22. Federico, S.; Roberto, C.; Gabriele, C.; Nicola, Z. A survey on multi-factor authentication for online banking in the wild. Comput. Secur. **2020**, 95, 101745. [CrossRef]
23. ALSaleem, B.O.; Alshoshan, A.I. Multi-Factor Authentication to Systems Login. In Proceedings of the 2021 National Computing Colleges Conference (NCCC), Taif, Saudi Arabia, 27–28 March 2021. [CrossRef]
24. Otta, S.P.; Panda, S. Decentralized Identity and Access Management of Cloud for Security as a Service. In Proceedings of the 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 3–8 January 2022. [CrossRef]
25. Otta, S.P.; Panda, S. Cloud Identity and Access Management Solution with Blockchain. In Blockchain Technology: Applications and Challenges; Springer: Berlin/Heidelberg, Germany, 2021; pp. 243–270. [CrossRef]
26. Gupta, M.; Sandhu, R.; Mawla, T.; Benson, J. Reachability analysis for attributes in ABAC with group hierarchy. IEEE Trans. Dependable Secur. Comput. **2022**, 20, 841–858. [CrossRef]
27. Barkadehi, M.H.; Nilashi, M.; Ibrahim, O.; Fardi, A.Z.; Samad, S. Authentication systems: A literature review and classification. Telemat. Infor. **2018**, 35, 1491–1511. [CrossRef]
28. Huang, J.C.; Shu, M.H.; Hsu, B.M.; Hu, C.M. Service architecture of IoT terminal connection based on blockchain identity authentication system. Comput. Commun. **2020**, 160, 411–422. [CrossRef]
29. NIST Special Publication 800-63B. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf (accessed on 22 December 2022).
30. Ibrokhimov, S.; Hui, K.L.; Al-Absi, A.A.; Sain, M. Multi-factor authentication in cyber physical system: A state of art survey. In Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 17–20 February 2019. [CrossRef]

31. Zahid, G.; Shafiq, A.; Khalid, M.; Hafizul, S.; Mohammad, M.H.; Giancarlo, F. An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical-Social-Systems. IEEE Access **2020**, 8, 47144–47160. [CrossRef]
32. Malina, L.; Dzurenda, P.; Hajny, J.; Martinasek, Z. Secure and efficient two-factor zero-knowledge authentication solution for access control systems. Comput. Secur. **2018**, 77, 500–513. [CrossRef]
33. Gajmal, Y.M.; Udayakumar, R. Analysis of Authentication based Data Access Control Systems in Cloud. J. Adv. Res. Dyn. Control Syst. **2020**, 12, 2961–2967. [CrossRef]
34. Li, Q.; Zhang, Q.; Huang, H.; Zhang, W.; Chen, W.; Wang, H. Secure, Efficient, and Weighted Access Control for Cloud-Assisted Industrial IoT. IEEE Internet Things J. **2022**, 9, 16917–16927. [CrossRef]
35. Prajapati, P.; Shah, P. A review on secure data deduplication: Cloud storage security issue. J. King Saud Univ.-Comput. Inf. Sci. **2022**, 34, 3996–4007. [CrossRef]
36. Yuan, C.; Shuai, G.; Xindi, H. A Secure Authentication Mechanism for Multi-Dimensional Identifier Network. In Proceedings of the 2022 International Conference on Networking and Network Applications (NaNA), Urumchi, China, 3–5 December 2022. [CrossRef]
37. Neha, C.K. Biometric re-authentication: An approach towards achieving transparency in user authentication. Multimed. Tools Appl. **2018**, 78, 6679–6700. [CrossRef]
38. Zuriati, A.; Zukarnain, A.M.; Mohd, K. Authentication Securing Methods for Mobile Identity Issues, Solutions and Challenges. Symmetry **2022**, 14, 821. [CrossRef]
39. Alamleh, H.; AlQahtani, A.A.S. Architecture for continuous authentication in location-based services. In Proceedings of the 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Zallaq, Bahrain, 20–21 December 2020. [CrossRef]
40. Gupta, M.; Sandhu, R. Authorization framework for secure cloud assisted connected cars and vehicular internet of things. In Proceedings of the 23nd ACM Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 7 June 2018. [CrossRef]
41. Ahmad, W.; Rasool, A.; Javed, A.R.; Baker, T.; Jalil, Z. Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. Electronics **2021**, 11, 16. [CrossRef]
42. Eranga, B.; Sachin, S.; Ravi, M.; Xueping, L.; Peter, F.; Nalin, R. Casper: A blockchain-based system for efficient and secure customer credential verification. J. Bank. Financ. Technol. **2021**, 6, 43–62. [CrossRef]
43. Rangwani, D.; Om, H. A Secure User Authentication Protocol Based on ECC for Cloud Computing Environment. Arab. J. Sci. Eng. **2021**, 46, 3865–3888. [CrossRef]
44. Cathey, G.; Benson, J. Edge centric secure data sharing with digital twins in smart ecosystems. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021; pp. 70–79.
45. Boonkrong, S. Methods and Threats of Authentication. In Authentication and Access Control; Springer: Berlin/Heidelberg, Germany, 2021; pp. 45–70. [CrossRef]
46. Carlsson-Wall, M.; Lukas, G.; Jesper, H.; Kalle, K.; Carl-Johan, N. Exploring the implications of cloud-based enterprise resource planning systems for public sector management accountants. Financ. Account. Manag. **2021**, 38, 177–201. [CrossRef]
47. Pasika, R.; Anca, D.J.; Madhusanka, L. Survey on Multi-Access Edge Computing Security and Privacy. IEEE Commun. Surv. Tutor. **2021**, 23, 1078–1124. [CrossRef]
48. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Comput. Sci. Rev. **2019**, 33, 1–48. [CrossRef]
49. Nafea, R.A.; Ami, A.M. Cyber Security Threats in Cloud: Literature Review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021. [CrossRef]
50. Tankard, C. Credential stuffing—The New Hack. Netw. Secur. **2021**, 2, 20. [CrossRef]
51. AlHumaidan, Y.; AlAjmi, L.; Aljamea, M.; Mahmud, M. Analysis of Cloud Computing Security in Perspective of Saudi Arabia. In Proceedings of the 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018. [CrossRef]
52. Sun, X. Critical Security Issues in Cloud Computing: A Survey. In Proceedings of the 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Omaha, NE, USA, 3–5 May 2018. [CrossRef]
53. Lu, Y.; Zhao, D. Providing impersonation resistance for biometric-based authentication scheme in mobile cloud computing service. Comput. Commun. **2022**, 182, 22–30. [CrossRef]
54. Malani, S.; Srinivas, J.; Das, A.K.; Srinathan, K.; Jo, M. Certificate-based anonymous device access control scheme for IoT environment. IEEE Internet Things J. **2019**, 6, 9762–9773. [CrossRef]
55. Kumar, G.S.; Kandavel, N.; Madhavan, K. To Discovery The Cloud Services Authentication An Expert Based System Using Multi-Factor Authentication. In Proceedings of the 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 March 2020. [CrossRef]
56. Singh, V.; Pandey, S.K. Revisiting Cloud Security Threats: Replay attack. In Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 14–15 December 2018. [CrossRef]

57. Ye, Z.; Guo, Y.; Ju, A.; Wei, F.; Zhang, R.; Ma, J. A Risk Analysis Framework for Social Engineering Attack Based on User Profiling. J. Organ. End User Comput. **2020**, 32, 37–49. [CrossRef]
58. Velásquez, I.; Caro, A.; Rodríguez, A. Authentication schemes and methods: A systematic literature review. Inf. Softw. Technol. **2018**, 94, 30–37. [CrossRef]
59. Ometov, A.; Petrov, V.; Bezzateev, S.; Andreev, S.; Koucheryavy, Y.; Gerla, M. Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications. IEEE Netw. **2019**, 33, 82–88. [CrossRef]
60. Abbott, J.; Patil, S. How Mandatory Second Factor Affects the Authentication User Experience. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 17 June 2020. [CrossRef]
61. Jaikla, T.; Pichetjamroen, S.; Vorakulpipat, C.; Pichetjamroen, A. A Secure Four-factor Attendance System for Smartphone Device. In Proceedings of the 2020 22nd International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 16–19 February 2020. [CrossRef]
62. Tse, K.W.; Hung, K. User Behavioral Biometrics Identification on Mobile Platform using Multimodal Fusion of Keystroke and Swipe Dynamics and Recurrent Neural Network. In Proceedings of the 2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 18–19 April 2020. [CrossRef]
63. Patel, S.C.; Jaiswal, S.; Singh, R.S.; Chauhan, J. Access Control Framework Using Multi-Factor Authentication in Cloud Computing. Int. J. Green Comput. **2018**, 9, 1–15. [CrossRef]
64. Six Types of Password Attacks & How to Stop Them. Available online: https://www.onelogin.com/learn/6-types-password-attacks (accessed on 27 June 2022).
65. Subangan, S.; Senthooran, V. Secure authentication mechanism for resistance to password attacks. In Proceedings of the 2019 19th International Conference on Advances in ICT for Emerging Regions (ICTer), Colombo, Sri Lanka, 2–5 September 2019. [CrossRef]
66. Alpatskiy, M.A.; Borzunov, G.I.; Epishkina, A.V.; Kogos, K.G. New Approach in the Rainbow Tables Method for Human-Like Passwords. In Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 27–30 January 2020. [CrossRef]
67. Liu, S.; Song, Y.; Zhang, M.; Zhao, J.; Yang, S.; Hou, K. An Identity Authentication Method Combining Liveness Detection and Face Recognition. Sensors **2019**, 19, 4733. [CrossRef] [PubMed]
68. Musa, A.; Vishi, K.; Rexha, B. Attack Analysis of Face Recognition Authentication Systems Using Fast Gradient Sign Method. Appl. Artif. Intell. **2021**, 35, 1346–1360. [CrossRef]
69. Kakkad, V.; Patel, M.; Shah, M. Biometric authentication and image encryption for image security in cloud framework. Multiscale Multidiscip. Model. Exp. Des. **2019**, 2, 233–248. [CrossRef]
70. AlQahtani, A.A.S.; El-Awadi, Z.; Min, M. A Survey on User Authentication Factors. In Proceedings of the 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 27–30 October 2021. [CrossRef]
71. Adiraju, R.V.; Masanipalli, K.K.; Reddy, T.D.; Pedapalli, R.; Chundru, S.; Panigrahy, A.K. An extensive survey on finger and palm vein recognition system. Mater. Today Proc. **2021**, 45, 1804–1808. [CrossRef]
72. Eric, F.; Vendel, T.; Alexandre, K.; Radu, S. A Tale of Location-Based User Authentication. In Proceedings of the 2019 IEEE International Conference on Big Data and Smart Computing (BigComp), Kyoto, Japan, 27 February–2 March 2019. [CrossRef]
73. Almadan, A.; Rattani, A. Compact CNN Models for On-device Ocular-based User Recognition in Mobile Devices. In Proceedings of the 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA, 5–7 December 2021. [CrossRef]
74. Reddy, M.V.B.; Goutham, V. Iris Technology: A Review on Iris Based Biometric Systems for Unique Human Identification. Int. J. Res.-Granthaalayah **2018**, 6, 80–90. [CrossRef]
75. Erdem, E.; Sandikkaya, M.T. OTPaaS—One Time Password as a Service. IEEE Trans. Inf. Forensics Secur. **2019**, 14, 743–756. [CrossRef]
76. Kim, H.; Han, J.; Park, C.; Yi, O. Analysis of Vulnerabilities That Can Occur When Generating One-Time Password. Appl. Sci. **2020**, 10, 2961. [CrossRef]
77. Ozkan, C.; Bicakci, K. Security Analysis of Mobile Authenticator Applications. In Proceedings of the 2020 International Conference on Information Security and Cryptology (ISCTURKEY), Ankara, Turkey, 3–4 December 2020. [CrossRef]
78. Gordin, I.; Graur, A.; Potorac, A. Two-factor authentication framework for private cloud. In Proceedings of the 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, 9–11 October 2019. [CrossRef]
79. Bouchaala, M.; Ghazel, C.; Saidane, L.A. Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card. J. Supercomput. **2021**, 78, 497–522. [CrossRef]
80. Bobba, S.; Paruchuri, V. Single Sign-On Using Contactless Smart Cards and Fingerprint Authentication. In Advances on Broad-Band Wireless Computing, Communication and Applications; Springer: Berlin/Heidelberg, Germany, 2021; pp. 158–166. [CrossRef]
81. Aiordachioaie, D.; Culea-Florescu, A.; Pavel, S.M. On Human Faces Thermal Image Processing for Classification Purposes. In Proceedings of the 2019 6th International Symposium on Electrical and Electronics Engineering (ISEEE), Galati, Romania, 18–20 October 2019. [CrossRef]
82. Kakarwal, S.N.; Chaudhari, K.P.; Deshmukh, R.R.; Patil, R.B. Thermal Face Recognition using Artificial Neural Network. In Proceedings of the 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), Aurangabad, India, 30–31 October 2020. [CrossRef]

83. Bowyer, K.W.; Boult, T.E.; Evans, N.; Hassner, T.; Kakadiaris, I.A.; Kittler, J.; Kumar, A.; Lu, J.; Maio, D.; Marcel, S.; et al. 2020 Index IEEE Transactions on Biometrics, Behavior, and Identity Science. IEEE Trans. Biom. Behav. Identity Sci. **2020**, 2, 431–437. [CrossRef]
84. Chang, Y.T.; Dupuis, M.J. My Voiceprint Is My Authenticator: A Two-Layer Authentication Approach Using Voiceprint for Voice Assistants. In Proceedings of the 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Leicester, UK, 19–23 August 2019. [CrossRef]
85. Debnath, S.; Ramalakshmi, K.; Senbagavalli, M. Multimodal Authentication System based on Audio-Visual data: A Review. In Proceedings of the 2022 International Conference for Advancement in Technology (ICONAT), Goa, India, 21–22 January 2022. [CrossRef]
86. Most Common Passwords: Latest 2022 Statistics. Available online: https://cybernews.com/best-password-managers/most-common-passwords/ (accessed on 12 January 2023).
87. Mawla, T. Activity Control: A Vision for "Active" Security Models for Smart Collaborative Systems. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, New York, NY, USA, 8–10 June 2022; pp. 207–216.
88. Dasgupta, D.; Roy, A.; Nag, A. Toward the design of adaptive selection strategies for multi-factor authentication. Comput. Secur. **2016**, 63, 85–116. [CrossRef]
89. Oke, B.A.; Olaniyi, O.M.; Aboaba, A.A.; Arulogun, O.T. Developing multifactor authentication technique for secure electronic voting system. In Proceedings of the 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, 29–31 October 2017. [CrossRef]
90. Sciarretta, G.; Carbone, R.; Ranise, S.; Viganò, L. Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Login. Princ. Secur. Trust. **2018**, 23, 188–213. [CrossRef]
91. Hammad, M.; Liu, Y.; Wang, K. Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint. IEEE Trans. Inf. Forensics Secur. **2019**, 7, 26527–26542. [CrossRef]
92. Zimmermann, V.; Gerber, N. The password is dead, long live the password—A laboratory study on user perceptions of authentication schemes. Int. J. Hum.-Comput. Stud. **2020**, 133, 26–44. [CrossRef]
93. Sharma, U.; Tomar, P.; Ali, S.S.; Saxena, N.; Bhadoria, R.S. Optimized Authentication System with High Security and Privacy. Electronics **2021**, 10, 458. [CrossRef]
94. Voege, P.; Ouda, A. An Innovative Multi-Factor Authentication Approach. In Proceedings of the 2022 International Symposium on Networks, Computers and Communications (ISNCC), Shenzhen, China, 19–22 July 2022. [CrossRef]
95. Wenting, L.; Haibo, C.; Ping, W.; Kaitai, L. Practical Threshold Multi-Factor Authentication. IEEE Access **2021**, 16, 3573–3588. [CrossRef]
96. Aghili, S.; Sedaghat, M.; Singelée, D.; Gupta, M. MLS-ABAC: Efficient multi-level security attribute-based access control scheme. Future Gener. Comput. Syst. **2022**, 131, 75–90. [CrossRef]
97. Riseul, R.; Soonja, Y.; Soo-Hyung, K.; David, H. Continuous Multimodal Biometric Authentication. IEEE Access **2021**, 9, 34541–34557.[CrossRef]
98. Georgios, F.; Cyrus, M.; Jim, P.; Eirini, E.T. Reinforcement Learning Toward Decision-Making for Multiple Trusted-Third-Parties in PUF-Cash. In Proceedings of the 2020 6th World Forum on Internet of Things (WF-IoT), New Orleans, LO, USA, 2–16 June 2020. [CrossRef]
99. Otta, S.P.; Kolipara, S.; Panda, S.; Hota, C. User Identification with Face Recognition: A Systematic Analysis. In Proceedings of the 2022 3rd International Conference for Emerging Technology (INCET), Belgaum, India, 27–29 May 2022. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.