JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A SURVEY ON DIFFERENT AUTHENTICATION TECHNIQUES USED FOR IMPROVING SECURITY

[1]Chandan Kumar, [2]Author Name: - Dr. Manoj Lipton, [3]Chetan Agrawal
[1]Designation of 1st Author: - Research Schooler, [2]Designation of 2nd Author: - Associate Professor, [3]Designation of 3rd Author: - Asst. Professor.
[1]Name of Department of 1st Author: - Department of CSE,
[1]Name of organization of 1st Author: - Radharaman Institute of Technology & Science
Bhopal, India

Abstract: *Cloud computing is a popular topic in the IT industry, but not much is known about the risks that come with this new technology and delivery model. Because cloud computing has a lot of useful features, many organizations use cloud storage to store their important data. Users can store their data remotely in the cloud and use clients to get to it whenever they need to. This technology offers services using one of three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). This model makes it possible for users and organizations all over the world to share their important information and important computing resources. One of the main things that slows down the growth of this technology in the information technology (IT) industry is making sure that users can't get to these important resources without permission. Authentication is one of the most important ways to make sure that only the right people can use registered services. The goal of this paper is to find out what's wrong with different authentication methods and figure out how to fix them.*

Index Terms - Cloud Computing, Authenticaion Mechanism, Cipher, Cryptography.

I. INTRODUCTION

According to the NIST' [1] definition of the cloud: Cloud computing is a model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services). These resources can be rapidly provisioned and released with minimal management effort or interaction from service providers. Cloud computing is a model. Cloud computing is a model. This model of cloud computing is made up of a total of five basic qualities, three service types, and four deployment models. Essential Characteristics:

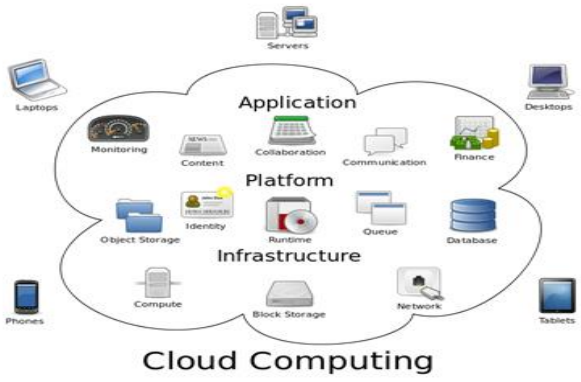

Figure 1: A cloud is used in the diagrams to depict the Internet

a) ***On-demand self-service***: A consumer is able to automatically and unidirectional provision computing capabilities, such as server time and network storage, based on their needs without being required to have human interaction with each individual service provider.

b) ***Broad network access*:** The capabilities may be accessed using conventional techniques and are made available over the network. This facilitates their usage by a variety of different thin and thick client systems (e.g., mobile phones, tablets, laptops, and workstations).

c) ***Resource pooling*:** Using a multi-tenant model, the computing resources of the provider are pooled so that they may serve numerous customers at the same time. Various physical and virtual resources are dynamically assigned and reassigned in response to the requirements of the customers. The client typically does not have any control or knowledge over the precise location of the delivered resources, but they may be able to designate location at a higher level of abstraction. This creates a perception of location independence for the customer (e.g., country, state, or datacenter). The terms "storage," "processing," "memory," and "network bandwidth" are all examples of resources.

d) Rapid elasticity: It is possible to elastically provide and release capabilities, and in certain circumstances this can be done automatically, in order to grow quickly outward and inward according with demand. The client frequently has the impression that the capabilities that are accessible for provisioning are limitless and that they can appropriate them in any quantity and at any moment. A service that is measured: By employing a metering capability at a level of abstraction that is appropriate to the sort of service being provided, cloud computing systems are able to automatically control and optimize resource use (e.g., storage, processing, bandwidth, and active user accounts). It is possible to monitor, regulate, and report on resource utilization, which provides transparency not only for the supplier of the utilized service but also for the customer of the service.

1.1 Authentication Attacks in Cloud Computing [2]

Figure 2 show the Classification of Authentication Attacks in the Cloud Environment.

Man-in-the-Middle Attack (MITM): Since the introduction of web2.0, MITM has seen a significant rise in use within the context of SAAS. In this scenario, the adversary alters the communication between the client and the server without the users' awareness by eavesdropping on the communication channel that has been created between authorized users.

Password Discovery Attack: In order to carry out this assault, the attacker uses a variety of methods to recover credentials that have been saved or communicated by a computer system. a few different tactics were utilized based on the amount of information that was accessible about the password.

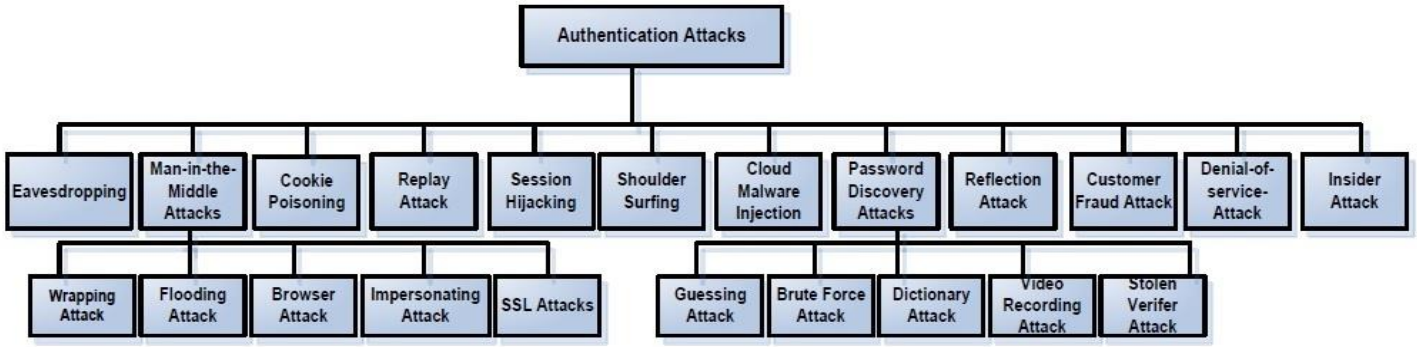

Figure 2: Classification of Authentication Attacks in the Cloud Environment [2]

Guessing Attack: People typically use passwords that are simple and easy to remember, making them susceptible to attacks based on guessing. An adversary first takes in some information relevant to the password, then makes an educated guess at what it may be, and then confirms that guess by repeatedly attempting to log in until he succeeds. Because there is no limit to the number of times the attacker may try to guess the correct password in an offline environment, the attacker has a good probability of successfully breaking the password. In contrast, when the game is played online, the user is prevented from logging in after a certain number of unsuccessful tries.

Brute Force Attack: This attack is carried out by the perpetrator attempting to guess passwords using every conceivable combination of letters, numbers, and alphabetic characters. This continues until the perpetrator successfully guesses the proper password. In order to be effective, a brute force attack—which is often carried out via automated methods—requires a significant amount of computational power and time.

Dictionary Attack: In this stage of the assault, the attacker looks through a pre-computed password dictionary in an effort to guess a password. A random password that is not based on a word that can be found in a dictionary is the best defence against this kind of assault. Even passwords written in native languages are not safe since cybercriminals have access to dictionaries for the majority of regional languages.

Attacks using Video Recording In these kinds of attacks, which are typically carried out in public locations, the perpetrators record the victim's password using a camera-equipped mobile phone or a small camera while the victim is in the process of entering the password.

Stolen Verifier Attack: This attack is carried out by the attacker by way of the verifier's password table, which is accessed by the attacker. After that, he initiates an offline guessing attack by executing a script that performs a hash on each element of the dictionary and compares the resultant message digest with the stored digest of the verifier until a match is discovered. This process continues until a match is found. When used against a cloud system that stores data for several clients, this attack has the potential to have catastrophic results. The password discovery attacks that were outlined earlier focus on getting the password of a legitimate user so that the stolen information may be used to unlawfully impersonate the user to a verifier. These kinds of attacks will be successful in authenticating the user if and only if the authentication procedure is completely dependent on static passwords. Using graphical passwords, one-time passwords, avoiding the storage of passwords, utilizing Zero Knowledge Proof (ZKP) mechanisms, protocols implementing 2-factor authentication mechanisms without password tables, etc. are all ways that this issue can be mitigated in a cloud environment. Other options include avoiding the storage of passwords altogether.

Session Hijacking: If the Session IDs that are sent to users who have successfully verified themselves are not adequately safeguarded, it is possible for those users' sessions to be taken over by an unauthorized third party, a practice known as session hijacking. Packet sniffing tools are used in session side-jacking, which allows an attacker to record a user's login sequence and, as a result, get the user's session key. The communication channel can be protected from this kind of Session hijacking attempt by using encryption. By utilizing a secure connection protocol such as HTTPS and encrypting the files that hold user or administrator login credentials, among other things, it is possible to counter these assaults that exploit gaps such as unsecured communication methods and unprotected data. A robust authentication mechanism that excludes the possibility of unauthorized authentication as well as mechanisms that protect secrets such as session keys or avoid the storage of secrets are required in a cloud environment in order to thwart attacks of this nature. Another option would be to avoid the storage of secrets altogether. Avoiding the transmission of session keys over the communication channel is one way to prevent the side-jacking attack from being successful. It is also possible to use a key exchange method, which calls for the client and the server to independently compute the session key and then compare their results to ensure that they provide the same key value.

Denial-of-Service (DOS Attacks): The primary purpose of a DOS assault is to prevent the target computer from responding to genuine service requests by overwhelming it with fraudulent service requests and thereby overloading it. Because it is unable to process all of the service requests on its own, it distributes the work load to other instances of the same type of service, which eventually results in flooding assaults. Because it allows for the pooling of resources, cloud computing is more susceptible to denial of service assaults. This assault on availability can be contained, at least to some degree, through the use of data transfer throttling, which purposefully regulates the amount of data transferred per unit time among the communicating entities, and through the restriction of the amount of network bandwidth that is made available. The overhead of the authentication process can be reduced on the server side by using an authentication protocol that performs one level of authentication at the client side.

Cloud Malware Injection Attack: The goal of the attack is to make a malicious service implementation or virtual machine instance look like a legitimate one of the cloud's running service instances so that it may be injected into the system. The attacker initiates the assault by generating their very own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and then injecting it into the cloud. If the adversary is successful in their endeavor, the cloud computing system will recognize the newly created instance as a legitimate one for the specific service that was the target of the assault. After then, the server will begin to reroute the legitimate user requests to the malicious server implementation, at which point the adversary's code will be carried out. The code is capable of doing a variety of tasks, from alterations to data that are imperceptible to the user to complete overhauls of the system's operation. To defend against this attack, one strategy involves storing a hash value on the file containing the first service instance image and comparing it to the hash values of all newly created service instance pictures. In the event that a genuine service instance is updated, the hash value will also be changed, which shows the presence of an adversary. Again, if an attacker is successful in creating a new service instance and inserting it into the cloud, then that instance ought to have a hash value that is comparable to that of an existing one. On the other hand, the likelihood of accidentally generating a service instance that has a hash value that is identical to the hash of another service instance is almost nonexistent.

Distributed Denial of Service Attacks: A distributed denial of service attack, often known as DDoS, is an advanced form of a distributed denial of service attack (DoS). It works by overwhelming the target server with such a high volume of packets that it is unable to process them, hence preventing it from providing essential services. In contrast to a DoS assault, a DDoS attack involves many dynamic networks that have already been infiltrated and is propagated from those networks.

The remaining portions of the paper are structured as follows: In the next section, we will talk about some of the research that has been done in the field of authentication and cloud security. The limitations of earlier algorithm designs are discussed in Section 3. In section 4, we talk about the issue that arises when authentication is performed. Our primary objective is to strengthen the security measures in place inside cloud computing in order to prevent unauthorized access. In Section 5, we outline the primary goal that we hope to achieve via our investigation of this field. In the next section, "Section 6," we will address the future work hypothesis. The discussion of methodology and procedures may be found in section 7. It lays forth a path for the work that will be done in the future. The findings and conclusions of this study are presented in Section 8.

II. LITERATURE REVIEW

In this paper [3] authors presented a handwriting authentication method. A mobile phone may be used in a secure manner to gain access to limited data that is stored in the cloud thanks to the method. Pre-processing, the extraction of features, the categorization process, and the authentication process are all parts of it. The process of classification makes use of three distinct classification methods: ANN, KNN, and the Euclidean Distance classifier. In order to attain a level of accuracy that is suitable in terms of both recognition and error rate, the classifier algorithm makes use of the parallel combination of classifiers.

The authors of this study [4] provide a graphical password authentication technique; it is possible to give an example of this by using the cloud as a platform. The new plan addresses a large number of the issues that are present in the previous system. From a user's point of view, it may also be helpful from a safety standpoint.

The authors of this study [5] offer a straightforward and efficient online signature verification system that is suited for user authentication on a mobile device. This method may be found in the appendix of the publication. The following are some of the advantages that the suggested algorithm has. To begin, a feature set that is based on a histogram that can be used to represent an online signature may be determined in linear time, and the system needs a space that is both small and fixed in size in order to store the signature template. Additionally, because the feature set only includes data regarding the distribution of the original online signature traits, the modification cannot be reversed. As a direct consequence of this, the confidentiality of the primary biometric data has been effectively preserved. Second, a user-specific classifier that is comprised of a user-specific quantization step size vector and its associated quantized feature vector can be trained utilizing only enrollment samples from that user, which eliminates the need for a training set that contains information from a large number of users. In comparison to other algorithms, the usefulness of the suggested technique in terms of its verification performance has been demonstrated by a number of tests that have been carried out on the MCYT and SUSIG datasets.

A security study of the online signature verification method is offered, along with a comparison to the use of a 4-digit PIN, and two usability metrics are also discussed. Further investigation will include the use of other biometric key binding approaches, such as fuzzy commitment. This will allow for the system's security to be improved, even in the event that its stored templates, helper data, or other components are breached, while also ensuring that its verification performance is maintained. In conclusion, it is possible to derive a fusion approach by combining the proposed method with other existing approaches, such as DTW, HMM-based, etc., in order to improve verification performance. This is particularly useful for applications in which maintaining the confidentiality of the signature traits is not as important. The authors of this paper [6] investigate whether or not people are able to guess the hand-drawn images that were used as the graphical password of others, if they know some cultural information about the users, such as where they came from, their religion, or even their hopes. Specifically, the authors look at whether or not people are able to guess the images if they know the user's hopes. In addition to that, the purpose of the study is to give evidence of a bias in the user choice of photos and to assess the influence that this could have on guess ability. In spite of this, the findings demonstrate that neither males nor females, nor people of diverse cultural backgrounds, are significantly different from one another in their ability to guess pictures. If a person's pass image does not contain any cultural or religious symbols, it is much more difficult to guess their pass image than if it does contain such symbols. However, one of the clear results of this work is that it appears to be highly possible to guess other people's pass images if they contain such symbols. In addition to that, the writers offer instructions on how to create a secure password. In this study [7], the authors had suggested using Images as part of an authentication technique. According to the authors, in order to access data in a safe manner, the key should be exchanged between the user and the cloud service provider (CSP). The user will only be validated by the CSP before being granted access to the cloud's data; however, the users will not share their keys with one another. According to the system that was suggested by the authors in order to obtain data from the cloud. After that key has been exchanged between the user and the cloud service provider (CSP), with the assistance of that key the CSP will provide the encrypted data to the user. In the first step, the user is authenticated by the cloud service provider using an image-based authentication mechanism. The proposed safe technique for accessing data stored in the cloud operates in three phases: the Registration phase, the Image-based Authentication phase, and the Key Exchange phase.

The authors of this work [8] give an overview of recent developments to automatic recognition of human facial activity using soft computing. The survey is presented in the context of this paper. The most exciting area of study right now is called soft computing. When applied to problems such as classification, prediction, optimization, pattern recognition, and image processing, amongst others, soft computing approaches tend to be highly successful. In most situations, the process of recognising facial behaviour occurs in three stages. The technique of recognising faces in photographs is referred to as face detection. The technique of emphasising the face portion that plays a part in identification of expression is called feature extraction, and the last step in the process is the creation of a classifier that detects the expression. There are many efficient ways available, but none of them are able to provide the best results in each and every circumstance when used to analyze facial expression. Every approach has its drawbacks that must be considered. The development of a human face behavior recognition system should eventually lead to the creation of a robust system that can operate effectively regardless of the conditions.

Application developers may be put in the position of dealing with a challenging series of circumstances, each of which requires its own identification solution in the absence of claim-based identity. Claim-based identification is helpful in giving a consistent answer across a broad variety of cloud service use cases, which is a benefit of using cloud services. It is possible to simplify the migration process by developing and deploying claim-based apps in addition to the already existing applications. Claim-based identification is

not exclusive to Microsoft suppliers; rather, it involves a large number of companies. The authors of this study [9] explain why claim-based identity solutions are necessary, as well as how cloud service providers might use them effectively in cloud applications.

The authors of this research [10] discovered a new privacy concern that arises while data accessing in cloud computing, and they proposed a solution to ensure privacy-preserving access authority sharing. The establishment of authentication helps to secure the confidentiality of data as well as the integrity of data. Since the wrapped values are traded off while the data is being sent, confidentiality of the data is maintained. The user's privacy is protected through anonymous access requests, which are used to discreetly communicate with the cloud server about the user's desired level of access. Forward security is achieved by the use of session IDs, which also serve to avoid session correlation. It demonstrates that the suggested technique has the potential to be implemented in cloud services for the purpose of protecting users' privacy. The authors of this study [11] argue that modern cryptosystems make use of authentication methods for the purpose of ensuring secure communication. Furthermore, they state that authentication procedures are necessary even in cryptosystems that are based on QKD (Quantum Key Distribution). According to the authors, there are currently no effective authentication procedures that are specifically dedicated to quantum cryptosystems. An authentication method for a cryptosystem that is based on QKD has been proposed by the authors.

The authors of this paper [12] present a trustworthy and safe three factor authentication technique that protects against a variety of security threats. A commonly implemented random oracle model is utilized to demonstrate that the suggested system possesses a level of demonstrable safety. In order to get the experimental findings, the authors put the cryptographic operations of the proposed scheme and related schemes through their paces on a desktop PC that included favorable technical requirements. In addition, the performance of the provided system is evaluated by contrasting it with other schemes already in existence. The performance study demonstrates that in comparison to analogous competing systems, our approach is not only lightweight but also efficient in terms of the expenses associated with computing and communication.

On the other hand, the authors of this study [13] contend that their approach has a number of flaws, one of which is that it is not resistant to assaults involving privileged insiders or impersonation. In addition, the purpose of this study is to demonstrate that the authentication phase of their system is flawed, and because of this flaw, the scheme proposed by Yu et al. is incapable of supporting a large number of users. After that, a better method is presented to oppose the vulnerabilities and incorrectness of the strategy that Yu et al. proposed. [Citation needed] The authors, making use of BAN logic, demonstrate that the suggested approach is secure. A textual explanation on the robustness of the suggested system is also provided by the authors with the purpose of providing a clear image of the security features. Additionally, the performance efficiency of the proposed method is comparable to that of other similar schemes since it makes use of symmetric key-based hash functions.

This research study [14] proposes a system with a basis of elliptical curve cryptography (ECC) to execute secure financial transactions over Virtual Private Networks (VPN) by establishing robust Multi-Factor Authentication (MFA) employing authentication credentials and biometric identities. The findings of the study demonstrate that the model that was provided is an excellent candidate for implementation in real time. According to the findings of the security research, the suggested model demonstrates a high degree of security while requiring a response time of no more than 12 seconds per user, on average.

A robust user authentication mechanism is the primary prerequisite for ensuring the safety of the cloud computing environment. This is because it prevents unauthorized users from gaining access to service providers. In this context, the authors make an effort to suggest potential preventative actions for the cloud environment. Therefore, the purpose of this paper [15] was to present a novel one-way hash and nonce-based two-factor secure authentication scheme with conventional user IDs, passwords, and an OTP verification procedure that is resistant to brute force attacks, session and account hijacking attacks, MITM attacks, and replay attacks.

In the table 1 we discuss the various authentication techniques and method used by those techniques. Also we discuss the advantage and disadvantage of those techniques.

Table 1: Various authentication techniques

S. No.	Schemes	Method	Ease of use	Advantages	Disadvantages
1	Image- based scheme	Single or multiple images are used	Selection of images	Easily remember the password	Very long process selection of number images.
2	Grid- based scheme	Grid platform is used to accommodate pixels	Simple take and draw scheme	No extra displays are needed grid is sufficient.	sequence can be changed or grids may be different

3	Triangle scheme	Set of images on convex surface	Complex as convex triangle	Crowded Display	convex surface assigning process takes longer time
4	Signature based scheme	User signature on grid platform	Own signature	Denied the access for mistake	Remembering the grid if not simple
5	Username and image password scheme[proposed system]	Username with selection of images as password	Username password remembrances	More strong authentication process	Access can be given if anyone knows sequence with username

III. Disadvantages of previous algorithms

1. 1. The majority of the methods offer a high level of protection, but they require extra hardware support, which is not always accessible in all locations.
2. 2. The overhead of a vast set of two-step authentication mechanisms uses up a lot of resources because of the complexity of the process.
3. 3. Because of the extensive use of resources that are required, many of the strategies outlined above are not applicable to real-world situations.

IV. PROBLEM DEFINITION

Misuse of data, inflexible access control, and insufficient monitoring are only some of the negative acts that unauthorized users have been responsible for that have posed a danger to cloud technology. The occurrence of these dangers may result in the users' sensitive and confidential data being corrupted or accessed illegally, both of which are serious problems. Although many different authentication techniques have been put into place to ensure the safety of these data, the fact remains that the majority of them are either overly complicated or demand a significant amount of network resources. Our primary objective is to strengthen the security measures in place inside cloud computing in order to prevent unauthorized access. We shall present a technique based on manual cypher authentication after doing research on the approaches described above. The approach that we have presented would provide enhanced protection against assaults, unauthorized authentication, and intrusions while preserving the concept of "ease of use."

V. OBJECTIVE

The following is a list of the primary goals:

1. Implementing a new authentication technique on the cloud or hybrid cloud that makes use of a manual cypher in order to guarantee data safety.
2. Authentication of the user from one cloud to another cloud when moving between clouds.
3. The combining of Cipher Queries in a dynamic manner.
4. A decrease in the amount of time and space required in comparison to earlier methods.
5. Keeping the Ease of Use in Mind.

VI. HYPOTHESES

In traditional methods of password authentication, the server keeps a password table or a verification table that lists the user identification (ID) and password (PW) for each of the users who have registered. It serves the purpose of verifying that the user is who they claim to be. Every user has their own unique ID and password. In order to get past the authentication step, a user must always provide their ID and password before being granted access to the resources that are stored on a server. The PW that is associated with the ID is checked against the verification table by the server. The user is considered to be authenticated by the server if the provided password is the same as the one that is saved in the verification table. However, there is a risk involved in carrying out such a procedure since an unauthorized user can be impersonated by an intruder who does this by intercepting the communications from the network and then logging in to the server using the information that was intercepted. It is still feasible to carry out an impersonation attack even if the PW is encrypted while the conversation is taking place. In addition to this, if an unauthorized user were to hack into the server, the information included in the verification table may be readily altered or taken. The most significant drawback of this strategy is that the verification table, which keeps the password in plain text form, must be protected. Encrypting the password through the use of a hash function and storing the test pattern that is generated as a consequence in a verification table is one approach that may be taken to address this issue. Another possible approach is to store the password in an encrypted form, which

makes it difficult for an attacker to deduce the password's contents even if the attacker is aware of the information included in the verification table.

VII. METHODOLOGY AND METHODS

Following an examination of the relevant published material, it has come to our attention that several strategies can be utilized in the authentication process. Although many different authentication techniques have been put into place to ensure the safety of these data, the fact remains that the majority of them are either overly complicated or demand a significant amount of network resources. Conventional password authentication systems are utilized in the majority of the published works. These schemes need the server to keep a password table or verification table, both of which contain the user identification (ID) and password (PW) for all of the registered users. It serves the purpose of verifying that the user is who they claim to be. In the part on the literature study that was just read, there was a brief overview of the many different cloud computing strategies and authentication protocols. A new strategy will be designed, and none of the techniques described in the previous paragraph will be applied directly. The strategies described in the previous paragraphs serve as a source of inspiration. Despite the fact that the UID and password method will serve as the foundation for the first stage in the authentication process.

VIII. CONCLUSION

Within the scope of this paper, we have discussed a variety of approaches that may be utilized for authentication. Even though there are a lot of different Authentication techniques that have been established for the authentication, none of them are completely safe. In addition, a significant portion of the methods need the use of supplementary hardware, which is not always accessible in all locations.

REFERENCE

[1] Peter Mell and Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, September 2011.
[2] B. Sumitra, C.R. Pethuru, M. Misbahuddin “A Survey of Cloud Authentication Attacks and Solution Approaches” http://www.ijircce.com/upload/2014/october/36_A%20Survey.pdf
[3] F. Omr, S. FoufoU, R. HamiIa & M. Jarraya presented paper entitled “Cloud-based Mobile System for Biometrics Authentication” at IEEE 2013 13th International Conference on ITS Telecommunications (ITST).
[4] Shraddha M. Gurav, Leena S. Gawade, Prathamey K. Rane & Nilesh R. Khochare presented paper entitled “Graphical Password Authentication” at IEEE 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.
[5] Napa Sae-Bae & Nasir Memon presented paper entitled “Online Signature Verification on Mobile Devices” at IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.
[6] Salem Jebriel & Dr. Ron Poet presented paper entitled “Exploring the Guessability of Hand Drawn Images Based on Cultural Characteristics” at IEEE 2014 6th International Conference on CSIT Published by the IEEE Computer Society.
[7] Anurag Singh Tomar, Gaurav Kumar Tak, Ruchi Chaudhary “Image based Authentication with Secure Key Exchange Mechanism in Cloud”, 2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom).
[8] Khyati Kantharia & Ghanshyam I Prajapati presented paper entitled “Facial Behavior Recognition using Soft Computing Techniques: A Survey” at IEEE 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
[9] Ashish Singh & Kakali Chatterjee presented paper entitled “Identity Management in Cloud computing Through Claim-Based Solution” at IEEE 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
[10] Hong Liu, Huansheng Ning, Qingxu Xiong & Laurence T. Yang presented paper entitled “Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing” at IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 1, JANUARY 2015.
[11] Minyoung Bae, Ju-Sung Kang, Yongjin Yeom, “A Study on the One-To-Many Authentication Scheme for Cryptosystem Based on Quantum Key Distribution” 978-1-5090-5140-3/17/$31.00 ©2017 IEEE.
[12] Muhammad Asad Saleem, SK Hafizul Islam, Shafiq Ahmed, Khalid Mahmood and Majid Hussain, “Provably secure biometric-based client–server secure communication over unreliable networks” Journal of Information Security and Applications 58 (2021) 102769.
[13] Sajid Hussain, Yousaf Bin Zikria, Ghulam Ali Mallah, Chien-Ming Chen, Mohammad Dahman Alshehri, Farruh Ishmanov and Shehzad Ashraf Chaudhry, “An Improved Authentication Scheme for Digital Rights Management System”, Wireless Communications and Mobile Computing, Volume 2022, Article ID 1041880.
[14] D. Prabakaran and Shyamala Ramachandran, “Multi-Factor Authentication for Secured Financial Transactions in Cloud Environment”, Computers Materials & Continua, DOI:10.32604/cmc.2022.019591.
[15] Sandeep kaur, Gaganpreet kaur and Mohammad Shabaz, “A Secure Two-Factor Authentication Framework in Cloud Computing”, Security and Communication Networks, Volume 2022, Article ID 7540891.