Asynchronous Password-Based Authentication and Service_Provider_ID Module for Secured Cloud Environment

S. Sudha and S. S. Manikandasaran

***Abstract*—Clouds are now considered as the dawn of Computing Technology. As the people of Information Technology, Business, and other Organization are living in Cloud Generation and Cloud environment offers umpteen of services over the Internet, security concepts like confidentiality and authentication mechanisms require being more robustness to foil the attempt of unauthorized persons. A very crucial security function of the cloud environment is user authentication. Previously, many authentication mechanisms such as simple username and password with OTP, Graphical password, Smart Card based mechanism, and Biometrics were devised, but those were suffered from various attacks by the hackers, computational cost, and expensive to implement. Moreover, the Cloud environment is now requiring innovative and sturdy authentication mechanismto make an authentication process more complicated; this paper proposes a multi-level - Asynchronous Password-based authentication process and Service_Provider_ID module. This mechanism provides a different and distinctive password for every session, which ensures a well-built authentication process and harmonizing of Service Provider ID and User Session ID validates the User session with the Cloud environment. This uniqueness leads to the highly secured authentication process in the Cloud environment.**

***Index Terms*—Asynchronous password, cloud computing, multi-level authentication, service provider id, user session-id.**

I. Introduction

The trend-setting cloud paradigm represents the cool conglomeration of several proven and promising web and enterprise technologies. The cloud-based concepts and their insights have gradually and perceptibly impacted the sectors like IT and business domains on various significant aspects [1]. The cloud computing environment has brought in a series of innovative and novelty-packed deployment, deliverance, utilization, and pricing models. The remarkable contribution of the much-discoursed and premeditated cloud computing is the faster apprehension and an abundance of dynamic, congregated, adaptive, on-demand and online compute infrastructures are the essential requirement for future IT [2]. The delightful distinctions here are that clouds guarantee most of the non-functional requirements such as availability, high performance, on-demand scalability/elasticity, affordability, global-scale accessibility and usability, energy efficiency, etc.

In the recent past, clouds have arrived onto the scene more powerfully and stretched the prospect and the edge of business applications, events, and data. While the cloud service contributions present a simplistic view of IT in case of Infrastructure-as-a-Service (IaaS) or a simple-minded view of programming in case of Platform-as-a-Service (PaaS) or a simplistic view of resources used in the case of Software-as-a-Service (SaaS), the underlying systems level support challenges are enormous and highly complicated [3]. These stalk from the need to offer a uniformly steady and robustly a simplistic view of computing while the underlying system is highly failure-prone, heterogeneous, resource-hogging, and exhibiting severe security shortcomings. As applications and data are diverse, distributed, and decentralized, cloud service suppliers go to great lengths to safeguard that customer data is secure within the hosted environment, and it poses new issues that need to be addressed by the integration of more than one authentication techniques [4].

Security-related issues are significant challenges that cloud service providers need to deal with in the cloud computing environment. One of the top security threats in the cloud is unauthorized access to credential information. Besides confidentiality and integrity, authentication is specific operational security to ensure that only authorized users can access the resources of the cloud. The traditional password method has been enhanced by various means such as salted password hashing, one-time-password (OTP), and Multi-factor Authentication [5]. It is vital to have a highly secure authentication system to prevent an unauthorized user from accessing the resources of the cloud. This scheme proposes the Random-Password-Based authentication system and synchronization of the User Session ID and Service Provider ID, which works as follows.

The key proposal of this system is a multi-factor authentication system and synchronization of the User Session ID and Service Provider ID. This innovative mechanism plays a significant role in the authentication process and prevents hackers from accessing sensitive information. This paper includes the following essential sections. Profound analysis and reviews of authentication mechanisms are explained in Section II, description of the proposed scheme are given in Section III, the security mechanism of the proposed scheme presented in Section IV, and the conclusion of the work is given in Section V.

Manuscript received December 13, 2019; revised March 1, 2020.

S. Sudha and S. S. Manikandasaran are with PG & Research Department of Computer Science, Adaikalamatha College, Bharathidasan University, India (e-mail: arthikumari10@ gmail.com, moni.tamil@gmail.com).

DOI: 10.7763/IJCTE.2020.V12.1269

II. Related Work

This section presents a detailed review of work related to traditional password-based authentication in the cloud computing environment.

Ibrahim A. Althamary *et al.* [6] proposed a well-known authentication scheme called "A More Secure Scheme for CAPTCHA-Based Authentication in Cloud Environment." This authentication mechanism combines the user's password with modified characters of CAPTCHA that a secret agreement between the cloud service provider and the user. In this work, during the time of the sign-in process, random characters are generated and will be displayed to the user in the form of CAPTCHA, and then it allows the user to enter some replacement characters instead of some characters in the CAPTCHA. Thus, the user can enter a new password for every session. This work also supports the concept of passwords with salted hashes. This scheme works well against the various attacks like phishing, keylogger, dictionary attack, and this scheme also resolves the password guessing. Based on this scheme, the user can experience a new password for every session.

A secure password mechanism in the cloud environment is always welcomed by the cloud user and everyone to evade the hackers to gain entry into the cloud environment and capture sensitive information. For this, M.Meena *et al.* [7] introduced a sturdy authentication mechanism called "System for 3 Level Security Verification using Image-Based Authentication and OTP". This mechanism proposes a three-level authentication. During the first level, the user has to enter the username and password, at the second level, identification of images from the 4 x 4 grid which is already set by the user during the registration phase, and in the third level, the user has to enter the OTP as received on their registered mobile. This gives the highest production against the brute-force and tempest attack. The disadvantage of this algorithm is password change option is not given and forgot password. A reset password option needs to be implemented.

A novel and strong Smart Card-based authentication were given by Candan *et al.* [8] that uses a secured protocol, which consists Elliptic curve, Symmetric Cipher, and the Hash function aims to authenticate a user to a server via smart card. During the first (Registration) phase generates a secure random number with a unique ID, Password, and Smart card. Elliptic Curve and EC Diffie-Hellman (ECDH) security algorithms have been used to give the secret value. This allows the user and server to communicate securely over the public channel. The critical two components, such as the password and the smart card, give better authentication services, and the illegitimate user cannot access the server. This concept provides better security against off-line dictionary and replays attacks.

In Ref. [9], Aldwairi *et al.* presented a Multistage Authentication System that includes three different authentication schemes. In the first stage, the user is authenticated only when present the correct username and password with the serial number of the devices. In the second stage, the user has to highlight them a right square of the given n right squares. Finally, the user has to select s images as per the specific order. This scheme is more immune and works well against the password guessing and brute-force attack.

To strengthen the authentication process in the cloud environment,Abdellaoui *et al.* [10] devised a novel scheme called "A Novel Strong Password Generator for Improving Cloud Authentication." This Password generator module consists of multi-factor authentication, a one-time password, and SHE 1. This work consists of three phases. The first phase allows the user to enter a traditional username and password. The One Time Password generated by the pixel value of the image of the user is done in the second phase. At the third level, OTP generated by the client is verified with the OTP generated by the server. If it matches, the client is authenticated; otherwise, authentication to the server will be denied. The innovative idea in this work is a password generator with the help of the pixel value of the image. Thus, the three levels of authentication work well against the guessing and shoulder-surfing attacks.

A secure authentication mechanism by using Dual Factor Authentication Protocol (DFAP) was implemented by Abdul *et al.* [11] This mechanism converts the user's authentication credentials into waveform by using the method of Scalar Vector Graphics and the same can be verified by the server with the help of user mobile token (UMT). When the user presents the valid credentials, the user can access the various resources on the cloud server. This mechanism keeps the various attackers away from accessing the server illegitimately.

To thwart the hacker's unauthorized accessing of the user's credential,Abdellaoui *et al.* [12] devised a scheme called image-based one-time password for the cloud environment (imOTPc). The security of the proposed scheme is enhanced by the one-way hash function using SHA-1, Image One-Time Password (imOTP), Secret Watermarking, and truncated part of IMEI of the registered mobile. This scheme also proposes two different types of access provision based on the authentication factor. First level authentication allows the user to access public information, and the second level allows accessing sensitive information. Thus, this robust and well-built authentication scheme keeps the various types of hackers away from gaining into the cloud server.

Hussein *et al.* [13] developed an authentication mechanism called "Design and Implementation of Multi-Factor Mechanism for Secure Authentication System." The proposed system delivers a good authentication process based on the user's login credentials such as ID Number, Mobile and its IMEI Number, and PIN. The server generates an OTP by merging the user's login information and sends it to the user in an encoded format. The server employs AES (Advanced Encryption Standard) to encode the OTP and also verifies the user mobile's IMEI number. If it matches, it forwards the OTP to the trusted user. Otherwise, it will be redirected to the first phase. Thus, the IMEI's verification based OTP prevents unauthorized access and ensures the user's certification and non-repudiation.

To reduce the threat of unauthorized authentication,Emam *et al.* [14] developed a two-factor authentication scheme called "Additional Authentication and Authorization using Registered Email-ID for Cloud Computing." In which the server sends a confidential URL link to the registered E-mail of the valid user for accessing the service of a particular session. This scheme allows an only authorized person can access the resources of the cloud using a secured link, but if a mail id is hacked by the hackers, the entire system's processes will collapse.

To have an enhanced authentication mechanism to protect sensitive information in the cloud, Nikhil Gajra *et al.* [15] developed a novel scheme called "Private Cloud Security: Secured User Authentication by using Enhanced Hybrid Algorithm." Cloud computing is very well-known for its services and storage, so it is imperative to protect the outsourced data in the cloud being administered by the cloud service provider. This paper focuses on a well-versed authentication mechanism against malicious users and also provides better security for outsourced data being administered by the cloud service provider. An authentication scheme is achieved by the Elliptic Curve Digital Signature Algorithm (ECDSA), and to safeguard the outsourced data, this paper proposes a hybrid of the AES and Blowfish algorithm. The key is generated, maintained, and exchanged by a well-defined mechanism called Elliptic Curve Diffie-Hellman (ECDH). To achieve high-level security, this research proposes MAES (Modified Advanced Encryption Standard) with 256-bit AES, which includes 14rounds, which is used for encrypting the outsourced data. This ensures high- level authentication and better encryption. This mechanism not only provides security protection for outsourced data, and also reduces the computation overhead.

ChitraRajagopal *et al.* [16] introduced a robust security algorithm called "Proposal and Implementation of Cloud Security Algorithm to Enhance the Security of the Layers." The cloud provides a massive amount of space for storing the data, which results in the unauthorized access of data and security breaches. This paper proposes a unique algorithm called Honey Encryption Algorithm combined with the DES algorithm to have an additional security layer for counteracting against the illegal access of data from the cloud server. Although this system amplifies the intensity of complexity, it works well against the illegitimate users and protects the sensitive data.

It is quite evident that the cloud environment offers enormous storage capacity for its users, but there are umpteen security issues associated with it. So it is better to have a well-equipped security and authentication mechanism. Considering this,Akanksha Bansal *et al.* [17] proposed an algorithm called "Providing Security, Integrity, and Authentication Using EYCK Algorithm in cloud storage." This paper proposed an algorithm called Electronic Curve Cryptography (EYCK) Algorithm for ensuring robust security, integrity, and authentication against the intruders. An algorithm given in this work exhibits excellent performance and takes less CPU time and reduces processing time.

Cloud computing services have seen an impressive increase in recent years. Hence, it is imperative to have a well-established authentication system and encryption mechanism to protect sensitive data from hackers. RushikeshNikam *et al.* [18] devised a scheme called "Cloud Storage Security using Multi-Factor Authentication." This work achieves confidentiality using CP-ABE (Ciphertext Policy – Attribute-Based Encryption) and Authentication with Multi-Factor Authentication. Security can be achieved at different levels, such as providing static username and password, and then QR Token Generator is used to generate a Token for issuing OTP, which provides multi-level security for the cloud environment. Multi-level security factors prove it is worthy that even if the malicious user exploits one level, the other level of security protects the cloud environment actively. Unfortunately, TOTP is prone to malware attacks.

R.Baudauria *et al.* [19] devised an authentication mechanism called "Secure Authentication of Cloud Data Mining API."This scheme proposes a One-Time Pass-Key and Domain Trust mechanism that is used to increase cloud security, but data mining is time-consuming and requires high-performance devices. Multi-factor Authentication Scheme for E-Services in Cloud Computing proposes a new model based on these E-Services that can be done with Secure Multi-factor Authentication methods, which include a three-tier architecture such as Username and Password, Mobile Token and Question Set. This makes it difficult for attackers to crack the system. During the first phase,the username and password verification and second phase verify the pattern, and the third phase verifies the e-mail security code. So this three-tier architecture provides more security to the user and protects the environment from various attacks. Data mining is used in this method, but data mining is time-consuming and needs high-performance devices.

The proliferation of the cloud computing environment paves the way for many enterprises and government agencies to get their job done with ease. However, the reliable authentication mechanism is required for accessing the data in the cloud environment. Hence, J. P. Singh *et al.* [20] introduced a new kind of mechanism called "Authentication and Encryption in Cloud Computing" This paper proposes a secure authentication mechanism based on a tree structure, which improves the user authentication process and Elliptic Curve Digital Signature Algorithm ensures the data integrity. This scheme takes less time for key generation and signature verifying process.

Yassin *et al.* [21] Use the biometric method to authenticate the client with the canny's edge detection. This work consists of the two factors; first is canny's edge detection and then symmetric encryption. It helps to authenticate, providing security performing with image encryption. Lower transmutation cost with high security makes this work more beautiful. A valid user can select a valid password.

In Ref. [22], a scheme is proposed to improve the rate of trust and reliability using two separate servers: one for authentication and the other for encryption. The use of two servers is to decline encryption procedures in the central server and the dependency of user authentication. Implementing an extension agent on the web browser for user authentication makes it possible to authenticate the user without reaching the cloud. Moreover, encryption is also performed before storing the data in the cloud.

A secure layer is designed as an extension of the browser or mobile applications for protecting against phishing and dictionary attacks. Therefore, users usually reuse their biometric or alphanumeric passwords to access different online services and split secret keys in different online social networks. A problem with this method is the possibility that online service and storage providers work together against the user [23]. Moreover, identity theft attacks users using some tools that can steal sensitive details from different social networks by making fake accounts [24].

III. Proposed Work

This proposed work ensures the multi-level authentication process at different stages. This authentication process works based on something the user has, which includes a password, OTP, User Session ID, and Service Provider ID. Besides verifying the User authentication, it also validates the user's session with the server when the User Session ID and Service Provider ID matches. Fig. 1 expounds on the workflow of this mechanism.

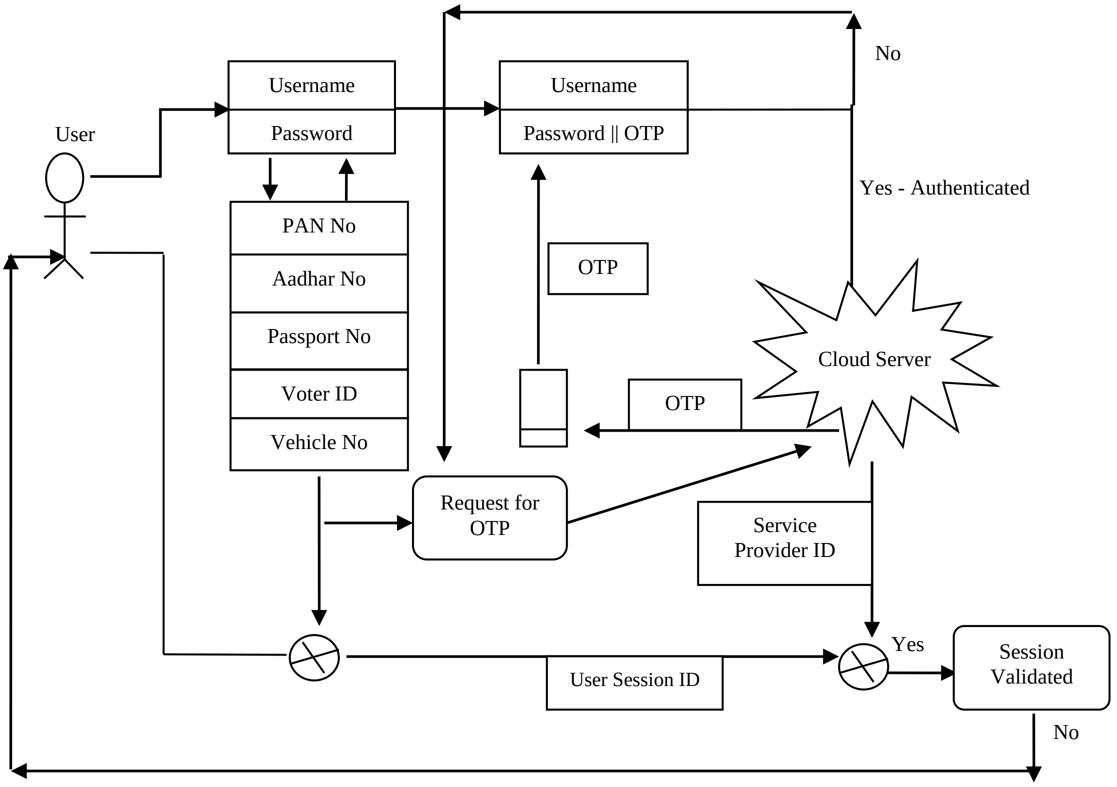

Fig. 1. Architecture of multilevel authentication system.

The proposed work elaborates on the authentication process at four levels. During the first level, traditional usernames and passwordsare used. At second level the user has to answer to the security question, and at this stage, Alphanumeric OTP will be sent to the user's email-id, and in the third level along with the same username, the user has to enter the password combined with the OTP that is the OTP will be appended with the old password. This technique facilitates the user to enjoy a new and unpredictable password for every session, and the server authenticates the user.

The uniqueness and novelty of this work is the Service_Provider_ID module, which creates the Service Provider ID. This must be synchronized with the User Session ID, if it matches, the user's session with the Cloud server will be validated in the final level. These authentication mechanisms not only provide the solution, which works well against the dictionary, shoulder-surfing, man-in-the-middle, and password guessing attacks, and also,the user cannot initiate their session with the server until the User Session ID and Service Provider ID matches.

The proposed concept is consisting of 3 different levels of the authentication process and Service_Provider_ID module, which is explained in the following sections.

A. Registration Phase

Fig. 2 explains the workflow of the registration phase clearly.In the registration phase, the following credentials of users are stored in the Cloud Server.

Step1: The user has to register the User name and password.

Step 2: In this step, the user has to record the Security questions like user's PAN Number, Aadhar Number, Voter ID, Passport Number, and Vehicle Registration Number, and its response will be stored in the Cloud server for a further authentication process. All these credentials must be stored with the three-digit index value.

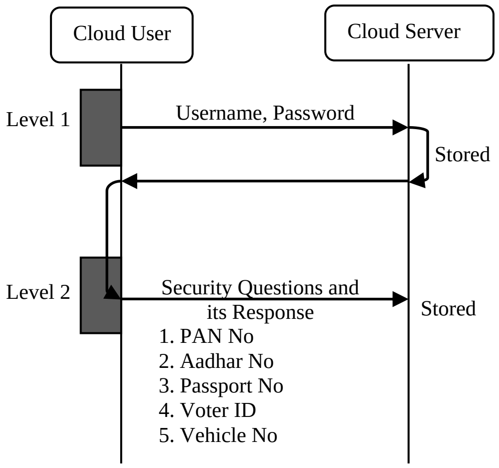

Fig. 2. Registration Phase.

B. Login Phase

During the Login Phase, the user presents the following valid credentials.

Step 1: The user presents their User name and password. If there is any discrepancy, the user has to give valid details again.

Step 2: In this step, the user has to enter the answer for anyone of the security questions. When the user enters the wrong answer, this step will redirect to Step 1.

Step 3: The user sends a request for OTP (One Time Password) to the Cloud Server. The server responds quickly, and the same will be sent to the user's Mobile Number or Email-id.

Step 4: The combination of an old password with OTP ensures a more robust authentication process here. In this step, the user enters the same User name, but for the password, the user has to follow the unique method such as instead of the old password, the user has to enter the old password along with OTP. Thus the user can enjoy a unique and different password for every session.

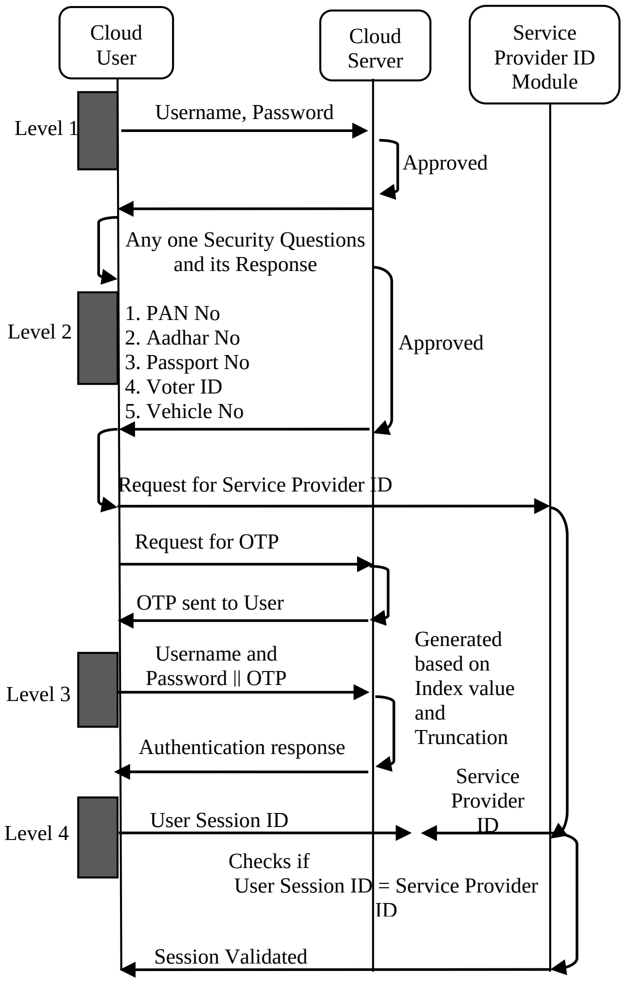

Fig. 3. The workflow of service_provider_ID module.

C. Rules for Creation of User Session ID

This module allows the user to create a User Session ID based on some constraint.

Rule 1: The user has a privilege to select a User Session ID but must follow some constraint as follows.

Rule 2: The user can create a five-digit User Session ID using any credentials which are already stored in the Cloud Server.

Rule 3: the user has to remember the index value of the credential and the truncation point, which informs from where the truncation begins in the selected credential.

Rule 4: Now, the User Session ID will be sent to the verification process.

D. Service_Provider_ID Module

Fig. 3 explains the workflow of the Service_Provider_ID module.

Step 1: This step gets the input parameter, such as index value and truncation point from the user.

Step 2: Index value determines which credential the module has to select, and the truncation point informs that from where the truncation begins to the creation of five digits Service Provider ID.

Step3: Based on the parameters, the Service_Provider_ID module creates the five digits Service Provider ID.

Step 4: Now, the Service Provider ID is sent to the verification process.

E. Session Validation Phase

In this step, the validation of User Session ID with Service Provider ID takes place. The user session can be validated with the server when User Session ID matches with Service Provider ID. Otherwise, the user's session with the server will be disconnected, and the user has to start from the first phase. Even the user authenticated with the server, the user cannot initiate a session until the User Session ID with Service Provider ID matches. Thus the Session Validation Phase plays a massive role in this work.

IV. Performance

The proposed system presents the authentication process at different levels. Everyone knows that the text-based password is elementary to remember, and the user no need to carry any extra equipment when they move from one place to another place. The main aim of this multi-level authentication is to eradicate the possessing of fingerprint devices or smart cards and other equipment. The authentication process in four stages gives different scope, and distinctive security parameters enhance the security measure. During the first stage, the user has to submit the Username and Password to move on to the second stage. The user's correct answer to the security question allows the user to move on to the third stage. At this stage, an OTP request will be given to Cloud Server, and the same will be sent to the user's registered mobile number. The distinctive approach here is that the user has to enter the new password, which can be formed by combining the Old Password and OTP. Thus the user can have a new password for every session, and the hackers cannot predict the OTP as well as the Password methodology. If the password is wrong, the user is stopped from accessing the Cloud services, and again the user has to give a request for OTP.

The unique and exclusive concept of this work is checking the User Session ID and Service Provider ID are equal. In this final stage, the user has to enter the five-digit alphanumeric code as the User Session ID. The user can use any security question to create the five-digit User Session ID. However, the user has to remember the index value of the security question and also the truncation point. While the index value determines the security question, the truncation point informs the positional value. The user can obtain five digits of User

Session ID from the positional value of the particular security question. As the user applies a recall-based approach for creating a User Session ID, the hackers cannot analyze on what basis the User Session ID is created. In this novel approach, the user neither uses any module nor any algorithm to create a User Session ID.

Service_Provider_ID module gets the input value of the index value and a truncation point from the user, and then, this module employs an algorithm to create five digits Service Provider ID. Based on the index value and truncation point, the module generates the Service Provider ID then it will be matched with the User Session ID, if the patterns do not match, the mechanism will stop the user from proceeding further, and the user's session with the server will be terminated automatically.

Thus, this mechanism not only provides the security and also has many distinctive features like a different password for every session, privacy-breaching, One Time Password, User Session ID, and Service Provider ID. These features make this work complicated and provide a superior authentication system against hackers. Apart from the authentication process, this work also performs the session validation. This mechanism also works well against the following attacks, which are as follows.

V. Results and Discussion

In recent years, the cloud environment is facing problems due to the weaknesses of inherent insecurity and compromised organizational infrastructure. With this remarkable development, a high-level authentication process has been achieved in the renowned cloud environment. Cloud environments, in general, are most vulnerable to security attacks, and special care must be taken explicitly to ensure that the valuable data do not get into the wrong hands. Hence this environment requires a high-level of authentication process so that unauthorized persons cannot penetrate this valuable environment. Almost all authentication mechanisms are suffering from different types of attacks. This work prevents any security-related issues that exist in other methods of authentication. The following section explains the different types of attacks and how this work mitigates these issues.

A. Man in the Middle Attack (MITM)

In this type, the attacker modifies the sensitive information between two parties who believe they are directly communicating with each other secretly. However, the proposed work is developed to prevent this attack by using a different password for every session. The attacker cannot get the user's valuable credentials as they are getting distinct the different passwords for every new session. Thus, it works well against the attack.

B. Guessing Password

The guessing of a password is not quite easy for them as this proposed work gives a random number for every session, and this can be appended to the existing password. Perhaps, if the hackers guessed the password in this stage, the hackers not aware of the working process of User Session ID and Service Provider ID. Thus, guessing of password attempt will be turned away successfully.

C. Short Password

The use of short passwords makes it very easy to crack an encrypted password. In this proposed work, the password length is remarkably long due to adding the length of Random numbers.

D. Denial of Service Attack

It is a kind of cyber-attack in which the hacker makes a system or network resource unavailable to its intended use by temporarily or indefinitely disrupting the services of a host connected to the environment. As the proposed work is enriched with three levels of authentication, the hacker cannot exploit any of the system resources easily.

E. Keylogger Attack

With the help of a random number, this type of attack can be prevented even if they exploited the password. It the attacker registers every character inserted from the keyboard using a keylogger attack service, these characters will be useless because every time a different password is used for signing in process. Apart from these, the hackers never know about the background process of Session Validation.

F. Dictionary Attack

In this type of attack, the hacker can apply the off-line dictionary attack. However, in the proposed scheme, even if attackers get the password from the hash, it will be useless because they need to know the random numbers not only that they need to learn more about the User Session ID and Service Provider ID.

VI. Conclusion

Cloud computing provides a plethora of benefits to its users. However, security is among the most critical issues that need special attention in cloud environments. The most important aspect of the cloud is to allow only authenticated users to access data and applications. In this paper, we reviewed several related authentication approaches in the cloud computing environment, which are developed previously to address the problem of the weak authentication process in the cloud environment. To augment the quality of the authentication process, this paper proposed an innovative multi-level authentication scheme. This paper not only highlights the importance of the authentication process and also validates the user's session with the server based on a constraint. According to this novelty scheme, the traditional username, and password method, answering the security question, and combining the OTP with an old password improves the authentication standard. Apart from these, an innovative methodology of Session validation based on the User Session ID and Service Provider ID gives a new scope of this work and proves its worth. Moreover, this scheme grants the user the power to use a new password for every session. Further, this scheme mitigates several threats as discussed earlier and also helps to prevent unauthorized access to cloud data as well as cloud processes. This model will increase the reliability and rate of trust in the cloud computing environment. Despite this, there are still many unsolved problems that exist in the cloud security concepts, particularly, data access and encrypting the data. It is paramount to safeguard the user's data; hence it is very needed to enhance the technical competency of the service provider to regulate the data access. In this place, encryption plays a vital role, and the same will be an attention-grabbing and abundant area for future works in the cloud environment.

Conflict of Interest

The authers declare no conflict of interest.

Author Contributions

Dr. S. S.Manikandasaran gave the importance and direction of research and also insisted to refer the related papers. S. Sudha analysed the requirement, developed, conducted the research and wrote documentation. Dr. S. S. Manikandasaran critically reviewed and guided the content of the article; all authors had approved the final version.

References

[1] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing: Implementation, Management, and Security*, CRC Press, 2016.

[2] R. K. Banyal, P. Jain, and V. K. Jain, "Multi-factor authentication framework for cloud computing," in *Proc. the 5th International Conference on Computational Intelligence, Modelling and Simulation (CIMSim)*, 2013.

[3] L. Arockiam and S. Monikandan. "Data security and privacy in cloud storage using hybrid symmetric encryption algorithm," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 8, pp. 3064-3070, 2013.

[4] S. Sudha and S. S. Manikandasaran, "A survey on different authentication schemes in cloud computing environment," *International Journal of Management, IT and Engineering (IJMIE)*, vol 9, issue 1, pp. 359-375, Jan 2019.

[5] S. S. Manikandasaran and S. Sudha, "Data access control techniques and security challenges in cloud computing: A survey," *International Journal of Computer Sciences and Engineering*, vol.06, issue 2, pp. 87-95, 2018.

[6] A. Althamary and E. M. El-Alfy, "A more secure scheme for CAPTCHA-based authentication in cloud environment," in *Proc. the 2017 8th International Conference on Information Technology (ICIT)*, Amman, 2017, pp. 405-411.

[7] M. Meena, H. S. Lamba, D. Taterwal, and M. Shaikh, "System for 3 level security verification using image-based authentication & OTP," *IOSR Journal of Engineering (IOSRJEN)*, vol. 13, pp. 46-52, 2018.

[8] O. M. Candan and A. Levi, "Robust two-factor smart card authentication," in *Proc. the IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, 2017.

[9] M. Aldwairi, R. Masri, H. Hassan, and M. E. Barachi, "A novel multi-stage authentication system for mobile applications," *International Journal of Computer Science and Information Security*, vol 14, issue 7, 2016.

[10] A. Abdellaoui, Y. I. Khamlichi, and H. Chaoui, "A novel strong password generator for improving cloud authentication," in *Proc. the International Conference on Computational Modeling and Security (CMS 2016)*, pp. 293–300, 2016.

[11] A. M. Abdul, S. Jena, and M. Balraju, "Dual factor authentication to procure cloud services," in *Proce. the 2016 Fourth International Conference on Parallel, Distributed and Grid Computing(PDGC)*, 2016.

[12] A. Abdellaoui, Y. I. Khamlichi, and H. Chaoui, "Out-of-band authentication using image-based one time password in the cloud environment," *International Journal of Security and Its Applications* vol. 9, no. 12, pp. 35-46, 2015.

[13] M. Singh and S. Singh, "Design and implementation of multi-tier authentication scheme in cloud," *International Journal of Computer Science Issues(IJCSI)*, vol. 9, issue 5, no 2, pp. 181-187, September 2012.

[14] A. H. M. Emam, "Additional authentication and authorization using registered email-ID for cloud computing," *International Journal of Soft Computing and Engineering (IJSCE)*, vol 3, issue 2, May 2013.

[15] G. Nikhil, S. K. Shamsuddin, and R. Pradnya, "Private cloud security: Secured user authentication by using enhanced hybrid algorithm," in *Proc. the International Conference on Advance in Communication and Computing Technologies*, 2014.

[16] P. Chitra-Rajagopal, C. Tanupriya, and K. Praveen, "Proposal and implementation of cloud security algorithm to enhance the security of the layers," in *Proc. the 5th International Conference on System Modeling and Advancement in Research Trends*, pp. 316-321, 2016.

[17] A. Bansal and A. Agrawal, "Providing security, integrity and authentication using ECC algorithm in cloud storage," in *Proc. the International Conference on Computer Communication and Informatics (ICCCI)*, 2017.

[18] R. Nikam and M. Potey, "Cloud storage security using multi-factor authentication," in *Proc. the 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, 2016, pp. 1-7.

[19] R. Bhadauria, R. Borgohain, A. Biswas, and S. Sanyal, "A survey on secure authentication of cloud data mining API," *ActaTechnicaCorviniensis – Bulletin of Engineering*, 2014.

[20] J. P. S. Mamta and S. Kumar, "Authentication and encryption in cloud computing," in *Proc. the 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, 2015, pp. 216-219.

[21] A. A.Yassin, A. A.Hussain, and M. K. Abdul-Aziz, "Cloud authentication based on encryption of digital image using edge detection," in *Proc. the International Symposium on Artificial Intelligence and signal Processing (AISP)*, 2015.

[22] F. F. Moghaddam, S. G. Moghaddam, S. Rouzbeh, S. K. Araghi, N. M. Alibeigi, and S. D. Varnosfaderani, "A scalable and efficient user authentication scheme for cloud computing environments," *in Proc. IEEE Region 10 Symposium*, 2014, pp. 508-513.

[23] T. Acar, M. Belenkiy, and A. Kupcu, "Single password authentication," *Computer Networks*, vol. 57, pp. 2597-2614, 2013.

[24] G. P. Malar and C. E. Shyni, "Facebook's trustee based social authentication," *International Journal of Emerging Technology in Computer Science &Elecronics*, vol. 12, 2015.

S. Sudha is a research scholar of PG & Research Department of Computer Science, Christhu Raj College, Trichy, Tamil Nadu, India-620012 (affiliated to Bharathidasan University, Trichy – 620024). She completed the M.Sc. in computer science at Bharathidasan University, Trichy in 2008, and completed the M.Phil. in computer science at Prist University, Tanjore. She has attended many international, national conferences, seminars, and workshopsand also published papers in leading journals. Her research interest includes soft computing, cloud computing, network security, cloud security, IoT, and image processing.

S. S. Manikandasaran is working as the associate director in PG and Research Department of Computer Science, Adaikalamatha College, Vallam, Thanjavur-613403, Tamil Nadu, India (affiliated to Bharathidasan University, Trichy-620024). He has 12 years of experience in teaching and 11 years of experience in research. He has completed his MCA and M.Tech in Bharathidasan University, Trichy in 2007, and 2009 respectively, and also completed his Ph.D. degree in ManonmaniamSundaranar University, Tirunelveli in 2015. He has attended many international and national conferences, seminars, and workshops. He has published 56 research articles in the International / national conferences and journals. He has delivered more than 40 lecturers in various national and international level seminars, workshops, and conferences. His research interest is cloud computing, network security, cloud security, IoT, and web technology.