An Analytical Survey for Improving Authentication Level in Cloud Computing

[1]Prof. Dr. Shital Agrawal, [2]Mr. Sahil Avinash Wagh, [3]Mr. Shreyas Kiran Badgujar, [4]Mr. Tanay Subhash Chhabhaiya.

[1]Asst.Professor,[2,3,4]UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharashtra, India.

[1] shital.s.agrawal@gmail.com , [2]sahil.wagh75@gmail.com, [3]badgujarshreyas7@gmail.com, [4]tanaychhabhaiya2001@gmail.com

Abstract - Cloud computing is a on-demand network. Cloud computing is very affordable and rapidly developing technology. In this type of network, you can approach your data anytime, anywhere as long you are a true cloud computing user. Data storage in a cloud computing environment is secure. In the cloud computing environment, there are no time and location restrictions on data usage so long as you have the right internet connection. Authentication is a very important concept in terms of security in cloud computing. Cloud computing is distributed computing and is helpful for storing and analyzing huge amounts of data in one place. You can use any cloud computing according to your needs. This paper focuses on the different verification stages used in cloud services and the user perspective on those authentication levels [1].

Keywords - Cloud Computing, Authentication, Security, Network, Data Multi Level Authentication.

I. INTRODUCTION

Cloud computing is online computing that offers terminals and mobile devices to share information, software and resources according to the user's wishes. This distributed network is an arrangement of grid and parallel computing. Cloud computing aims to create and evaluate a high-quality service environment with authoritative functions by organizing low-cost computing units using advanced deployment models such as SaaS (Software-as-a-Service), PaaS (Platform as a Service), IaaS. (Infrastructure as a Service) provides efficient computing power to end users. According to your requirements, you can use any cloud computing [3].

According, the end user uses the SaaS model of cloud service. It is the final application software utilized by the end user, supported by PaaS and IaaS respectively. Developers can code software on a PaaS platform to create software and applications. User access a virtual server in seconds and pay only for the resources used with the IaaS model. Infrastructure components are directly accessible to users in the IaaS model. In the (IaaS) model, users directly access infrastructure components. Authentication is very important for the secure use of these cloud services.

Cloud-computing is a term referring to using of managed third-party services to make hardware & system capabilities available over the internet.[9]

II. AIMS AND OBJECTIVE

a) Aim

The goal of the research paper "Analytical study to improve the authentication level of cloud services" is to comprehensively evaluate existing authentication mechanisms and practices in cloud service environments, identify weaknesses and areas for development and propose strategies and recommendations to improve the whole. authentication protection in the cloud.

b) Objective

- Assess Current Authentication Methods: Evaluate the existing authentication methods and mechanisms used in cloud computing environments, including password-based, multi-factor, biometric, and single sign-on solutions.
- Identify Vulnerabilities and Weaknesses: Identify and document vulnerabilities, Defenselessness, and major security risks in the current authentication systems and practices within cloud computing.
- Evaluate Authentication Protocols: Analyze the effectiveness and suitability of authentication protocols and standards, such as OAuth, SAML, and OpenID Connect, in cloud environments.

 DOI : 10.35291/2454-9150.2024.0257

III. LITERATURE SURVEY

Paper 1: Data Security in Cloud Computing

All types of organizations are aware of the advantages of cloud computing. some are just starting their migration journey, while others are implementing cutting-edge multi-cloud, hybrid methods. Due to the particular threats that cloud computing presents, data security is one of the largest implementation hurdles at any level. The traditional network perimeter that guided cybersecurity efforts in the past is undermined by the cloud. A distinct strategy is needed for data security in cloud computing, one that takes into account the intricacy of cloud security models and data governance in addition to potential attacks.[4]

Paper 2: Paas : The Next Hype of Cloud Computing

Cloud Computing is anticipated to gotten to be the driving constrain of data innovation to revolutionize the long run. Directly number of companies is attempting to receive this unused innovation either as benefit suppliers, enablers or vendors. Beneath the complete cloud umbrella, PaaS appears to have a moderately little showcase share. Be that as it may, it is anticipated to offer much more because it is compared with its partners SaaS and IaaS. This paper is pointed to survey and analyze long-standing time of PaaS innovation. It implies that PaaS innovation has built up solid roots and prepared to hit the advertise with superior innovation administrations. This investigate will talk about future PaaS advertise patterns, development and commerce competitors. Within the current energetic period, a few companies within the advertise are advertising PaaS administrations. [2]

Paper 3: A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

The utilization of computer power (hardware and software) offered as a service through a network is known as cloud computing (typically the internet). The name stems from the widespread use of an internet symbol in system diagrams as an abstract for the complicated architecture it encompasses. all data, software, and processing of a user are trusted to remote services in cloud computing. The widespread cloud computing technology, smart phones may now store and access personal information from any location at any time. Consequently, the database security issue in mobile cloud is becoming increasingly serious, impeding the mobile phone usage is increasing cloud. There have been numerous studies undertaken to increase cloud security. However, because mobile devices have very limited processing abilities and power, the majority of them are not appropriate for mobile cloud. For mobile cloud apps, applications with low computing overhead are in high demand. [9]

IV. EXISTING SYSTEM

Different methods of using cloud computing and authentication services are: i) Simple password ii) Third party verification iii) Graphical password iv) Biometric and v) 3D password object. Text passwords are susceptible to brute force or dictionary attacks and are therefore easily cracked. Smaller cloud deployments do not favor third-party authentication. Based on the notion that people can remember and recognize visuals more easily than words, graphic passwords require less memory than text passwords. The primary drawback of biometrics is its disregard for the individual features of the user. A special scanning device is used to verify users, that will not allow remote and online users. 3D Password does not support multiple authentication levels. By using one or together of them in multi-level authentication, the possibility of password cracking is reduced. Strict authentication is achieved by implementing multi-level authentication technology in secure cloud transmission.[8]

The decrypt key form is changed so it can be securely supplied to proxy servers. To the measures of the file, introduce sluggish re-encryption and a description field in the attributes.[9]

V. COMPARATIVE STUDY

Sr. No.	Author	Paper Title	Publication	Technology	Purpose
1.	D. Patil, N. Mahajan	An Analytical survey for improving Authentication levels in Cloud Computing	IEEE, 2021	SaaS, PaaS, IaaS Technology	Focusing and survey of users view on different authentication levels used in cloud computing.
2.	Ahmed Albugmi, Madini O.Alassafi, Robert Walters and Gray Wills	Data Security in Cloud Computing	IEEE,2019	Hybrid strategies	Organizations in all sectors recognize the benefits of cloud computing.
3.	Robail Yasrab	(PaaS): The Next Hype of Cloud Computing	IEEE,2019	PaaS technology	The PaaS technology has established strong roots and ready to hit the market with better technology services.
4.	Prof. Kanchan Umavane, Nidhi Sharma, Vrushali Gadhari, Vedangi Pawar, S Mohd Huzafia	A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing	IJREAM,2022	Cloud Computing	Simple, Secure data-sharing mechanism for mobile using cloud computing.

Table 1: Comparative Study

 DOI : 10.35291/2454-9150.2024.0257

VI. PROBLEM STATEMENT

Current authentication mechanisms for cloud service systems often do not provide the necessary level of protection to protect against new threats and vulnerabilities. The problem is to conduct a comprehensive analytical study aimed at improving the authentication level of cloud services.

VII. PROPOSED SYSTEM

The proposed level is a mixture of the authentication levels mentioned above. This new level of authentication uses a number of encryption techniques, such as creating a color code at each login to hide information. This new technology is completely seamless, which does not bother the user when moving to the cloud computing environment.

So this article is about the research of different authentication levels and the user's opinion about these authentication levels. The future work after this study is to suggest a new level of authentication that reduces user frustration.

VIII. ALGORITHM

Step 1: Key Generation: Generates a new encryption key using Fernet.generate_key().

Step 2: Storing the Key in a File: Writes the generated key to a file named 'filekey.key' in binary mode ('wb').

Step 3: Reading the Key from the File: Reads the encryption key from the file 'filekey.key' in binary mode ('rb').

Step 4: Encrypting a File: Encrypts the content of the file 'nba.csv' using the Fernet encryption key and writes the encrypted data back to the same file, effectively overwriting its contents with the encrypted data.

Step 5: Decrypting a File: Reads the encrypted data from the file 'nba.csv', decrypts it using the same Fernet key, and then overwrites 'nba.csv' with the decrypted content.

Algorithm for Encryption and Decryption

```
# Key Generation
key ← Fernet.generate_key()
# Storing the Key in a File
with open('filekey.key', 'wb') as filekey:    filekey.write(key)
# Reading the Key from the File
with open('filekey.key', 'rb') as filekey:
key ← filekey.read()
# Encrypting a File
fernet ← Fernet(key)
with open('nba.csv', 'rb') as file:
original ← file.read()
encrypted ← fernet.encrypt(original)
with open('nba.csv', 'wb') as encrypted_file:
encrypted_file.write(encrypted)
# Decrypting a File
fernet ← Fernet(key)
with open('nba.csv', 'rb') as enc_file:
encrypted ← enc_file.read()
decrypted ← fernet.decrypt(encrypted)
with open('nba.csv', 'wb') as dec_file:
dec_file.write(decrypted)
```

IX. MATHEMATICAL MODEL

Security Authentication

The encryption contains three stages of algorithm.

1.Key formation process

A. Select the two quality arrangements, for illustration, ATGC and TCGA..
B. change over the key era to parallel
C. The key is isolated into four break even with parts (K1, K2, K3, and K4).
D. Used coherent operations (XOR, XNOR) as shown in conditions (1), (2), and (3). XOR was used between each pair of keys to generate a subkey (Sk1, Sk2), and XNOR was used between two subkeys to make the most key (KK).

$$SK1 \leftarrow K1 + K2 + K2 \quad (1)$$

$$SK2 \leftarrow K3 + K4 + K3 \quad (2)$$

$$KK1 \leftarrow SK1 \ (\text{xnor}) \ SK2 + SK2 \quad (3)$$

2. Encryption process

The scrambled message is isolated into pieces within the encryption prepare steps (each alluded to as M … N) of break even with length. The proposed calculation will scramble the piece estimate 256-bit with 256-bit key for encryption. The another subsections will give a depiction of the encryption handle steps.

3. Decryption process

The decoding prepare is turned around of the encryption handle. It takes put after the client demands information from the cloud and affirms the user's login through the verification prepare. It comprises of two stages. The primary one, decode the moment layer utilized the hereditary qualities procedure based on the CDMB and the primary layer unscrambles the logical-mathematical function such as (XOR, XNOR, moving) with part the first plaintext and key into rise to parts.

X. SYSTEM ARCHITECTURE

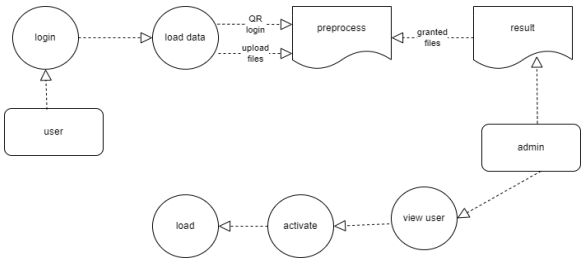

Fig.1: System Architecture

A user must first signing in to the system before they can perform other tasks. For which user must register itself to interact and authenticate with the system in user section. There is also a special section for administrator to manage the system with special features which will help admin to

 DOI : 10.35291/2454-9150.2024.0257

work efficiently. A unique way of authorization as security for cloud computing is QR code allowed Load Data in which user use to scan QR Code from registered device to confirm identity. As soon as the QR Code Scan is confirmed data files will be available to retrieve as well as for uploading purpose also. Preprocessing is a section where the upload data is processed which involves cleaning, formatting or transforming the data in which system can understand for better retrieval of data. Granted or Access section represents the component of the system that determines whether a user is authorized to perform an action. For example, a user may not be enable to view certain data unless they have been granted permission to do so by the system administrator. As all the authentication is successful the user can see the files that user can download

XI. ADVANTAGES

- Enhanced Security: Advanced authentication methods help reduce the possibility of unauthorized entry and data breaches. By identifying weaknesses and vulnerabilities in existing authentication systems, research can lead to more effective security measures.
- Mitigating security threats: thorough research can reveal potential security risks and exposures, allowing organizations to address them before malicious actors can take advantage of them. This proactive approach reduces the likelihood of security breaches.
- Cost savings: Identifying inefficient or expensive authentication methods and replacing them with more efficient alternatives can lead to cost savings. In addition, improved data security can reduce the financial impact of data breaches.
- Data Protection: A stronger authentication system helps protect sensitive data stored in the cloud. This is particularly important for the organizations that handle confidential information or personal data.

XII. DESIGN DETAILS

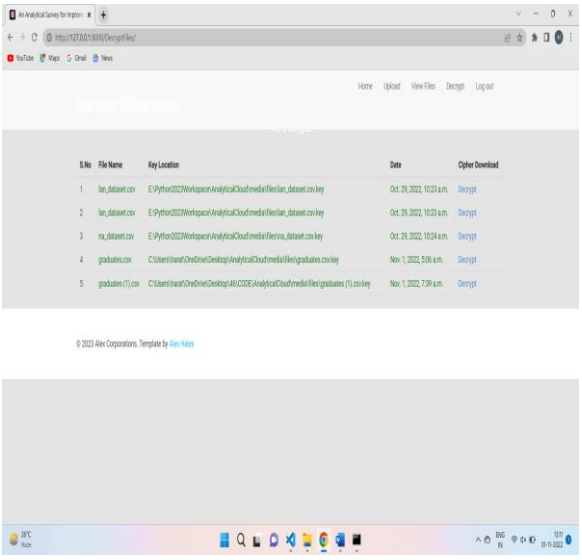

Fig 2: Decrypt file Dashboard

XIII. CONCLUSION

Thus we have tried to implement the paper D. Patil, N. Mahajan, "An analytical survey for improving authentication level in cloud computing", IEEE 2021, and the conclusion as follow: The proposed level is a mixture of the authentication levels mentioned above. This new level of authentication uses a number of encryption techniques, such as creating a color code at each login to hide information. This new technology is completely seamless, which does not bother the user when moving to the cloud computing environment. So this article is about research on different verification levels and the user's opinion about these authentication levels. The future work after this study is to suggest a new level of authentication that reduces user frustration.

REFERENCE

[1] D. Patil, N. Mahajan "An Analytical survey for improving Authentication levels in Cloud Computing" IEEE (2021)

[2] Robail Yasrab "(Paas): The Next Hype of Cloud Computing"(2019).

[3] Richa Pandey, Sanjeev Bisht, Lalit Mohan "A Comparative Study on SaaS, PaaS and IaaS Cloud Delivery Models in Cloud Computing", International Journal on Emerging Technologies (2017)

[4] Madini O.Alassafi, Ahmed Albugmi, Robert Walters and Gray Wills, "Data Security in Cloud Computing"Conference Paper ·Fifth International Conference on Future Generation Communication Technologies (FGCT), IEEE,At: Luton, UKVolume: (2016)

[5] Sara Alfatih Adam, Adil Yousif and Mohammed Bakri Bashir "Multilevel Authentication Scheme for Cloud Computing" International Journal of Grid and Distributed (2016)

[6] J. W. Ritting house and J. F. Ransome, "Cloud computing: implementation, management, and security" CRC press, 2016.

[7] Vaishnavi Deokar, Sayali Deshpande, Radhika Devkar "Password Generation Techniques For Accessing Cloud Services" International Journal of Inventive Engineering and Sciences (IJIES) (2013)

[8] Dinesha H.A, V.K. Agarwal "Multi-level Authentication Technique for Accessing Cloud Services" Conference: ICCCA- publisher: IEEE (2012)

[9] Prof. Kanchan Umavane, Nidhi Sharma, Vrushali Gadhari, Vedangi Pawar, S Mohd Huzafia "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing" International Journal for Research in Engineering Application & Management (IJREAM) ISSN : 2454-9150 Vol-08, Issue-01, APR 2022.

 DOI : 10.35291/2454-9150.2024.0257