International Journal of Management, IT & Engineering
Vol. 9 Issue 1, January 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A SURVEY ON DIFFERENT AUTHENTICATION SCHEMES IN CLOUD COMPUTING ENVIRONMENT

S.Sudha[1], Dr.S.S.Manikandasaran[2]

[1]Research Scholar of Bharathidasan University,
Assistant Professor of Computer Science,
Srinivasan College of Arts & Science, Perambalur, Tamil Nadu, India.

[2] Research Supervisor, Director,
Departmentof Computer Applications,
Christhu Raj College, Tiruchirappalli, Tamil Nadu, India.
{arthikumari10, moni.tamil}@gmail.com

Abstract: Cloud computing technology has been a new buzzword in the IT industry and expecting a new horizon for the coming world and it is also considered as a pinnacle of computing technology. Business and IT professional is progressively marching towards cloud generations as it consists of an internet-based ubiquitous computing technology and on-demand network model, which consists of software and provides the services like computation, data access, and storage service that don't have need of user's facts of the physical locality and configuration of the system that delivers the services. The paradigm of cloud computing is new, keeps everyone connected on-the-go and offers a plethora of services over the internet, hence, data security is paramount in cloud computing environment to have an access to these resources securely. Purloining an individual's legitimacy is the most insidious way of invading user's privacy; hence, authentication technique is need of the hour. Authentication technique is an unparalleled key technology for information security, which is a mechanism to ascertain proof of identities of the user to get access to information safely and mitigate the security risks in the cloud environment. In this paper, we focus on authentication techniques, which is the most challenging and promising component and there are three main approaches to user authentication are knowledge-based, possession-based, and biometric-based. In this paper, a comprehensive review and assessment of the various authentication approaches, strategies, and mechanisms has been done for a deep understanding of a secure and sturdy authentication process prevailing in a cloud environment.
Keywords: Cloud computing, Authentication, Encryption algorithm, security.

1. Introduction

Technology in its broadest sense is now more significant than ever in the field of computing. The pinnacle of technological advances in the computing field is that of Cloud Computing. Cloud offers a myriad of services and benefits to the people of the computer industry and business world. A potential application of Cloud computing ranges from Business applications, Data Storage & Backup, Management applications, Social applications and Entertainment and Art applications. The following companies are providing numerous services from the cloud. Some notable examples are *Google:* delivers various services to users, including document applications, text translation, email access, maps and much more. *www.salesforce.com. Microsoft*: Microsoft office online service-this provides platforms to build customized cloud services.

Cloud computing has a variety of characteristics such as Shared infrastructure, dynamic provisioning, Network access and managed metering. Cloud offers different kinds of services and models which make the cloud computing feasible and accessible to end users. Deployment model includes public, private, community and hybrid model and service model includes Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), and Software-as-a-Service (SaaS). Cloud computing is a newly sprouting and prominent model for the deliverance of platforms, software, and infrastructure to the outer world. The cloud computing-based services and applications offer the following benefits to its users, including Cost savings, scalability/flexibility, reliability, maintenance and mobile access. Cloud computing is playing a significant role in changing the computer industry.

The impact of cloud computing is immeasurable but, as with any new technology, there are potential downsides, such as: *Making the correct choice:* Cloud offers various services like PaaS, SaaS, IaaS. So, it is very imperative to select the best one based on our business needs. *Lack of Standards:* Cloud does not have a single platform for standardization. Clouds are fully documented interface but no standard has been defined so far. *Continuously Evolving:* Clouds are dynamic in nature and so user requirements, interfaces, networking, and storage. *Vendor Lock-in:* Data portability is very essential. Moving from one service provider to another is a daunting task on the cloud. *Service Provider availability:* The availability of a service provider is paramount and also his/her sustainability and reputation. *Security and Privacy:* These two are the main factors in cloud computing as huge data is located in different places. The user can access the shared resources which reside on cloud and nowadays, terabytes of data are stored in the cloud for an easy way of access and providing 24 hours availability at anywhere, any place and any time. It is a tedious task to maintain the security of the data on the cloud; hence, it is the responsibility of CSP (Cloud Service Provider) to ensure adequate authentication mechanism to access the data in cloud environment securely.

A well-established authentication is need of the hour as it enables cloud service provider to keep all their resources secure by allowing only authorized user to access or process the protected resources.As Cloud server and services are travel in open network, which causes the breach in the authentication process. Hence cloud service provider uses authentication to control which users have access to which resources and also this mechanism enables a remote user to securely access their applications and data's. User authentication is one of the approaches to achieve foolproof security. But still, there is a need of strong authentication mechanism through which users of cloud can be validated.

2. Authentication in Cloud Environment

Cloud computing environment has a rich set of distributed resources and enriched with good characteristics as we delineated above. Cloud permits the user to Store and to access the data available on cloud environment requires well-versed authentication mechanism which performs the following tasks such as, it is a process of proving or showing something to be true, genuine, or valid and it verifies the identity of a user or process. Before providing access to shared resources, user's identity must be verified by an authentication process. The security concerns mentioned above happens in the absence of a proper authentication mechanism and it can be avoided by adopting various authentication mechanisms. Cloud allows its customer to store their data but they are unaware of the location of data, where is it stored? So it requires transparency and every cloud service accessed by the customer, requires exchanging the authentication information. Hence, to prevent false accessing of cloud resources, a well-established authentication mechanism is paramount. After a successful authentication, a user's process is usually subjected to an authorization process as well, to verify whether the authenticated entity should be permitted access to a protected resource or system. Though user validity is authenticated, they could not access a resource if that user was not granted a permission to access it.

In a cloud computing environment three different types of authentication factors are used. The authentication factor consists of some portion of facts or trait that can be used to authenticate a user to access a system and its resources. Three important

factors to be considered to authenticate users are knowledge factor, the possession factor and the inherence factor. **Knowledge factor:** defines "Something you know", means the credentials such as personal identification number (PIN), a username, a password or the respond to a secret question. **Possession factor:** which consists "Something you have" that is the credential that the user's hardware device like a cellular (smart) phone are capable to receive a authentication message or one-time password or PIN which are generated by authentication app. **Inherence factor:** means "Something you are" is typically based on some form of biometric identification, including finger or thumbprints, facial recognition, retina scan or any other form of biometric data. Apart from these factors, the following authentication protocols are used to ensure and support authentication process in a cloud environment such as Extensible Authentication Protocol (EAP), Challenge-Handshake Authentication Protocol (CHAP), Lightweight Directory Access Protocol (LDAP) and Single Sign-on Protocol (SSO). These protocols consist of various strategies to verify user's identity and ensure the secure access to resources in a cloud environment.

2.1 Authentication Issues

The cloud computing environment offers the massive range of services and it is helpful for users who in search of a precise cloud computing resource, Despite the numerous advantages of this technology, there are a few issues such as security and privacy that inadvertently affect the reliability of this technology, hence user authentication is the most important security issues in cloud computing environment. Here is some security issues are listed out in the cloud computing environment such as:

Cloud service providers may request customers to use and store their account credentials in the cloud; this information can be accessed by cloud service providers. This presents a privacy issue to the customer's private information.The privacy of the sensitive information is specified by Cloud service providers, so it is difficult for customers to make sure the proper rules are enforced. There is a lack of transparency in the cloud environment that allows the customers to supervise their own private information.Multiple cloud service allows the customer to store his/her password in multiple clouds, the more cloud service the customer is subscript to, the more replica of the user's credentials will be. This is definitely a security issue for the customers and the cloud service providers.The multiple replicas of account credentials will cause different authentication processes. Exchanging of authentication information for every cloud service may lead to an exploit of the authentication mechanism.Cloud service providers may use diverse authentication technologies for authenticating users; this may have a lesser amount of impact on SaaS than PaaS and IaaS.

2.2 Security Breaches in the Cloud Environment

A security breach is an act that contravenes security policies, practices, or procedures by unauthorized persons in a cloud environment and also security breaches are garnering more attention recently in the field of cloud environment causes heavy losses to the organization. This section presents various infamous security breaches happened global level. They are as follows:

- **WannaCry Ransomware**: happened in May 2017, was a type of malevolent software from cryptvirology that intimidates to reveal the user's data or perpetually obstruct access to it unless a requested ransom is made. This attack is carried out by Trojan that is disguised as a legitimate file that forces the user to download or open to hacking the system. This attack was targeted Microsoft Windows operating system and affected more than 2,00,000 systems across 150 countries with total damages ranging from hundreds of millions to billions of dollars. This attack was stopped within a few days of its discovery due to the immediate release of patches by Microsoft.
- **Yahoo!:** Two major data breaches shattered the services of the Internet Service providing company Yahoo. Both breaches registered a huge impact on the history of the Internet. Breaches that happened in 2014 and 2016 where hackers developed

web cookies to falsely access the credentials of users and hacked their account without a password. Later, Yahoo confirmed that over 3 million users account were hacked.

- **LinkedIn:** Profession networking site faced worst data breaches in the year of 2012. LinkedIn lost over 167million Account credentials in that breach. Authorities of LinkedIn immediately invalidated the password of the accounts impacted, and they advised the customer to reset their passwords. Later security officials of the LinkedIn have beefed up the security mechanism of password databases with a new technique called hashing and salting.
- **Uber:** A massive hack that hit Uber in 2016, to delete users credentials and keep breach quiet firm paid $1,00,000. They hacked 57million users and drivers credentials; however sensitive information such as location data, birth date, and bank information had not been compromised.
- **Facebook:** The Facebook-Cambridge Analytica data scandal involves the collection of credentials of 87 million users of Facebook. The way that Cambridge Analytica gathered user's information was called inappropriate. The stolen data was used in the 2016 presidential election for influence voter opinion by the political representatives who hired Cambridge Analytica. This scandal paved the way for ethical standards for social media sites and many demanded greater security to prevent such an incident.

2.3 Authentication techniques in the cloud environment

Cloud computing authentication technique hinges on two important goals such as 1) Ensuring authorized persons can access the resources, 2) keeping an unauthorized person away from gaining access to resources in this environment. There is a number of components involved in accomplishing these tasks. This section expounds the various authentication techniques in the cloud environment as follows.

- Password based Authentication
- 2-Factor Authentication
- Multi-Factor Authentication
- Single Sign-on
- Key Stroke Analysis
- Graphical Authentication
- Remote User Authentication
- Shared Authority based Authentication
- **Password-Based Authentication:** Single-factor authentication scheme allows the user to define username and password to login to the cloud to access the data. This scheme is still in practice but it is not considered as best practice as a password leak leads to data breaches.
- **2-Factor Authentication:** It is referred to as 2-way verification and provides an extra layer of security to safeguard the user's data. It strengthens the security layer so the hacker cannot access the data available in the cloud.
- **Multi-Factor Authentication:** It supports two or more credentials for better security transaction. It improves the authentication status by including physical characteristics of user's biometrics such as fingerprint, voice, typed characters, eyries, and patterns in keypress intervals etc. It is more robust against the unauthorized person and illegal access.
- **Single sign-on:** Is a session and authentication process, by which user can access multiple applications with a single set of login credentials. Exchanging of user credentials across cloud are done by the SSO protocols such as Kerberos and SAML (Security Assertion Markup Language).
- **KeyStroke Analysis:** It is also called Keystroke biometrics that is used for an authentication process. Keystroke biometrics includes fingerprints, retinal scans, and DNA to verify the user's authentication to access the resources from the cloud.
- **Graphical Authentication:** A graphical password authentication system allows a user to select an image from the graphical user interface and verifies the user's identity before allowing them to access the resources from the cloud.

- **Remote User Authentication:** A kind of authentication mechanism to verify the legitimacy of a user based on a smart card or biometric attributes and allows them to communicate with the cloud server to access the shared resources.
- **Shared Authority based Authentication:** To encounter the privacy issue for cloud storage, a Shared Authority based privacy-preserving authentication protocol has been implemented.

3. Related work

Technological advancement as well as the growing popularity of online banking, customers face potential risks like hacking of account, loss of money etc. Hence it is very essential to have a strong authentication mechanism. Chao Li et al[1], proposed a strong "A Two-Factor Authentication Design of Fingerprint Recognition System Based on DSP and RF Card". In this paper, fingerprint recognition combined with Smart card verification is proposed. The author proposed a strong authentication algorithm processing unit called TI's (Tenas Instrument) TMS320VC5510 (DSP). This architecture consists of five significant modules: Image gathering, Image processing, storage devices, Synchronous and asynchronous communication, and human-machine interaction. FPC1011C is a novel leading-edge capacitive fingerprint sensor based on the Certus Sensor Platform provides a strong fingerprint authentication system. In this system, the RF card component contains a universal asynchronous receiver/transmitter (UART) interface, which is designed to receive and transmit the data in a secure way. This algorithm exhibits high performance with low computation.

The proliferation of e-commerce facilitates user to perform a transaction through systems which are connected to the remote server to access the given services. To ensure remote authentication Tsague et al[2], implemented a good authentication scheme called "An Advanced Mutual-Authentication Algorithm Using 3DES for Smart Card Systems". In this paper, the author proposed an advanced mutual authentication scheme using 3DES to enhance smart cards based mutual authentication schemes security levels and to circumvent the different attacks. This scheme provides mutual authentication of identity, verification of the authenticity of the remote server, smart card reader and secures session key agreement, providing much security protection for smart card users and the server. In this scheme, Smart card details are encrypted using 3DES encryption technique. The design of this scheme consists of three phases such as registration; authentication and Password update which works well against various attacks.

The Internet has turned-up almost all the field and so online shopping and one can buy anything on-the-go. As online transactions are done by credit card, there may be various attacks are possible. To perform any transactions securely Muhammet et al[3], devised a system called "Combining Biometric ID Cards and Online Credit Card Transactions". This proposed system uses the concept of Turkish e-ID pilot system to verify user identification using strong multi-factor authentication which combines Biometric ID as well as Credit Card parameters. Turkish e-ID system offers, various Identity Verification Package (IVP), which include different parameters such as timestamp, biometric details, and demographic data to provide strong authentication system. This approach protects both end-user and business people from unauthorized services.

With the increase of heterogeneous information system in the enterprise, there are different access mechanisms and access policies require powerful authentication mechanism. Having this in mind, Yang et al[4], implemented a well-authenticated system called "The Optimization Mechanism Research of Distributed Unified Authentication Based on Cache". This paper proposes a unified authentication mechanism based on a cache with distributed architecture. It can manage multiple nodes and deal with high concurrent requests, so as to ensure the stability of the authentication system and improve the response time. The author also designs and implements a multi-factor cache replacement algorithm based on Hybrid (Hybrid-MF). The results show that the cache-based distributed unified authentication mechanism

proposed in this paper can effectively improve the response time and deal with concurrent pressure better.

Jaspher Willsie, et al[5], introduced an Elliptic Curve cryptographic algorithm used for secure key generation and exchange. To raise the security level Smart Card based authentication scheme is proposed. Login & mutual authentication scheme verifies the client's authentication with an authentication server (AS) using Biohash which develops a hashed password and provides a biometric template. This scheme uses ECC based encryption, verification, and Signing. One of the advantages of ECC based scheme key size is low (i.e) 160 bits when compared to 1024 of RSA. This secure framework enables secure user authentication in cloud computing and mobile cloud users. The proposed scheme ensures low communication cost and biometric framework provides secure storage and transmission.

To secure organizational data from hackers, R.Nikam, et al[6], implemented a novel approach called "Cloud Storage Security using Multi-Factor Authentication". This paper proposes CP-ABE (Ciphertext-Policy – Attribute-Based Encryption and Multi-Factor Authentication (MFA) ensures the sharing of data between peer organization keeping the identity anonymous. In this paper, static username and password ensure initial level authentication followed by OTP based on Token (TOTP Algorithm) generator technique that is considered as credentials for users. This multi-level security system provides better cloud storage security using MFA, Encryption technique and this security check keep the hacker away from accessing the cloud environment.

The proliferation of ubiquitous computing environment and internet technology needs strong authentication technique. As authentication plays a very vital role in the field of a cloud environment, Salman H.Khan et al[7], proposed "Multi-Factor Authentication on Cloud". This paper proposes a novel authentication verification mechanism that combines human inherence factor (handwritten signature biometrics) with standard knowledge factor (traditional user-specified password) to have an enhanced security mechanism. In this proposed scheme, GAE (Google Application Engine) is used as cloud service provider, a hierarchical approach is used to perform signature matching and to ensure the authenticity of biometric, decision forest classifier is used. Easily scalable, low cost and resource allocation makes this scheme works well in smaller groups environment, but not suitable for large groups.

To address the security vulnerabilities of the traditional e-voting system, Oke B.A et al[8], introduced a system called "Developing Multifactor Authentication Technique for Secure Electronic Voting System". A well-known Multifactor Authentication scheme using Biometric fingerprint and a smart card that is cryptographically secured is proposed in this paper. This paper will focus on authentication, issues in verifying and validating the legitimate voters. Enhanced Feistel block cipher and First-moment feature extraction technique makes this system more secure and provides better confidentiality. The disadvantage of this system is, the Multifactor authentication is not integrated with the cryptographic model.

Cloud computing environment is known for providing various services over the internet; hence data security plays a very vital role. To have a secure access to cloud services one needs a good authentication system. R.K.Banyal et al[9], implemented a novel framework called "Multi-factor Authentication Framework for Cloud Computing". In this proposed framework, the user is authenticated using multifactor's which includes a Secret key, One Time Password and IMEI Number. Arithmetic Captcha Expression is also used to enhance the authentication process to access the cloud services and resources. A novel approach called Secret Splitting of Authentication Factor boost the security mechanism and provides the additional layer of security for this trusted environment. This scheme mitigates almost all possible attacks in a cloud environment.

Y.Shah et al[10],coined a well-known authentication system called "Multi-Factor Authentication as a Service". In this scheme, Multi-Factor authentication architecture combines the features of Identity Federation and Single-Sign-on methodologies such as the OpenID framework which provides for the modular integration of various factors of authentication. MFAaaS aggregates authentication factors and exposes them to services. This improved federated identity management framework to provide enhanced secure

MFA, which consists of all forms of authentication factors including both on-device and in-network authentication.

As most of the organization started to utilize the functionality of cloud, security plays an important concept to safeguard the data access and services. Niharika Gupta et al [11], implemented an authentication scheme called "Implementing High Grade Security in Cloud Applications using Multifactor Authentication and Cryptography". The author proposed a robust authentication scheme based on the Ticket-based one-time password to achieve a high-security mechanism for restricting the unauthorized access. This work uses multiple hashing encryptions methodology to thwart an unauthorized user from gaining the access rights. This paper also packed with different methodologies such as DoS Attack and Brute Force Attack Prevention, Prevent Phishing Attacks using Image Verification, SQL Injection Prevention and SMS based OTP Approach to have sturdy authentication mechanism and for storage of data in the cloud securely.

The integration of Internet of Things with Cloud paved a new concept called Cloud of Things which provides scalability, virtualized control and access to services provided by IoT. Here security plays a very crucial role in deploying the CoT. To address this Rohan et al[12], introduced a concept called "A Multifactor Authentication System using Secret Splitting in the perspectives of CoT". This paper clearly explains the Multifactor Authentication Scheme in three phases. Using multiple factors such as a smart card, biometric and encryption algorithm for authentication increases the security level.

Cloud computing model consists of the data owner, service provider and users. To have a secure transmission of data between these entities needs a strong security mechanism. The data in the cloud should always be kept confidential, maintain its integrity and above all accessed by an authenticated person. To achieve these, Nalini.S et al[13], devised an authentication mechanism called "MLA Scheme: Multi-Level Authentication for data in Cloud using NTP-Server and Biometric". The author proposed a multi-level Authentication scheme such as password-based authentication at initial level then biometric and timestamp-based authentication using NTP server. The crypto-system model ensures a strong authentication process which combines the functionality of biometric (fingerprint), and NTP time-stamps generated by NTP Server, data confidentiality, and integrity thus strong multi-level authentication is ensured.

Cloud computing field are faced an exponential growth in recent years that leads to many challenges and issues. One of the important challenges is ensuring the user authentication. To provide a strong authentication scheme B. S. Al-Attab et al[14], proposed a novel authentication scheme called "Authentication Scheme for Insecure Networks in Cloud Computing". The proposed authentication scheme combines the functionalities of USB Token based on Hash function and Diffie-Hellman key exchange. This two-factor authentication protects the network and also data with less cost and without needing any additional device. Yet, the user's data is still susceptible to various attacks.

The proliferation of cloud computing environment paves a way for many enterprises and government agencies to get their job done with ease. Yet, the strong authentication mechanism is required for accessing the data in the cloud environment. Hence, J. P. Singh et al[15], introduced a new kind of mechanism called "Authentication and Encryption in Cloud Computing" This paper proposes strong authentication mechanism based on tree structure which improves the user's authentication process and Elliptic Curve Digital Signature Algorithm ensures the data integrity. This method increases the efficiency of storage and retrieval of data. This scheme takes less time for key generation and signature verifying process.

Yassin et al[16], proposes the two- factor authentication scheme which consists of password authentication and canny's edge detection to encrypt/decrypt the image. In this work, mutual authentication and one-time password between user and service provider are done at the first phase. During the second phase, Canny[s edge detection feature are utilised to encrypt/decrypt image which ensures mutual authentication, session key agreement, defends from replay attack, impersonation attack, forgery attack, reflection attacks, and parallel session attacks. It has lower transmutation cost with high security. A Valid user can select the valid password.

S.M.Barhate et al[17], had a review on "User Authentication issues in Cloud Computing". This paper highlights the interoperability environment in the cloud, which throws security challenges and privacy. Four different kinds of interoperability use cases are proposed to address the security challenges. This paper clearly explains interoperability, authentication algorithms such as RSA, AES, MD5, OTP Password Generation Algorithm, DES, Rijndael Encryption Algorithm, user authentication and authorization techniques and authentication protocols such as LDAP, EAP, and SSO protocols were also studied.

The proliferation of CRAN (Cloud Radio Access Network) requires a good authentic mechanism to guarantee the secure access to resources and services. Hence Hui Yang et al[18], devised a novel authentication technique called "Blockchain-based trusted authentication in cloud radio over fiber network for 5G". In this paper, the author proposed a kind of authentication scheme called BAA (Blockchain-based Anonymous Access) for a blockchain-based trusted authentication (BTA) architecture in C-RoFN for 5G. Network access authentication can be done by BTA with a tripartite agreement between manufacturer, uses and network operator. Blockchain-based Authentication provides better security, credibility and accessing of the network with low network cost.

Justin LeJeune, et al[19], proposed a new approach called "An Algorithmic Approach to Improving Cloud Security - The MIST and Malachi Algorithms". This paper proposes two different kind's algorithms called MIST and Malachi which ensures strict measures and methodologies for strengthening the cloud against the security attacks. This MIST algorithm works well against the weak password and account breach by incorporating highly user-specific questions. The Malachi algorithm safeguards the account information and protects the hackers from accessing the login credentials. Less computation makes this algorithm weak and it provides less security.

Emerging and popular cloud environment provide huge storage provision and it requires distinctive encryption and decryption algorithm to protect the data. Ali AZOUGAGHE, et al[20], proposed a new algorithm called "An Efficient Algorithm for Data Security in Cloud Storage". This paper proposed asymmetric encryption of Elgamal encryption scheme and symmetric encryption of AESC algorithm. The author also viewed as an extension of the Diffie-Hellman key exchange protocol. This algorithm implemented for file upload and file download phases. The author compares two algorithms such as RSA and Elgamal algorithms. The efficient way of algorithm carried out experiments on text file sizes. Two algorithm key sizes of 1024 for RSA and 160 bits for Elgamal.AES algorithm provide a fast and safe symmetric algorithm. The advantage of this paper, an unauthorized user never gets the data accidentally because two keys coming from two different locations.

Table 1. Comparisons of various authentication factor

Name of the Work	Authentication Factor	Verification Scheme, Methodology, Advantage, and Limitations
A Two-Factor Authentication Design of Fingerprint Recognition System Based on DSP and RF Card	Two Factor Authentication	– Fingerprint recognition – Five modules: Image gathering, Image processing, storage devices, Synchronous and asynchronous communication, and human-machine interaction – Universal Asynchronous Receiver/Transmitter (UART) Interface. – Certus Sensor platform provides a strong authentication system – Speed optimization causes less quantizing accuracy – Low image processing
An Advanced Mutual-Authentication	Mutual Authentication	– Proposes authentication algorithm using 3DES – Smart Card details are encrypted using 3DES – It consists of three phases like registration,

Algorithm Using 3DES for Smart Card Systems		authentication and password update – Good authentication scheme – Heavy computational process
Combining Biometric ID Cards and Online Credit Card Transactions	Multi Factor Authentication	– Biometric ID and Credit Card parameters – Propose Multi-factor authentication combines biometric-ID and Credit Card parameters – Turkish-ID consists Identify Verification Package – Ready to use Security and Identification Infrastructure – Fraud possibility is very high
The Optimization Mechanism Research of Distributed Unified Authentication Based on Cache	Multi Factor Authentication	– Cache-based Unified authentication mechanism – Manage multiple nodes and deals concurrent requests – Multifactor cache replacement algorithm – The Hybrid-MF algorithm can deal with complex user better – Good response time – Improved cache hit ratio – Maintaining cache is a time-consuming task
A Secure framework for Enhancing User authentication in Cloud Environment Using Biometrics	Mutual Authentication	– Provides secure user authentication, mutual authentication, session key issue and proxy issue – Smart card based user authentication – Highly used in the mobile cloud – Secure key generation and exchange algorithm – Insecure Biohash technique – No clear explanation for computing the Nonce of value
Cloud Storage Security using Multi-Factor Authentication	Multi Factor Authentication	– Static Username and Password ensures initial level authentication and OTP based on (TOTP) Algorithm – Authentication and Encryption (CP-ABE) provides the safest environment – Provides a good authentication system. – Ensures better storage security – Computational cost is high
Multi-Factor Authentication on Cloud	Multi Factor Authentication	– Combines Human inherence factor and traditional password schemes – Hierarchical based Signature matching and Decision forest classifier are used to verify the authenticity – Low cost and good resource allocation scheme – Not fit for large groups
Developing Multifactor Authentication Technique for Secure Electronic Voting System	Multi Factor Authentication	– Biometric Fingerprint and a Smart Card based authentication scheme – Feistel Block Cipher – First-moment feature extraction technique – More secure and provides better confidentiality – Not integrated with the cryptographic model
Multi-factor Authentication Framework for Cloud Computing	Multi Factor Authentication	– Multi-factors such as Secret key, One Time Password and IMEI Number – Arithmetic Captcha Expression is also used to enhance the authentication process – Secret splitting of Authentication Factor – Mitigates the hacker's effect

		– Too many authentication parameters
Multi-Factor Authentication as a Service	Multi Factor Authentication	– Identity Federation and Single Sign-on methodology such as OpenID Framework – MFAaaS aggregates all authentication factors – Secured MFA provides better security – Unpopular
Implementing High Grade Security in Cloud Applications using Multifactor Authentication and Cryptography	Multi Factor Authentication	– Ticket-based One Time Password – Multiple hashing encryption methodology – Image verification, SQL Injection and SMS based OTP for sturdy authentication scheme – Prevents unauthorized attacks such as DDoS and Brute Force – Heavy computational process
A Multifactor Authentication System using Secret Splitting in the perspectives of CoT	Multi Factor Authentication	– Multiple factors such as smart card, biometric and encryption algorithm provide better security – This system uses Ex-OR operations, Encryption and Diffie-Hellman key exchange algorithm – Multiple factors increase the security level – Requires a number of hardware devices
MLA Scheme: Multi-Level Authentication for data in Cloud using NTP-Server and Biometric	Multi Level Authentication	– Multi level authentication combines the Password-based authentication, Biometric and Time-stamp based authentication using NTP Server – Exhibits strong authentication process – Only suitable for UNIX environment
Authentication Scheme for Insecure Networks in Cloud Computing	Two Factor Authentication	– Two-factor authentication combines the functionalities of USB Token based on Hash function and Diffie-Hellman key Exchange scheme – Protects data and network with low cost – User's data is susceptible to various attacks
Authentication and Encryption in Cloud Computing	Single Factor Authentication	– Tree structure based authentication keeps the unauthorized person at the bay – Elliptic Curve Digital Signature algorithm ensures data integrity – Takes very less time for key generation and signature verifying process – Simple authentication scheme
Cloud Authentication Based on Encryption of Digital Image Using Edge Detection	Two Factor Authentication	– Authentication phase consists of Image and User's password – A biometric method with Canny's edge detection – Edge Pixels of Image is encrypted using a stream cipher – Works well against the various attacks – Low transmutation cost – Use of MD5 may exhibit poor security scheme
User Authentication issues in Cloud Computing	Authentication Algorithm MD5	– Interoperability – RSA, AES and MD5 algorithm for authentication and encrypting the files – Authentication protocols such as LDAP, EAP, and SSO are explained – Insist the Security, Privacy measure, and

		Interoperability – Security issues are not addressed fully
Blockchain-based Trusted Authentication in Cloud Radio over Fiber Network for 5G	BTA (Blockchain-based Trusted Authentication)	– Authentication scheme called BAA (Blockchain-based Anonymous Access) for a blockchain-based trusted authentication (BTA) architecture in C-RoFN for 5G – Provides better security with the low-cost network – Agreement amount tri-party may be weak
An algorithmic approach to Improving Cloud Security: The MIST and Malachi Algorithms	MIST and Malachi Algorithms	– Data integrity and strong security – Users data protected through account security – To eliminate the weak passwords and account recovery vulnerability – MIST-Implementation of the question and answer system – Malachi-Different approach to account security – An innovative method for account recovery – To protect accounts in regular logins. – Statistical analysis not efficient
An Efficient Algorithm for Data Security in Cloud Storage	AES Algorithm	– Symmetric (AES) and Asymmetric (Elgamal encryption scheme) encryption – 128-bits keys for 10 cycles of repetition, 192-bit keys for 12 cycles and 256-bit keys for 14 cycles, in symmetric key encryption with rotation – Includes file upload and file download phases – AES is safe and fast in both directions (upload and download) – Takes more time for execution
An Enhanced Hybrid Data Security Algorithm for Cloud	AES, ECC and SHA-256	– Combination of hybrid data security cryptographic algorithm such as DES, AES, RSA, ELgamalMD5, SHA – Has a fine security concept – Large message size not applicable
Data Storage Security Algorithms for Multi-Cloud Environment	Public Auditability Algorithm, Data Dynamics Algorithm, Integrity Proof Algorithm, Privacy-Preserving Algorithm	– Need advanced cryptographic technique to secure data – Auditability - for storing and securing data – TPA (Third Party Auditor) – for privacy and secrecy of data and manages data based on SLA's (Service Level Agreements) – Ensures integrity and confidentiality of data – Auditing uses low-cost communication and computing technology – Data consistency is checked by TPA without downloading the data – Too many algorithms make the work cumbersome
Private Cloud Security: Secured User Authentication by using Enhanced Hybrid Algorithm	Enhanced Hybrid Algorithm	– Elliptic Curve Authentication Algorithm verifies the Authentication – Hybrid of AES and Blowfish provides good security – Key Generation and Exchange are done by Elliptic Curve – Diffie Hellman – MAES (Modified Advanced Encryption Standard) with 256-bit – Enhanced authentication scheme. – Attack by XSL (Extended Sparse Linearization)

		is possible
Proposal and Implementation of Cloud Security Algorithm to Enhance the Security of the Layers	Honey Encryption Algorithm	– Honey Encryption Algorithm combined with DES provides supplementary Security layer – Honey Encryption Algorithm increases the probability of deciphering the key – Data is more secure and free from all types of attacks – Level of complexity is high
Providing Security, Integrity and Authentication Using ECC Algorithm in cloud storage	Electronic Curve Cryptographic Algorithm	– Electronic Curve Cryptographic Algorithm for better security, authentication – Data Integrity is verified by Metadata – Metadata are created and encrypted by ECC – Less CPU power and Processing time – Not fit for the big environment
A Two-Factor Authentication Design of Fingerprint Recognition System Based on DSP and RF Card	Two Factor Authentication	– Fingerprint recognition – Five modules: Image gathering, Image processing, storage devices, Synchronous and asynchronous communication, and human-machine interaction – Universal Asynchronous Receiver/Transmitter (UART) Interface – Certus Sensor platform provides a strong authentication system – Speed optimization causes less quantizing accuracy – Low image processing
An Advanced Mutual-Authentication Algorithm Using 3DES for Smart Card Systems	Mutual Authentication	– Proposes authentication algorithm using 3DES – Smart Card details are encrypted using 3DES – It consists of three phases like registration, authentication and password update – Good authentication scheme – Heavy computational process
Combining Biometric ID Cards and Online Credit Card Transactions	Multi Factor Authentication	– Biometric ID and Credit Card parameters. – Propose Multi-factor authentication combines biometric-ID and Credit Card parameters – Turkish-ID consists Identify Verification Package – Ready to use Security and Identification Infrastructure – Fraud possibility is very high
The Optimization Mechanism Research of Distributed Unified Authentication Based on Cache	Multi Factor Authentication	– Cache-based Unified authentication mechanism – Manage multiple nodes and deals concurrent requests – Multifactor cache replacement algorithm. – The Hybrid-MF algorithm can deal with complex user better – Good response time – Improved cache hit ratio – Maintaining cache is a time-consuming task
A Secure framework for Enhancing User authentication in Cloud Environment	Mutual Authentication	– Provides secure user authentication, mutual authentication, session key issue and proxy issue – Smart card based user authentication – Highly used in the mobile cloud – Secure key generation and exchange algorithm

Using Biometrics		– Insecure Biohash technique – No clear explanation for computing the Nonce of value
Cloud Storage Security using Multi-Factor Authentication	Multi Factor Authentication	– Static Username and Password ensures initial level authentication and OTP based on (TOTP) Algorithm – Authentication and Encryption (CP-ABE) provides the safest environment – Provides a good authentication system – Ensures better storage security – Computational cost is high
Multi-Factor Authentication on Cloud	Multi Factor Authentication	– Combines Human inherence factor and traditional password schemes – Hierarchical based Signature matching and Decision forest classifier are used to verify the authenticity – Low cost and good resource allocation scheme – Not fit for large groups
Developing Multifactor Authentication Technique for Secure Electronic Voting System	Multi Factor Authentication	– Biometric Fingerprint and a Smart Card based authentication scheme – Feistel Block Cipher – First-moment feature extraction technique – More secure and provides better confidentiality – Not integrated with the cryptographic model
Multi-factor Authentication Framework for Cloud Computing	Multi Factor Authentication	– Multi-factors such as Secret key, One Time Password and IMEI Number Arithmetic Captcha Expression is also used to enhance the authentication process – Secret splitting of Authentication Factor – Mitigates the hacker's effect – Too many authentication parameters
Multi-Factor Authentication as a Service	Multi Factor Authentication	– Identity Federation and Single Sign-on methodology such as OpenID Framework – MFAaaS aggregates all authentication factors – Secured MFA provides better security – Unpopular
Implementing High Grade Security in Cloud Applications using Multifactor Authentication and Cryptography	Multi Factor Authentication	– Ticket-based One Time Password – Multiple hashing encryption methodology – Image verification, SQL Injection and SMS based OTP for sturdy authentication scheme – Prevents unauthorized attacks such as DDoS and Brute Force – Heavy computational process
A Multifactor Authentication System using Secret Splitting in the perspectives of CoT	Multi Factor Authentication	– Multiple factors such as smart card, biometric and encryption algorithm provide better security – This system uses Ex-OR operations, Encryption and Diffie-Hellman key exchange algorithm – Multiple factors increase the security level – Requires a number of hardware devices
MLA Scheme: Multi-Level Authentication	Multi Level Authentication	– Multi level authentication combines the Password-based authentication, Biometric and Time-stamp based authentication using NTP

for data in Cloud using NTP-Server and Biometric		Server – Exhibits strong authentication process – Only suitable for UNIX environment
Authentication Scheme for Insecure Networks in Cloud Computing	Two Factor Authentication	– Two-factor authentication combines the functionalities of USB Token based on Hash function and Diffie-Hellman key Exchange scheme – Protects data and network with low cost – User's data is susceptible to various attacks
Authentication and Encryption in Cloud Computing	Single Factor Authentication	– Tree structure based authentication keeps the unauthorized person at the bay – Elliptic Curve Digital Signature algorithm ensures data integrity – Takes very less time for key generation and signature verifying process – Simple authentication scheme
Cloud Authentication Based on Encryption of Digital Image Using Edge Detection	Two Factor Authentication	– Authentication phase consists of Image and User's password – A biometric method with Canny's edge detection – Edge Pixels of Image is encrypted using a stream cipher – Works well against the various attacks – Low transmutation cost – Use of MD5 may exhibit poor security scheme
User Authentication issues in Cloud Computing	Authentication Algorithm MD5	– Interoperability – RSA, AES and MD5 algorithm for authentication and encrypting the files – Authentication protocols such as LDAP, EAP, and SSO are explained – Insist the Security, Privacy measure, and Interoperability – Security issues are not addressed fully
Blockchain-based Trusted Authentication in Cloud Radio over Fiber Network for 5G	BTA (Blockchain-based Trusted Authentication)	– Authentication scheme called BAA (Blockchain-based Anonymous Access) for a blockchain-based trusted authentication (BTA) architecture in C-RoFN for 5G – Provides better security with the low-cost network – Agreement amount tri-party may be weak
An algorithmic approach to Improving Cloud Security: The MIST and Malachi Algorithms	MIST and Malachi Algorithms	– Data integrity and strong security – To eliminate the weak passwords and account recovery vulnerability – MIST-Implementation of the question and answer system – Malachi-Different approach to account security – An innovative method for account recovery – To protect accounts in regular logins – Statistical analysis not efficient
An Efficient Algorithm for Data Security in Cloud Storage	AES Algorithm	– Symmetric (AES) and Asymmetric (Elgamal encryption scheme) encryption – 128-bits keys for 10 cycles of repetition, 192-bit keys for 12 cycles and 256-bit keys for 14 cycles, in symmetric key encryption with rotation – Includes file upload and file download phases – AES is safe and fast in both directions (upload

	and download) – Takes more time for execution

4. Authentication Algorithm

Many organizations and enterprises store their important data on the cloud and these data are also accessed by many people (end user). To verify the user identity or credential for accessing the data or valuable resources available in the cloud environment, the cloud service provider employs an authentication process which involves in the process of validating a user's identity and allows them to access the needed resources from the cloud environment. It is the mechanism of verifying an incoming request with a set of identifying credentials and gives them permission to access the same. Encryption involves the process of transforming data from one format into another so that it is unreadable by anyone who does not have proper credential information. To provide better security to cloud users, a number of authentication algorithm and encryption algorithms are designed with distinctive features. To verify the authenticity of the cloud environment, the authentication algorithm uses the concept of a shared key. Two famous authentication algorithms are widely used in the cloud environment, they are MD5 and SHA1.

MD5 (Message Digest – Algorithm) is a widely used hash function, capable of producing a 128-bit fixed-length message digest which is typically represented as a sequence of 32 hexadecimal digits. To have an additional level of hashing MD5-HMAC (Hashed Message Authentication Code) can be used. The security of MD5 is severely compromised, as the size (128 bits) is small enough. The MD5 exhibits the poor security against the collision attack and not suitable for applications like SSL Certificates and Digital Signatures.

SHA-1 (Secure Hash Algorithm-1) a strong authentication algorithm is capable of producing 160-bit message digest from 264-bit of input message, which ensures that data has not been altered and begins from intended source. SHA-1 HMAC (Hashed Message Authentication Code) provides additional level hashing. SHA-256, SHA-384, and SHA-512 are variants of SHA-1 which are capable to process of Advanced Encryption Standard (AES), Data Encryption Standard (DES) and Triple (3DES) DES Encryption. SHA-1 Algorithm is widely used in security applications and protocols which includes TLS and SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 provides better security against various attacks.

Table 2. The comparison between MD5 and SHA

Key for Comparison	MD5	SHA
Security	Less secure than SHA	High secure than MD5
Message Digest Length	128 Bits	Upto 512 Bits
Attackers effect	2^{128} bit operations required to break	2^{160} bit operations required to break
Attacks to find two messages producing the same MD	2^{64} bit iteration needed to break	2^{80} bit iteration needed to break
Speed	Faster, only 64 iterations	Slower, required 80 iterations
Success rate	Vulnerable	More secure than MD5

5. Conclusion

As explained, Cloud undoubtedly is the best thing in the computing world. Cloud computing is also known as distributed computing since it has the capability to run many applications over a single resource on a network. The Cloud environment is known for a wide range of computing resources such as networks, storage, servers, and services. These precious resources can be accessed and processed by the valid users from the cloud server at anytime and anywhere via the secure channel of the Internet with great flexibility and ease. Yet, the ever-growing computing technology still faces major problem related to the authenticity of the user, where authentication is a process which ensures and verifies the legitimate user's identity before allowing them to access the data from the cloud and also it prevents the unauthorized user's from accessing the data. From the above discussion, it is evident that various existing authentication schemes have many problems and disadvantages, so, it is imperative to have well-defined authentication schemes to allow the legitimate users to access the various resources from the opulent cloud computing environment. In our proposed scheme, it is planned to implement strong multi-factor authentication based on three basic requirements such as something the user knows, something users have and the user is, for allowing the legitimate user to access the cloud storage server and data's with less computational cost and time.

6. Reference

1. Chao, Li.,& Jin, Qi. (2010). A Two-Factor Authentication Design of Fingerprint Recognition System Based on DSP and RF Card. *The 2nd International Conference on Computer and Automation Engineering (ICCAE),* Singapore, 441-445.
2. Tsague, H. D., Nelwamondo, F., &Msimang, N. (2012). An Advanced Mutual-Authentication Algorithm using 3DES for Smart Card Systems. *Second International Conference on Cloud and Green Computing*, Xiangtan, 660-666.
3. Yildiz, M., &Göktürk, M. (2010). Combining Biometric ID Cards and Online Credit Card Transactions. *Fourth International Conference on Digital Society*, St. Maarten, 20-24.
4. Yang, D., &Kai, F. (2017). The Optimization Mechanism Research of Distributed Unified Authentication Based on Cache. *14th Web Information Systems and Applications Conference (WISA)*, Liuzhou, 297-300.
5. Kathrine, G. J. W. (2017). A Secure Framework for Enhancing User Authentication in Cloud Environment using Biometrics. *International Conference on Signal Processing and Communication (ICSPC)*, Coimbatore, 283-287.
6. Nikam, R., &Potey, M. (2016). Cloud Storage Security using Multi-Factor Authentication. *International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Jaipur, 1-7.
7. Khan, S. H.,& Akbar, M. A. (2015). Multi-Factor Authentication on Cloud. *International Conference on Digital Image Computing: Techniques and Applications (DICTA)*, Adelaide, SA, 1-7.
8. Oke, B. A., Olaniyi, O. M., Aboaba, A. A., &Arulogun, O. T. (2017). Developing Multifactor Authentication Technique for Secure Electronic Voting System. *International Conference on Computing Networking and Informatics (ICCNI)*, Lagos, 1-6.
9. Banyal, R. K., Jain, P., &Jain, V. K. (2013). Multi-Factor Authentication Framework for Cloud Computing. *Fifth International Conference on Computational Intelligence, Modelling and Simulation*, Seoul, 105-110.
10. Shah, Y., Choyi, V., &Subramanian, L. (2015). Multi-factor Authentication as a Service. *3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, San Francisco, CA, 144-150.
11. Gupta., Niharika., Rani., &Rama. (2015). Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography. *International Journal of Web & Semantic Technology.* 6. 09-17.

12. Shah, R. H., &Salapurkar, D. P. (2017). A Multifactor Authentication System using Secret Splitting in the Perspective of Cloud of Things. *International Conference on Emerging Trends & Innovation in ICT (ICEI)*, Pune, pp. 1-4.
13. Nalini, S., &Andrews, J. (2016). MLA Scheme: Multi-Level Authentication for Data in Cloud using NTP-server and Biometric. *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC),* Chennai, pp. 1-3.
14. Al-Attab, B. S.,& Fadewar, H. S. (2016). Authentication Scheme for Insecure Networks in Cloud Computing. *International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC),* Jalgaon, pp. 158-163.
15. Singh, J. P., Mamta., &Kumar, S. (2015). Authentication and Encryption in Cloud Computing. *International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM),* Chennai, pp. 216-219.
16. Ali Yassin, A., Abullah., Hussain, A., &Keyan Abdul-Aziz Mutlaq. (2015). Cloud Authentication Based on Encryption of Digital Image Using Edge Detection. *International Symposium on Artificial Intelligence and signal Processing (AISP).*
17. Barhatel, S. M., &Dhore, M. P. (2016). User Authentication Issues in Cloud Computing. *National Conference on Recent Trends in Computer Science and Information Technology,* pp. 30-35.
18. Yang, H., Zheng, H., Zhang, J., Wu, Y., Lee, Y., &Ji, Y. (2017). Blockchain-Based Trusted Authentication in Cloud Radio over Fiber Network for 5G.*16th International Conference on Optical Communications and Networks (ICOCN)*, Wuzhen, pp. 1-3.
19. LeJeune, J., Tunstall, C., Yang, K. P., &Alkadi, I. (2016). An Algorithmic Approach to Improving Cloud Security: The MIST and Malachi Algorithms.*IEEE Aerospace Conference*, Big Sky, MT, pp. 1-7.
20. Azougaghe, A., Kartit, Z., Hedabou, M., Belkasmi, M., &El Marraki, M. (2015). An Efficient Algorithm for Data Security in Cloud Storage. *15th International Conference on Intelligent Systems Design and Applications (ISDA)*, Marrakech, pp. 421-427.