A Novel Cloud Authentication Framework

Latifa Khalid ALnwihel
Department of Computer Science
King Faisal University
Alahsa, Kingdom of Saudi Arabia
Latifaalnwihel@gmail.com

Abdul Raouf Khan
Department of Computer Science
King Faisal University
Alahsa, Kingdom of Saudi Arabia
raoufkhan@kfu.edu.sa

***Abstract*— Cloud computing is a medium that provides cost reduction with storage and fast computation environment. Various organization are marching to the cloud because of the several advantages provided such as remote access, cost efficiencies and simplified IT infrastructure and management. However, for any distributed or shared system, security is the main requirement. The research work discuss the numerous researchers work regarding cloud security issues, threats, known vulnerabilities and their solutions. Hence, the available threats in the cloud system are discussed to come up with an improved framework that provide data security through multiple techniques. The proposed research work combines cryptography, authorization and authentication mechanisms in order to ensure access control.**

Keywords—cloud computing, threat, vulnerabilities, cryptography, authorization, authentication.

I. INTRODUCTION

Nowadays the need for data has extended and led to increased number of online users. Besides, the reality of the difficult and expensive traditional computing infrastructure, it become impossible for consumer to access data anywhere and at any time. Thus, for saving data, the external storage system become on handy. Due to the raised usage of internet globally, cloud computing concept developed dramatically. Cloud environment provide a collection of computing resources which is managed by cloud service providers. Cloud provider who provides the cloud services to users is responsible for allowing users to get the most services that cloud provides like creating their web services etc. In the form of software, infrastructure, and platform the cloud services are delivered by the cloud service providers over the internet through virtualization and multi-tenancy techniques. Cloud computing is a medium which works via internet to uploaded data and applications with help of remote servers. It offers users and organization the ability to use applications, access individual files without the need for installation from any computer has internet connection. Moreover, the issue of limited resources has been solved with the cloud development, it also offered resource sharing among multiple users in order to reduce services cost.

A primary concern regarding cloud computing and it is for both cloud users and cloud providers, is the security of the services provided through cloud. Therefore, cloud computing security become at risk due to the different threats and attacks. Hence, the cloud services are vulnerable to various security threats and attacks such as data breaches, insecure interfaces and APIs, account hijacking, denial-of-service (DoS) attacks, authentication attacks etc. Appropriate authentication and data protection schemes are the answer to most of the security threats. However, such issues are not of cloud providers concerns due to lack of innovation and authentication vulnerabilities. The cloud data must be secured against unauthorized access. Thus, authentication mechanism must be involved prior user access to cloud. In this research work, cloud environment threats and the available solutions are studied to provide methodologies to overcome the data security issue. Thus, the research focus on exploring the different available authentication frameworks to propose a framework that guarantees access control in the cloud and provide authentication through multiple methodologies.

The remainder of this paper is structured as follows. Section II describe the available related works regarding various authentication and access control frameworks and models in the field of security in cloud computing. In Section III, threats and vulnerabilities in the cloud computing infrastructure are discussed. Section IV specifies the proposed framework which intended to ensure access control through authentication. Section V concludes and summarize the overall work which has been done.

II. LITERATURE REVIEW

A. *Authentication Frameworks*

Established on the traditional elliptic curve cryptography digital signature system, Longge et al. [1] propose an improved model to guarantee the security of transmitted data and achieve better efficiency in the cloud. The aim of the paper is to use Digital Signature Scheme Based on Elliptic Curve in order to develops the identification protocols according to the cloud needs such as security, authentication and efficiency. The identification protocol confirms that only genuine customers are allowed to sign and verify the document. As a result, the signature forgery is prevented, and the integrity of the data is ensured. Two parts composed to form the signature scheme; first the signature algorithm which consist of the message signature written by the signers' private key. The authentication algorithm is the second part, it works by authenticating the signature through the signer's public key. The operator is responsible to ensure the computer network's identity, in this

978-1-7281-7624-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CSCI51800.2020.00243

process, one of the parties responsible to assure the second party identity. The developed algorithm, in order to improve the signature efficiency, modular inversion is not required. According to the elliptic curve digital signature system, the identification information of the signer or the verifier are entered to the verification system/ log signature. The client and the server side are connected through shared network by common channel transmission which might be prone to malicious attacks. Therefore, the paper claim that the server side should gain more attention towered the user identification to enhance the system security. Thus, server identification protocol is introduced to confirm that only genuine customer are allowed signing the document along with verification request, while maintaining data integrity and avoiding imitation of signature. The introduced algorithm includes the participants' seeking to access, personal information, ID number, their public key and the signer signature. From the experiment conducted in the paper, it appears that the proposed algorithm can eliminate the modular inverse operation which enhance the operational efficiency in order to be employed in the cloud. However, multiplicative group of a finite field solution algorithm index is not usable to the proposed model which need to be found.

Jian Shen et al. [2] propose a lightweight mutual authentication based on identity system for cloud computing by using string concatenation, hash functions and exclusive-or operations. Three roles form the scheme; user, cloud server and agency. The agency acts as a third party who's employed to generate security parameters and identity for authorized users and cloud server. Request phase, response phase and authentication phase are three phases that the scheme go through. In the request phase, the customer and the cloud server generate a random number and identity request to be sent to the agency respectively. Accordingly, to the legitimacy the agency processes the request by either generating identity or not, response phase. The agency will produce the identity for the user and cloud server along with timestamp and security parameters, if the request satisfies the verification process. In the third phase the user sends the received identity, timestamp and the random number to the cloud server. Then the server will verify the validity of the timestamp of the customer by computing using (string concatenation operations, the one-way hash functions and XOR operations), the user is authenticated if the result is equal otherwise the server reject login. While in the server authentication phase, the cloud server directs the received identity, timestamp and the random number to the user. After that the user will check the validity of the timestamp of the server by computing using (string concatenation operations, the one-way hash functions and XOR operations), the server is authenticated if the result is equal otherwise it is illegal, and the user avoid accessing it. Having the agency as a third party can be drawback to this scheme since main computation are transferred to it.

Subhash et al. [3] propose a framework by combining Kerberos and Pretty Good Privacy (PGP) to achieve fine grained security in cloud. Kerberos is an authentication protocol which provide confidentiality, message integrity and mutual authentication. This protocol can prevent replay attacks and eavesdropping, by verifying the communicating parties' identities as it adopts secret key cryptography. Authentication Server, real server and Ticket Granting Servers are the three servers that form the Kerberos system. Based on the concept of third trusted party, the authentication server act as the third trusted party in the system. This server keeps the registered users' credentials in its database and responsible to verify the user and generate a session key for user and Ticket Granting Servers communication. The Ticket Granting Servers provides session key to be used for real server and user communication and it generate a ticket for the real server. The real server provides users services. Pretty Good Privacy (PGP) is cryptographic computer program which provide privacy and authentication by data encryption. PGP comes in two versions public key RSA and Diffie-Hellman. The proposed framework workflow as, Kerberos get the user identity from registration, then it provides ticket for user and real server (service provider) communication. For later use the Kerberos send the user identity (credentials) to the real server. Afterward the user gets to encrypt the data to be sent through cloud. The user is authenticated by PGP which submit the encrypted data of the user to the cloud. The real server delivers the desired data to PGP. Then the user authentication information and the data are decrypted by PGP, the user get to receive the decrypted data if the user access is authorized. The authentication starts when authentication server receives the user service request and submit an encrypted message along with permanent symmetric key. This message consists of (1) session key to be used in user and Ticket Granting Servers communication and (2) an encrypted ticket for Ticket Granting Servers with its symmetric key. The permanent symmetric key is created by appropriate algorithm when the user type in his/her symmetric password which is used to create the permanent symmetric key and then destroyed immediately. The user now uses the created permanent symmetric key to decrypt the received message and obtain the session key and the ticket. Then the user submits the ticket, the name of the real server and the timestamp (encrypted by session key) to the Ticket Granting Servers. The Ticket Granting Servers deliver two tickets, one for user encrypted with the session key, second ticket for server encrypted with its public key. The user submit ticket along with timestamp which is encrypted by the user ticket to the real server. As a result, the real server adds 1 to the timestamp to confirm receiving and encrypt the message by the user ticket to be sent to the user. After Kerberos authentication, the user use PGP for next data encryption and authentication for integrity and confidentiality purpose. To ensure authentication and integrity, digest calculation and digital signature are used. The PGP provides confidentiality by compressing message and encrypting it with a session key and encrypt the session key and send both encryptions concatenated to the real server. The real server decrypts the session key using his/her private key and apply it to decrypt the message to find the compressed message. Note that the paper states that Kerberos cannot delivers the feature of non-repudiation in communication.

Pachipala et al. [4] propose a method by using RSA for data security storage in the cloud. RSA is implemented before the sensitive data is kept in the cloud and whenever these data requested for usage by the user, the data are decrypted. This method can prevent unauthorized access to the cloud where the data are encrypted then stored in the cloud. However key generation mechanism needs to be revised since it is not durable against major attacks regarding user identity and the privacy of cloud data.

For assuring confidentiality and privacy of cloud users, Shiva et al. [5] propose a framework of two-layers attribute-based encryption. In the proposed framework a coarse-grained encryption is performed by the owner to guarantee data confidentiality. In the first layer of the framework Hashed Message Authentication Code (HMAC) algorithm applied on sensitive attributes to produce encrypted data. Then in the second layer by employing some substitution technique the data is re-encrypted and access control policies are performed. Also, mechanism is introduced in which user data is decrypted when the identity attributes fulfil the owner policies while keeping the customer identity attribute confidential. The system consists of users, owner, cloud storage service and identity provider. The identity provider issue special identity attribute by assigning unique token for users. The user identity is encoded in the unique token and only the identity attribute value is represented. To download decrypted files on the owner site, the user is required to register. By registering the user is given identity token by the owner and accordingly formed key using Key Derivation algorithm to be used in decrypting. Noting that the owner has no awareness about the user identity attribute value or the type of policy condition the user confirmed to. Before uploading to the cloud, the user has to encrypt the file and if authorization policies changes, data files must be re-encrypted. Managing encryption keys are user responsibilities. The efficiency of the method reduces in case of huge data. Having several encrypted copies with the same key which required to be stored cause high computational costs. Furthermore, key management issue is huge drawback in the framework.

With the help of Message Authentication Code (MAC) and Secure Socket Layer (SSL), Sandeep in [6] propose a framework to protect the data throughput the entire cloud process. Two phases form this proposed framework. In the first phase the data transferring and storing is performed by dividing the process into three sections, Index Building and encryption, Classification and Message Authentication Code (MAC). Based on the cryptographic parameters; availability, integrity and confidentiality the data in the cloud is kept in different segments, private, public, limited access. It is the responsibility of the owner to classify the data into these segments in which the user specifies where his/ her data lies and sensitivity rating (SR) will be calculated. Index builder is used to help in case of encrypted data retrieval (searching throughout encoded data). This method is performed by assigning an index to a list of keywords while each keyword holds a list of pointers to the files in which that keyword shows. For more security the index is also encrypted. Secure Socket Layer (SSL) encryption is employed in the mechanism in which encryption and decryption is accomplished by a single key to prevent unauthorized access. Message Authentication Code (MAC) is produced after data encryption to be transferred with it into the cloud. It is used to verify whether the data has been altered during data transmission. Afterward, the encrypted data will be stored in the cloud based on the calculated Sensitivity Rating (private, public, limited access). In the second phase data retrieval is clarified in which the user is supposed to register to the owner by receiving a username and password. The user credentials are stored in the cloud directory. In this phase if accessing cloud data is required then the user will submit the username along with the request of accessing. Also, double authentication is carried on, one verification of digital signature and second integrity. Based in the request sensitive rate, the cloud take action, if the request for public segment then no authentication is required. Otherwise if private or limited access segment is requested then authentication is a must by checking the provided username. To authenticate the user the password is submitted to the owner then the user receives from the owner a security question if the answer is correct then the customer is authenticated. The digital signature and the customer identity are sent to the cloud by the owner to specify that this user approved to access the data. Later on, the owner sends their digital signature when the user submits the request for data along with the requested data keyword and the master key for decryption purpose. The user gets to forward the received from the owner to the cloud beside search request. If the digital signature is verified, then using the keyword, search request is processed by returning a list of matching encrypted data. Finally, to check the integrity of the data MAC is used. There is key size and cost trade off occurs in the framework if the key size increases then the cost increases.

B. *Access Control Frameworks*

Miao et al. [7] presented an approach for privacy preserved access control in cloud computing. The authors presented encryption scheme of two-tier in order to reach fine-grained and flexible access control. This is done by proposing a server re-encryption mechanism (SRM) and policy hidden attribute-set based encryption. This scheme aims to prevent cloud provider from observing and intruding on the user data while allowing data owner to define cloud users. Policy-hiding features is supported in this scheme to provide security against collusion attacks initiated by malicious users. Attribute-set-based encryption act as the base tire of the system and the surface tier is server re-encryption mechanism. Every data file is tied with an access structure in which various attributes sets are produced. Using attribute-set based encryption enable multiple customers to apply corresponding secret key to decrypt the data file, which is not used to encrypt access structure. Server re-encryption mechanism is involved in the scheme to avoid the situation when the user leaves or joins the cloud from updating their private keys. Although cloud server is responsible for data re-encryption, attribute list and file content are not disclosed. In this scheme the data is encrypted and sent by the data owner to the cloud and invoke second level dynamic password generator which is performed by server re-encryption mechanism (SRM). In the first phase of this scheme, according to the access policies, the data owner gets to perform attribute-set based encryption before sending the data to the cloud (Base phase). In the second phase, when the cloud server receives the data owner request, a dynamic encryption operation is performed on the encrypted data. The user can obtain the desired file by downloading it from the cloud through decryption key. This access control is not flexible if attribute-set based scheme goes alone. Moreover, it turned out that this presented scheme, lack scalability and flexibility, which make it ineffective.

By addressing the issue of insecure APIs in CC, Avvari et al. [8] proposes a mechanism of two stage access control by adopting the Role Based Access Control Model (RBAC). The proposed access control policy in executed at the API level. In this paper the authors assume that the customer is authenticated by some method, in the first stage after the user is authenticated, credentials and attributes of the user is taken. Taking the user attribute such as the IP address or the domain name helps to identify where the user belongs to. Via the user attributes it is checked with the maintained database of the registered users which identifies their domain name or any other attribute. Typically, the first stage acts as defense to confirm that only registered customers from the database can access the cloud resources. In organization, the cloud service provider and the organization itself decide on a set of roles and then associate the permissions with the roles and then customers tied to these roles. In case if the enterprise is willing to make changes, immediate updates need to be done in the organization's policy. In the second stage, according to the user role the permissions to the cloud services are determined which is carried out by the Role Based Access Control. For organizations this mechanism can simplify the process to map a customer's local role to the role to access the service in the cloud which referred as global role. However, in this mechanism, authentication is an important aspect which is not clarified.

Attribute-based access control offers data owners the ability to integrate data access policies in the encrypted data, therefore, Yan et al. [9] presents a scheme for Temporal Access Control Encryption (TACE) by employing proxy-based re-encryption mechanism based on the present time and cryptographic integer comparisons. The need to associate each outsourced resource with access policy on a set of temporal attributes is the main purpose to propose this scheme. According to the comparative attributes a license is assigned to user which accumulate numerous privileges. Proxy-based re-encryption mechanism is implemented to apply valid matches between customer's privileges and access policies with respect to the present time. RSA and Co-CDH assumption are used to prove the security of the used function (forward and backward derivation functions). The authors goal is to accomplish temporal cloud data access control upon saved files. Since TACE scheme aims for temporal cloud access control and re-encryption method, five algorithms are included. The framework starts by taking as input a list of attribute and security parameter to produce the public key and master key (setup algorithm). Then the access privilege, the user ID number and the master key are taken as input to produce the user private key (key generation algorithm). Next, the public key is taken as input along with a temporal access policy to produce a random session key and ciphertext header (encryption algorithm). The public key, current time and the ciphertext header are taken as input to produce new ciphertext header (re-encryption algorithm). Finally, the new ciphertext header on the current time and the user private key is taken as input to output a session key (decryption algorithm). The used integer comparison scheme is based on OR/AND logical operations and bitwise comparisons. This scheme is applicable only to systems wherein both service providers and data owners exists within the exact trusted domain.

III. THREATS AND VULNERABILITIES

Threat is defined according to NIST Security Glossary as "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" [10]. In other word threat refers to possible danger which leads to system harm. Threats occurrence affects the cloud in term of illegal or damaging access of user's confidential data. While vulnerabilities refer to weaknesses or flaws exploited by a threat that cause the intended system to fail in specific security policy, consequently initiating harm or loss. According to the Cloud Security Alliance (CSA) [11], the 2019 Top Threats are reported in this section. The ranking of the Egregious Eleven threats are based on the importance according the survey results, they are listed as;

1. Data Breaches
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking
6. Insider Threat
7. Insecure Interfaces and APIs
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services

1. *Data Breaches*

It occurs when the user confidential data are viewed, released or stolen by unauthorized individuals. A data that is leaked which is not intended to be released for public is considered data breaches such as health information. This has multiple effects on the business field, it can affect the trust and reputation of partners, brand impact causing the market value to decrease, loss of intellectual property and other. This happens due to vulnerabilities such as human errors, targeted attacks, poor security practices, poor review of controls, application vulnerabilities, incorrect authentication or authorization mechanisms, operating-system failures or undependable use of encryption keys. CSA implies that through encryption techniques, data can be protected against this threat, yet system performance is negatively affected.

2. *Misconfiguration and Inadequate Change Control*

This threats a new top threat which could lead to data breaches threat. It occurs due to incorrect set up of computing assets resulting in malicious activity such as excessive permissions, unsecured data storage elements, Standard security controls disabled and unchangeable configuration settings and Default credentials. In the cloud computing environment, misconfiguration is caused due to the absence of control change. CSA implies that automation should be involved by the organization in which technologies are employed to continuously misconfigured resources and provide solution in real-time.

3. *Lack of Cloud Security Architecture and Strategy*

Since organization are transferring their work to the cloud, many of them ignore the challenge of implementing a security architecture to avoid attacks. Moreover, they lack the understanding of the responsibilities of the security of the shared resources. In the cloud environment this introduces a lack of security architecture and strategy exposing the organization to various security attacks. CSA indicate that this could be avoided by developing a robust security strategy and appropriate security architecture framework to create a strong base and perform the required business activities in the environment.

4. *Insufficient Identity, Credentials, Access and Key Management*

The organizations make use of access management, credential, identity which embrace policies and tools to secure, manage and monitor the available resources in the cloud. It is an important aspect for organizations to understand the security regarding cloud provider identity solution, especially if identity federated with a cloud provider. This include infrastructure, processes and segmentation among users. Multifactor authentication systems, phone authentication and One-Time Password (OTP) are the best practices in which password theft addressed. Cryptographic keys management helps to address attacks regarding unauthorized access to keys. According to CSA, to avoid high risk of misuse, it is a good practice to prevent embedding cryptographic keys and credentials in distributed public repositories or source code.

5. *Account Hijacking*

It refers to attackers gaining unauthorized access to user account in order to take over the control of it. The cloud security depends on Application Programming Interfaces APIs since this threat happens through APIs when the cloud service provider offers users services through these interfaces. It has various forms such as fraud, exploitation of software vulnerabilities and phishing which leads to data loss. This threat happens due to the vulnerabilities such as Man in the middle attack, weak credentials, malware infection or social engineering attacks. CSA recommend involving in-depth defense and identity and access management (IAM) controls indicating that it’s the mitigation key for account hijacking and to promote threats awareness through organization to enclose breach damage.

6. *Insider Threat*

Malicious employees in the cloud can perform insider attacks to steal the user confidential data since they have authorized access. The attacker could be third-party contractor, current or previous employee or industry partner. This involves information theft, fraud, damage and misuse of the available resources. This threat occurs due to the vulnerabilities such as system administrator, business partner, former employee or third-party connector. To help mitigate and minimize the consequences of insider threats, CSA recommends the following actions, regular employee awareness training, security education and training for employee, access restricted to critical systems, misconfigured cloud servers Fixing.

7. *Insecure Interfaces and APIs*

Since cloud is accessed through APIs (Application Programming Interfaces) and user interfaces (UIs) which expose the cloud resources, it is required to secure them to manage and monitor the provided cloud services. Providing security to APIs include multiple features such as access control, authentication, activity monitoring and encryption technique to deliver security and availability to the provided services. Additionally, to provide protection against intentional malicious access and accidental threats. This threat happens due to the vulnerabilities such as weak API credentials, hypervisor bugs, operating system bugs or key managements. CSA recommends using standard and open API frameworks, appropriate protection of API keys and evade reuse and API hygiene practice.

IV. THE IMPROVED FRAMEWORK

To accomplish access control in the cloud, only authorized indivduals can access to the cloud. Therefore, authentication and authorization are significant requirements to provide access control and ensure data privacy. The access control is assured through 3-step authentication and Reputation Value (RV).

Authorization is provided via Ciphertext-Policy Attribute-Based Encryption (CP-ABE) usage. Confidentiality is garanteed within Ciphertext Policy-Identity–Attribute-Based Encryption (CP-IDABE) mechanism. Fig. 1 presents the introduced framework. The proposed framework consists of Data Owner (DO), User, the Cloud Service Provider (CSP) and Cloud Server (CS). For Cloud Server, Two- Server Architecture is used in order to avoid DoS attacks and to ensure the availability requirement. It also avoids Single Point Failure (SOF) where server fails to perform. Therefore, the cloud server involves two authentication servers; Front-end Authentication Server (FAS) and Back-end Authentication Server (BAS). Note that although user and data owner can only interact with Front-end Authentication Server (FAS), but both servers accomplish the desired tasks together. Thus when (FAS) receive a request of any type, it is forwarded to the Back-end Authentication Server (BAS) to make account of it and perform it as one server. The proposed framework has three phases Registration phase, Authentication phase and Encryption phase. Each phase is described below:

1. Registration Phase

This phase ensure that users are registered to the cloud. Through this process the user enters his/her username, password, answers to five question. This information allows the user to access the cloud through the log in process. The five questions will appear as a pop-up window when the user request data from the cloud, perform as authorization process in the cloud to avoid any chance of malicious user. Based on the user identity and the attributes of the answered question the data owner design the access policy. The user credentials are stored in the (BAS) for later use in encrypted form. Note that the five question changes periodically. The user is promoted to update the password periodically. When the user is registered, a Reputation Value (RV) is assigned to the user by (BAS) through (FAS). After this phase the user can login to access the cloud when authentication phase is accomplished.

2. Authentication Phase

The user can access the cloud by first registering to the cloud. In the login process the user goes through 3-step authentication process. In the first step user identity is authenticated by comparing the entered username and password (user credentials) to the stored data in the Back-end Authentication Server (BAS), if user identity match then the second step is displayed. The second step verifies if the user is a human or robot by using CAPTCHA method. After successfully passing the second step, in the third step One-Time-Password (OTP) is sent to the user contact information which can be email or phone number. This step ensure that the user is the genuine user who registered to the cloud. Upon the user access to cloud the Reputation Value (RV) is incremented with every access to the cloud. If this phase is achieved, then the user acquired cloud access which is limited for a specific period of time.

3. Encryption Phase

Attribute-Based Encryption (ABE) known for its capabilities to maintain the privacy of the data and fulfil access control in a fine-grained manner [12]. Through Ciphertext Policy–Attribute-based Encryption (CP-ABE) confidentiality and access control requirements can be guaranteed, in which access policy are defined by data owner through a set of attributes which are required from the user to retain to decrypt

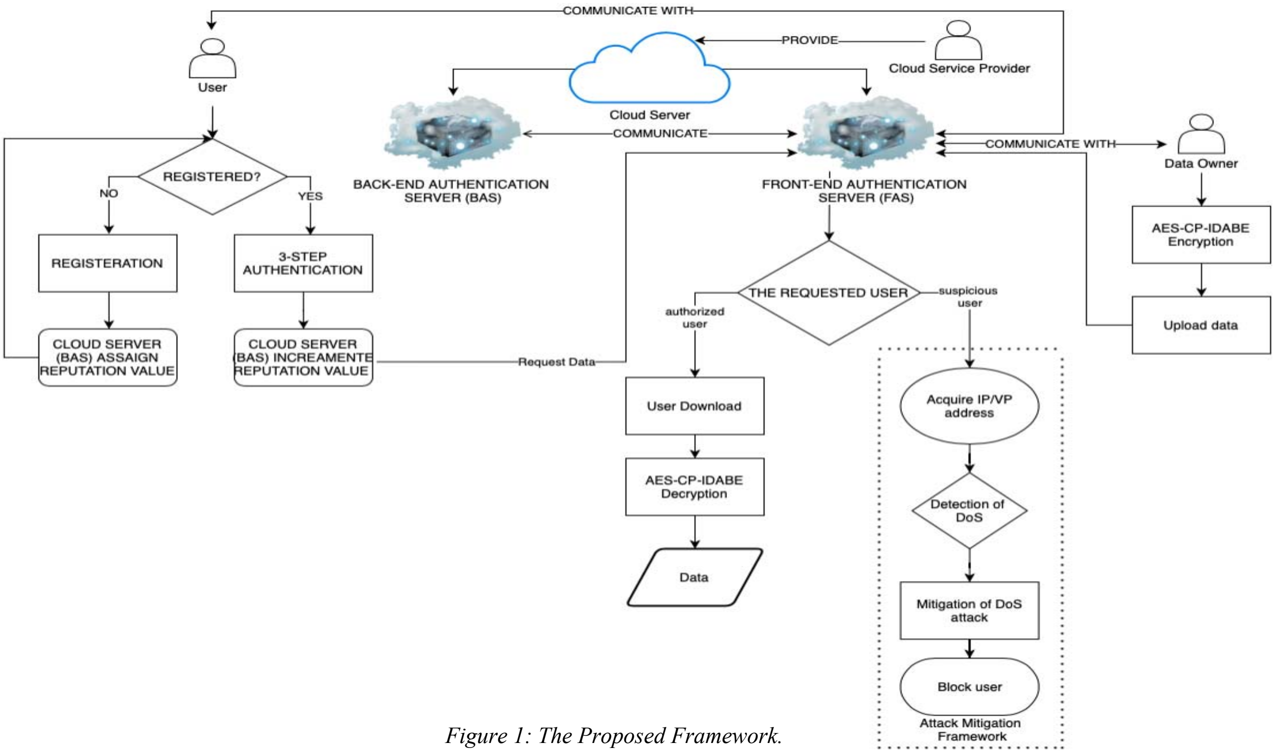

Figure 1: The Proposed Framework.

the ciphertext. In the encryption process the data is encrypted twice, once by the Ciphertext Policy-Identity–Attribute-Based Encryption (CP-IDABE) and another by AES algorithm. The set of attributes are used to provide user access to the desired data in the cloud.

The introduced double encryption mechanism AES–CP–IDABE, encrypt the data in the cloud with the CP–IDABE algorithm obtained secret key and public key, based on the secret parameter and its access policy. The digital signature is generated through the user identity, the access policy and the master key to provide access control. Verifying message is yields along with the digital signature. The encrypted data is encrypted again with AES algorithm to gain the double encrypted ciphertext along with the secret key and the message. While digital signature obtained through signature key. The proposed framework also, involve Denial of Service (DoS) attack detection and mitigation system, in order to avoid this type of attack in the cloud. The attack detection and mitigation framework is initiated by the Cloud Service Provider. In order to mitigate the attack, the framework works by capturing the IP address and then store it in the cloud server. In case of suspicious/melicios access to the cloud, then the user is blocked to maintain the cloud from Denial of Service attack (DoS).

V. CONCLUSION

This research work consider several issues in cloud computing architecture, access control, data confidentiality, data privacy and data availability. Through authentication, authorization and cryptographic mechanisms, a secure authentication framework is designed. Thus, an encryption model introduced by Sonali et al. [13] named "Advanced Encryption Standard–Ciphertext-Identity and Attribute-based Encryption" (AES–CP–IDABE) is adopted in the paper. The framework is formed of three phases, Registration phase, Authentication phase and Encryption phase to accomplish access control and privacy in the cloud environment. Finally, the main objectives of the research have been satisfied which are access control, confidentiality, data privacy, integrity and availability through the improved framework. In addition to better user experience in cloud via data protection, the proposed framework provide a strong authentication mechanism that is resistant against various threats like insecure interfaces, account hijacking, data breaches and authentication-based attacks like password discovery attacks and DoS attacks.

REFERENCES

[1] Longge Wang, Tao Song. (2016). An improved digital signature algorithm and authentication protocols in cloud platform. *International Conference on Smart Cloud* (pp. 319-324). USA: IEEE.

[2] Jian Shen, Dengzhi Liu, Shaohua Chang, Jun Shen, Debiao He. (2015). A Lightweight Mutual Authentication Scheme for User and Server in Cloud . *First International Conference on Computational Intelligence Theory, Systems and Applications (CCITSA)* (pp. 183-186). Taiwan: IEEE.

[3] Subhash Chandra Patel, Ravi Shankar Singh, Sumit Jaiswal. (2015). Secure and Privacy Enhanced Authentication Framework for Cloud Computing. *2nd International Conference on Electronics and Communication Systems (ICECS)* (pp. 1631-1634). India: IEEE.

[4] Pachipala Yellamma, Challa Narasimham, Velagapudi Sreenivas. (2013). DATA SECURITY IN CLOUD USING RSA. *Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT).* India: IEEE.

[5] Shiva Verma, Sachin Ahuja. (2016). A Hybrid Two Layer Attribute Based Encryption for Privacy Preserving in Public Cloud. *International Conference on Inventive Computation Technologies (ICICT).* India: IEEE.

[6] Sandeep K. Sood. (2012). A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications, Elsevier*, 1831–1838.

[7] Miao Zhou, Yi Mu, Willy Susilo, Man Ho Au, Jun Yan. (2011). Privacy-Preserved Access Control for Cloud Computing. *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 83-90). China: IEEE.

[8] Avvari Sirisha, G. Geetha Kumari. (2010). API Access Control in Cloud Using the Role Based Access Control Model. *Trendz in Information Sciences & Computing(TISC2010)* (pp. 135-137). India: IEEE.

[9] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and Shanbiao Wang. (2012). Towards Temporal Access Control in Cloud Computing. *The 31st Annual IEEE International Conference on Computer Communications: Mini-Conference*, (pp. 2576-2580).

[10] Celia Paulsen, Robert Byers. (2019). Glossary of Key Information Security Terms. In R. Kissel (Ed.). (pp. 1-218). Withdrawn NIST Technical Series Publication.

[11] Cloud Security Alliance CSA. (2020). *The Egregious 11 Cloud Computing Top Threats in 2019.* Cloud Security Alliance CSA.

[12] R. Velumadhava Rao, K. Selvamani. (2015). Data Security Challenges and Its Solutions in Cloud Computing. *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015)* (pp. 204-209). Elsevier.

[13] Sonali Chandel, Geng Yang and Sumit Chakravarty. (2020). AES–CP–IDABE: A Privacy Protection Framework against a DoS Attack in the Cloud Environment with the Access Control Mechanism. *Information*, 1-15.