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

DESIGNING SECURE AND EFFICIENT BIOMETRIC- BASED SECURE ACCESS MECHANISM FOR CLOUD SERVICES

Allu Yuvasri *1, G. Vinuthna Reddy *2, K. Akash *3, M. Vaishnavi *4 Dr. M.V.S. Prasad *5 , Shivaprasad Satla6

*1,2,3,4 Students of the Department of Computer Science and Engineering - Data Science, Malla Reddy Engineering College, Maisammaguda, Medchal, Hyderabad, Telangana

*5,6 Professor,Department of Computer Science and Engineering - Data Science
Malla Reddy Engineering College, Maisammaguda, Medchal, Hyderabad, Telangana.

Abstract : This study has been undertaken to investigate the determinants of stock returns in Karachi Stock Exchange (KSE) using two assets pricing models the classical Capital Asset Pricing Model and Arbitrage Pricing Theory model. To test the CAPM market return is used and macroeconomic variables are used to test the APT. The macroeconomic variables include inflation, oil prices, interest rate and exchange rate. For the very purpose monthly time series data has been arranged from Jan 2010 to Dec 2014. The analytical framework contains. Rather than an on location server cloud services will be services that are accessible from a dispersed cloud stockpiling worker. These measured frameworks are worked by an outsider and give clients access to PC assets, for example, investigation or systems administration over the Internet. Cloud Computing is utilized to give processing assets over the Internet and is utilized to store information on cloud workers. Security and information insurance have been a critical field of interest in cloud processing because of the sharing of assets. Cloud service suppliers store and hold client data through server farms that are influenced by information spillage.. It is observed that many mechanisms have stressed data protection and have neglected privacy in the subsequent process. Authentication aids with preserving and verifying the identity of a recipient. We also suggest an effective technique to use two biometric models for safe message transmission to create a session key between two interacting parties. Finally, the reliability and utility of the proposed solution was seen by detailed trials and a comparative analysis. Index Terms - Authentication, biometric-based security, cloud service access, session key.

IndexTerms **- Cloud Computing, Biometric Authentication, Finger Print Images, Remote Servers, Cryptography, Encryption**

I. INTRODUCTION

Cloud services are a norm in our society. However, providing secure access to cloud services is not a trivial task, and designing robust authentication, authorization and accounting for access is an ongoing challenge, both operationally and research-wise. A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos [1], OAuth [2] and OpenID [3] (see [1], [4]– [12]). Generally, these protocols seek to establish a secure delegated access mechanism among two communicating entities connected in a distributed system. These protocols are based on the underlying assumption that the remote server responsible for authentication is a trusted entity in the network. Specifically, a user first registers with a remote server. This is needed to ensure the authorization of the owner. When a user wishes to access a server, the remote server authenticates the user and the user also authenticates the server.

Once both verifications are successfully carried out, the user obtains access to the services from some remote server. One key limitation in existing authentication mechanisms is that the user's credentials are stored in the authentication server, which can be stolen and (mis)used to gain unauthorized access to various services. Also, to ensure secure and fast communication, existing mechanisms generally use symmetric key cryptography, which requires a number of cryptographic keys to be shared during the authentication process. This strategy results in an overhead to the authentication protocols. Designing secure and efficient authentication protocols is challenging, as evidenced by the weaknesses revealed in the published protocols of Jiang et al.

Specifically, we will first provide an alternative to conventional password-based authentication mechanism. Then, we demonstrate how one can build a secure communication between communicating parties involved in the authentication protocol, without having any secret pre-loaded (i.e., shared) information. In the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, we generate a private key that is used to enroll the user's credential secretly in the database of an authentication server. In the authentication phase, we capture a new biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a query. This queried biometric data is then transmitted to the authentication server for matching with the stored data. Oncethe user is authenticated successfully, he/she is ready to access his/her service from the desired server. To obtain secure access to the service server, mutual authentication

between the user and authentication server, and also between the user and service server have been proposed using a short-term session key. Using two fingerprint data, we present a fast and robust approach to generate the session key. In addition, a biometricbased message authenticator is also generated for message authenticity purpose. We summarize the key contributions/benefits related to the proposed approach as below. 1) An effective way to transmit the user's biometric data through the unsecured network channels to an authentication server is presented. 2) We propose an approach to generate a revocable private key directly from an irrevocable fingerprint image. There is no need to store the private key or a direct form of the user's biometric data anywhere. 3) We mitigate the limitation in traditional mechanisms that require the user's credentials to be stored in the purposes. PROPOSALFRAMEWORK: In this segment, we initially talk about the system model and threat model utilized in the proposed biometric-based authentication protocol (BioCAP), prior to introducing the different stages in BioCAP.

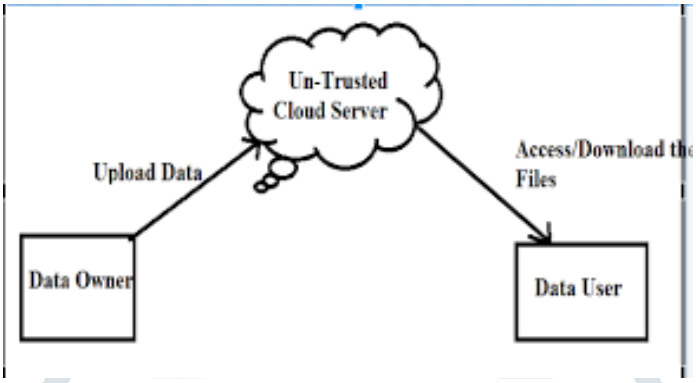

Figure 1 : Secure access mechanism for cloud services

The demand for remote data storage and computation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services. In this paper, we design a new biometric-based authentication protocol to provide secure access to a remote (cloud) server. In the proposed approach, we consider biometric data of a user as a secret credential. We then derive a unique identity from the user's biometric data, which is further used to generate the user's private key. In addition, we propose an efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission. In other words, there is no need to store the user's private key anywhere and the session key is generated without sharing any prior information. A detailed RealOrRandom (ROR) model based formal security analysis, informal (non-mathematical) security analysis and also formal security verification using the broadly-accepted Automated Validation of (AVISPA)toolreveal that the proposed approach h can resist several known attacks against (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utility of the proposed approach.

2. LITERATURE SURVEY

1.7.1C. Neuman, S. Hartman, K. Raeburn, "The kerberos network authentication service (v5)," RFC 4120, 2005.
This document provides an overview and specification of Version 5 of the Kerberos protocol, and it obsoletes RFC 1510 to clarify aspects of the protocol and its intended use that require more detailed or clearer explanation than was provided in RFC 1510. This document is intended to provide a detailed description of the protocol, suitable for implementation, together with descriptions of the appropriate use of protocol messages and fields within those messages.

1.7.2"OAuth Protocol." [Online]. Available: http://www.oauth.net/
The OAuth 2.0 specification defines a delegation protocol that is useful for conveying authorization decisions across a network of web-enabled applications and APIs. OAuth is used in a wide variety of applications, including providing mechanisms for user authentication. This has led many developers and API providers to incorrectly conclude that OAuth is itself an authentication protocol and to mistakenly use it as such. Let's say that again, to be clear: OAuth 2.0 is not an authentication protocol. Much of the confusion comes from the fact that OAuth is used inside of authentication protocols, and developers will see the OAuth components and interact with the OAuth flow and assume that by simply using OAuth, they can accomplish user authentication. This turns out to be not only untrue, but also dangerous for service providers, developers, and end users. This article is intended to help potential identity providers with the question of how to build an authentication and identity API using OAuth 2.0 as the base. Essentially, if you're saying "I have OAuth 2.0, and I need authentication and identity", then read on.

1.7.3 "OpenID Protocol." [Online]. Available: http://openid.net/
OpenID Authentication provides a way to prove that an end user controls an Identifier. It does this without the Relying Party needing access to end user credentials such as a password or to other sensitive information such as an email address. OpenID is decentralized. No central authority must approve or register Relying Parties or OpenID Providers. An end user can freely choose which OpenID Provider to use, and can preserve their Identifier if they switch OpenID Providers. While nothing in the protocol requires JavaScript or modern browsers, the authentication scheme plays nicely with "AJAX"-style setups. This means an end user can prove their Identity to a Relying Party without having to leave their current Web page. OpenID Authentication uses only standard HTTP(S) requests and responses, so it does not require any special capabilities of the UserAgent or other client software. OpenID is not tied to the use of cookies or any other specific mechanism of Relying Party or OpenID Provider session management. Extensions to User-Agents can simplify the end user interaction, though are not required to utilize the protocol. The exchange of profile information, or the exchange of other information not covered in this specification, can be addressed through

additional service types built on top of this protocol to create a framework. OpenID Authentication is designed to provide a base service to enable portable, user-centric digital identity in a free and decentralized manner.

3. PROPOSED SYSTEM

In the proposed approach, we consider a fingerprint picture of a client as a mystery qualification. From the fingerprint picture, we create a private key that is utilized to enlist the client's certification covertly in the database of an authentication server. In the authentication stage, we catch another biometric fingerprint picture of the client, and hence produce the private key and scramble the biometric data as a question. This questioned biometric data is then communicated to the authentication server for coordinating with the put away data. When the client is validated effectively, he/she is prepared to access his/her service from the ideal server. To get secure access to the service server, common authentication between the client and authentication server, and furthermore between the client and service server have been proposed utilizing a transient session key. Utilizing two fingerprint data, we present a quick and powerful way to deal with create the session key[1]. Likewise, a biometric-based message authenticator is produced for message realness purposes.

PROPOSAL FRAMEWORK: In this segment, we initially talk about the system model and threat model utilized in the proposed biometric-based authentication protocol (BioCAP), prior to introducing the different stages in BioCAP. A. System Model An outline of BioCAP is appeared in Fig. 3, which involves three elements. These elements are the client(s) (C), authentication server(s) (AS), and some asset server (RS). AS contains a database of clients' enlisted data, while AS creates RS's private key during the sending stage and it is divided among AS and RS. Likewise, both AS and RS incorporate an enormous vault of a comparative arrangement of engineered fingerprint pictures. Some manufactured fingerprint databases, for example, some openly accessible databases, are utilized in the proposed approach. At the point when C wishes to access a service from RS, C initially sends an authentication solicitation to AS. AS checks C's solicitation and sends an answer message to C upon fruitful confirmation. When C acquires the authentication answer message, C sends a service solicitation to RS for getting access. RS at that point confirms the service demand. On the off chance that the service demand is confirmed effectively, RS sends an answer to C. C and RS commonly validate one another. A session key among C and AS, and C and RS are utilized for resulting secure message interchanges. Further, the message legitimacy is constrained by a message authenticator.

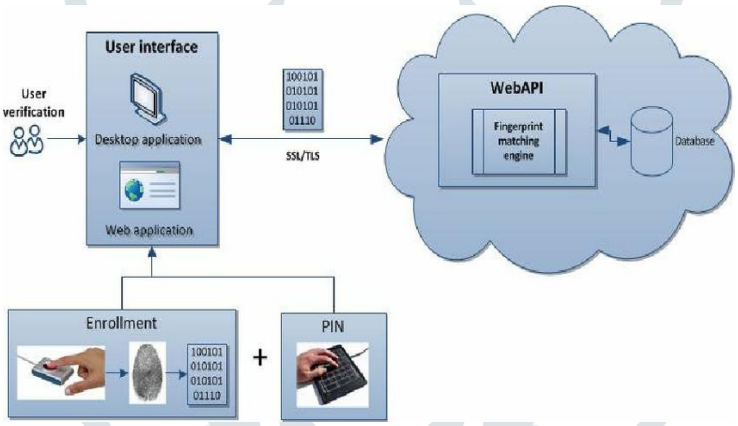

Figure 1: Scheme of the biometric verification system in the cloud

BioCAP has two key cycles, to be specific: client enrollment and client authentication. The client enlistment requires a private key generation, though client authentication requires the generation of the session key and the message authenticator. BioCAP gives an arrangement to turn over the private key of a client. Additionally, BioCAP is secure, computationally more affordable, and defeats the inborn shortcomings of biometric confirmation. Also, BioCAP doesn't require pre-shared keys, and gives a smooth common authentication system, and requests less number of keys to be overseen from application and client perspective.

4. IMPLEMENTATION

To run project double click on ‘run.bat’ file to get below output:
To run project double click on ‘run.bat’ file to get below output:

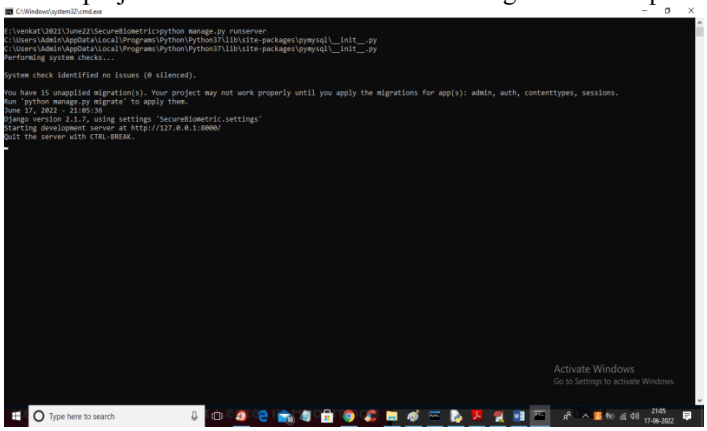

Fig.2 The command prompt for the secure biometry to run the server

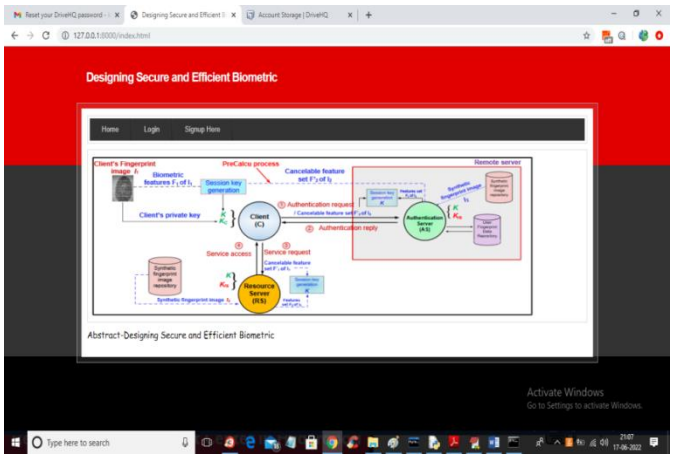

Fig.3 The front page of the website of secure biometry

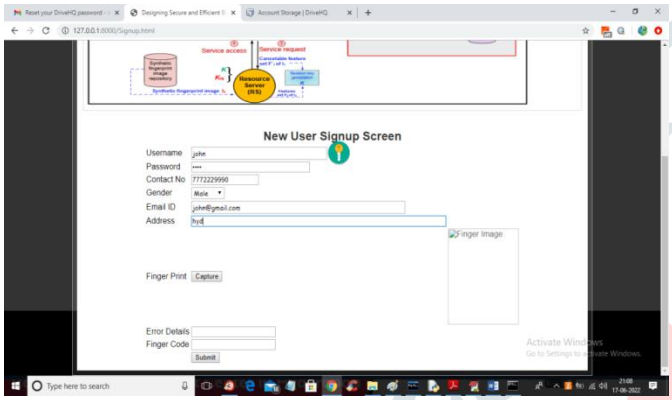

Fig.4 New User Signup Screen

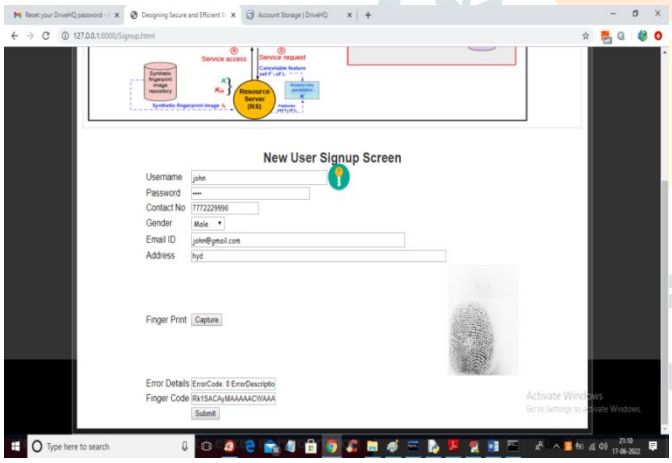

Fig.5 New User Signup Screen with User details

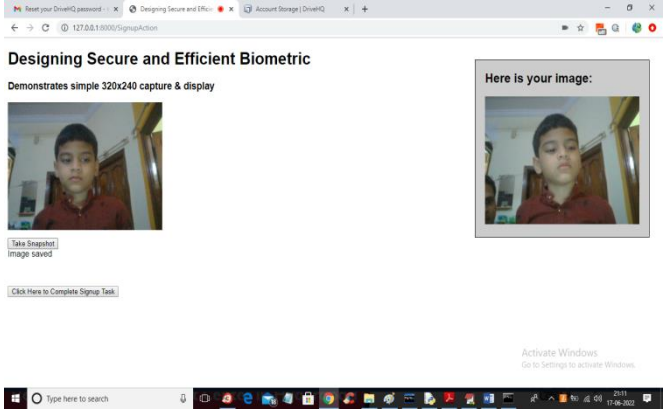

Fig.6 Capturing the face page for the verification and completing signup process

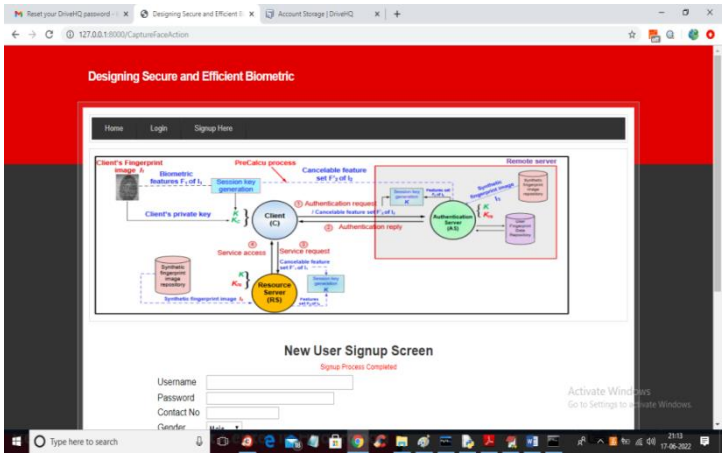

Fig.7 Signup Process Completed page

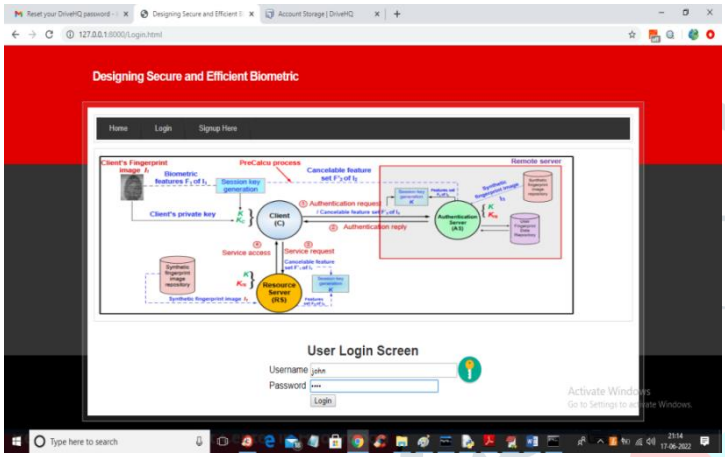

Fig.8 User Login Screen

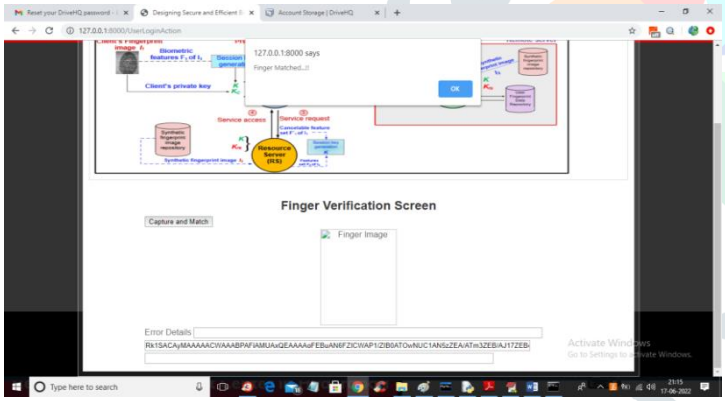

Fig.9 Finger Verification Screen

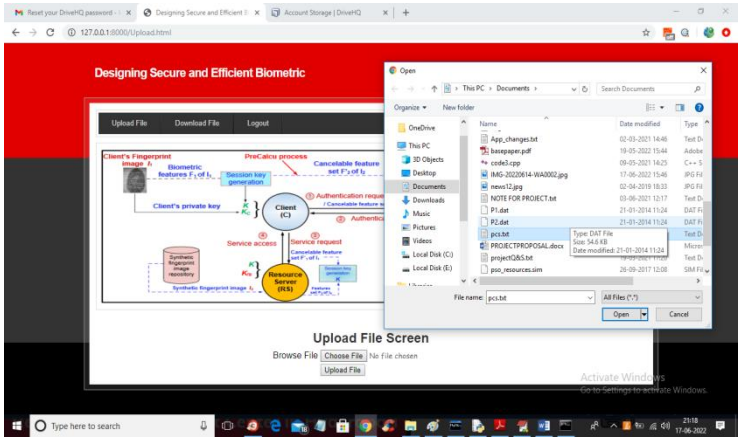

Fig.10: Upload File Screen

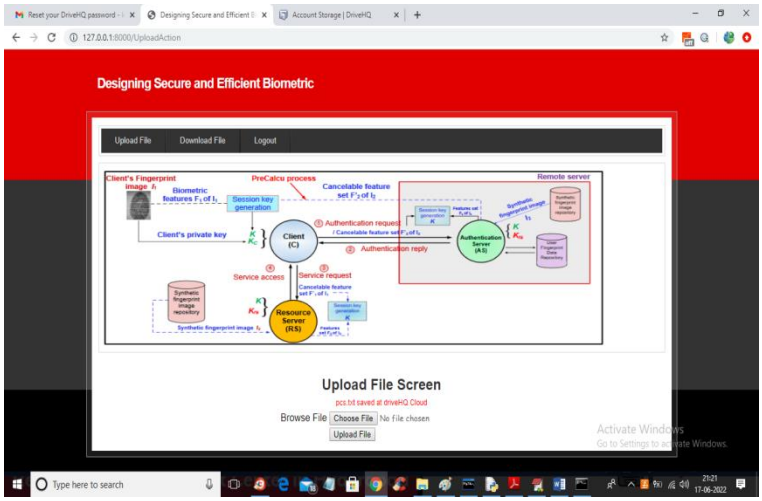

Fig.11 File Saved Screen

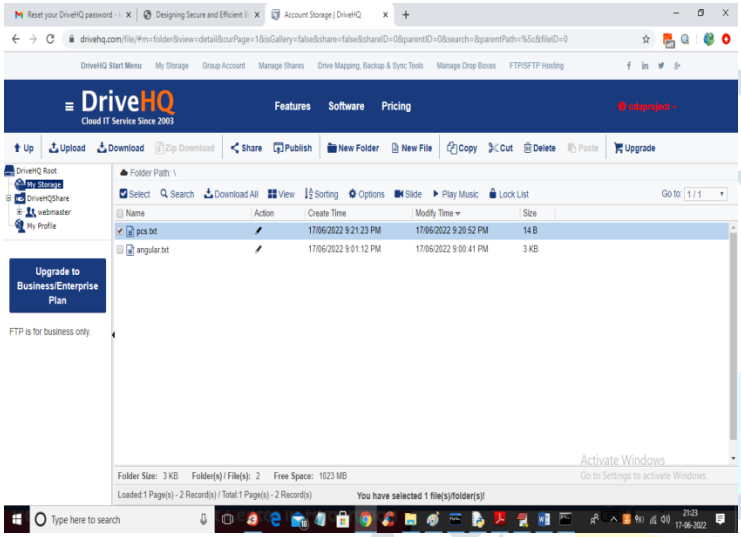

Fig.12 DriveHQ Cloud Service

5. CONCLUSION

In this, the imperative of establishing a secure and efficient biometric-based access mechanism for cloud services is underscored to safeguard the confidentiality and integrity of sensitive data. Biometric authentication emerges as a promising solution, reducing reliance on vulnerable password-based systems by leveraging unique individual characteristics. Throughout this study, the challenges and considerations in implementing biometric-based secure access mechanisms for cloud services have been examined, highlighting the need for a holistic approach. The inherent resistance of biometric authentication to impersonation attacks significantly mitigates the risk of unauthorized access and data breaches in cloud environments. Moreover, it enhances user experience and operational efficiency by eliminating complex passwords and reducing administrative overhead. However, successful implementation requires addressing privacy concerns, scalability, and interoperability challenges. Techniques like biometric template protection and secure transmission protocols are crucial for safeguarding user privacy, while standards-based approaches facilitate interoperability across platforms.

REFERENCES

[1] Ali, A. 2001.Macroeconomic variables as common pervasive risk factors and the empirical content of the Arbitrage Pricing Theory. Journal of Empirical finance, 5(3): 221–240.
[2] Basu, S. 1997. The Investment Performance of Common Stocks in Relation to their Price to Earnings Ratio: A Test of the Efficient Markets Hypothesis. Journal of Finance, 33(3): 663-682.
[3] Bhatti, U. and Hanif. M. 2010. Validity of Capital Assets Pricing Model.Evidence from KSE-Pakistan.European Journal of Economics, Finance and Administrative Science, 3 (20).
[4] R. S. Krishna, K. K. Srinivas, P. Anudeep and P. A. H. Vardhini, "Ear-Based Biometric System Using Artificial Intelligence," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2021, pp. 377-382, doi: 10.1109/ISPCC53510.2021.9609409.
[5] C. Neuman, S. Hartman, K. Raeburn, “The kerberos network authentication service (v5),” RFC 4120, 2005.
[6] Vardhini, P. H., Ravinder, M., Reddy, P. S., & Supraja, M. (2019). Power optimized Arduino baggage tracking system with finger print authentication. Journal of Applied Science and Computations J-ASC, 6(4), 3655-3660.
[7] S.Shivaprasad, M Sadanandam “Speech Based Query Searching Technique And Its Application In Library Management System”,International Journal Of Recent Technology and Engineering ISSN: 2277-3878, Volume-8 Issue-3, September 2019. DOI: 10.35940/ijrte.C4779.098319
[8] “OpenID Protocol.” [Online]. Available: http://openid.net/

[9] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.
[10] Vardhini, P. H., Babu, Y. M. M., & Veni, A. K. (2019). Industry Parameters Monitoring and Controlling system based on Embedded Web server. International Journal of Emerging Technologies and Innovative Research, 6(2), 80-84.
[11] A. Kehne, J. Schonwalder, and H. Langendorfer, “A nonce-based protocol for multiple authentications,” ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89, 1992.
[12] B. Neuman and S. Stubblebine, “A note on the use of timestamps as nonces,” Oper. Syst. Rev., vol. 27, no. 2, pp. 10–14, 1993.
[13] P. A. H. Vardhini, R. Pavan Kumar, T. Singh, H. V. R. Puliyala and S. Chamarthy, "Efficient IoT based Smart Home Assistance System with Electrical Control Unit," 2022 International Mobile and Embedded Technology Conference (MECON), Noida, India, 2022, pp. 475-479, doi: 10.1109/MECON53876.2022.9752276.
[14] J. Astorga, E. Jacob, M. Huarte, and M. Higuero, “Ladon : endto-end authorisation support for resource-deprived environments,” IET Infomration Security, vol. 6, no. 2, pp. 93– 101, 2012.
[15] Shivaprasad, S., Sadanandam, M. Identification of regional dialects of Telugu language using text independent speech processing models. Int J Speech Technol 23, 251–258 (2020). https://doi.org/10.1007/s10772-020-09678-y
[16] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, “SPINS: security protocols for sensor networks,” ACM Wireless Networking, vol. 8, no. 5, pp. 521–534, 2002.
[17] P. Kaijser, T. Parker, and D. Pinkas, “SESAME: The solution to security for open distributed systems,” Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.
[18] Vardhini, PA Harsha, and K. Murali Chandra Babu. "Home Automation System with Remote Android Smart Device for Physically Challenged." Journal of Applied Science and Computations 5.8 (2018): 967-972.
[19] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.
[20] D. Kothandaraman, N. Praveena, K. Varadarajkumar, B. Madhav Rao, Dharmesh Dhabliya, Shivaprasad Satla, Worku Abera, "[Retracted] Intelligent Forecasting of Air Quality and Pollution Prediction Using Machine Learning", Adsorption Science & Technology, vol. 2022, Article ID 5086622, 15 pages, 2022. https://doi.org/10.1155/2022/5086622
[21] Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070–1081, 2015.
[22] P.A. Harsha Vardhini and Kattula Deepthi, "FPGA based brain computer interface system", International journal of innovative research in science and engineering, January 2017.
[23] O. Althobaiti, M. Al-Rodhaan, and A. AlDhelaan, “An efficient biometric authentication protocol for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–13, 2013, Article ID 407971, http://dx.doi.org/ 10.1155/2013/407971.
[24] K. Xue, C. Ma, P. Hong, and R. Ding, “A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 316 – 323, 2013.
[25] P. A. H. Vardhini, V. K. R. Yasa and G. J. Raju, "Raspberry Pi Vehicle Gateway System with Image Processing based Authorization Detection using IoT," 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2021, pp. 1-5, doi: 10.1109/CONECCT52877.2021.9622528.
[26] M. Turkanovic, B. Brumen, and M. Holbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion,” Ad Hoc Networks, vol. 20, pp. 96 – 112, 2014.
[27] M. Park, H. Kim, and S. Lee, “Privacy Preserving Biometric-Based User Authentication Protocol Using Smart Cards,” in 17th International Conference on Computational Science and Engineering, Chengdu, China, 2014, pp. 1541–1544.
[28] P. K. Dhillon and S. Kalra, “A lightweight biometrics based remote user authentication scheme for IoT services,” Journal of Information Security and Applications, vol. 34, pp. 255 – 270, 2017.
[29] Satla, S., Manchala, S. (2021). Dialect identification in Telugu language speech utterance using modified features with deep neural network. Traitement du Signal, Vol. 38, No. 6, pp. 1793-1799. https://doi.org/10.18280/ts.380623