Key Management Protocol With Secure Communication For Cloud Computing

Mr. D.Sandeep
Department Of Information technology
MLR Institute of Technology

Ch.Sai Kiran
Department Of Information technology
MLR Institute of Technology

D.Hussain
Department Of InformationTechnology
MLR Institute of Technology

G.Anish
Department of Information Technology
MLR Institute of Technology

G.Shiva Kumar Yadav
Department of Information Technology
MLR Institute of Technology

***Abstract* - Cloud computing technology is growing faster hence many organizations have shifted to this platform. For protecting the privacy of communication and for accessing the services. maka protocols gains more attention . maka protocols lack dynamic revocation mechanism, which is used to prevent malicious users from being revoked immediately to overcome these shortcomings, we have proposed a dynamically revocable and provable maka protocolto accomplish dynamic user management . According to the results and the summary of the testing techniques our proposedsystem can meet various criteria and is also suited for multi server architecture too . However many of the Makaprotocols does not have revocation mechanism but our system has dynamic mechanism .**

Keywords : Cloud Computing , Key Management , Malicious Users , Dynamic Revocation

I.INTRODUCTION

Cloud computing has many features and it provides many services to its clients hence many organizations have been shifting to cloud nowadays .To provide security to its users and to protect the data ofcustomers from malicious users or attackers we need to have mutual authentication and key agreement protocols.One of the most important technical developments in recent years has been cloud computing, which provides users with access to a variety of services without requiring them to have local storage or processing power. Security is a big worry as cloud computing becomes more and moreprevalent in both personal and professional settings. To safeguard user data and uphold the integrity of cloud services, it is now morecrucial than ever to implement secure authentication and key agreement mechanisms. As they demand the participation of three entities for authentication— the user, the server, and a trusted third party—three-factor MAKA protocols are particularly successful in this regard. Despite thewidespread adoption of three-factor MAKA protocols, many of thecurrent protocols lack a formal security proof, which leads to a variety of attacks on related protocols. Furthermore, a lot of these protocols have significant communication and computation costs, which might be a concern for smart devices with limited resources . The proposed protocol makes use of Schnorr signatures to enable user dynamic administration. The performance analysis shows that the protocol is suitable for smart devices with limited computing resources, and the security analysis reveals that it can meet a variety of demands in multi-server scenarios.

II. Literature survey

[1] Even though a hacker can access the system's data on the user's communication with the system, the password authentication method known as "Password Authentication with Insecure Communication" is claimed to be secure. One-way password authentication is the method used in this situation

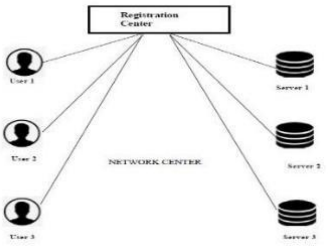
.[2] With significantly lower computing costs and greater functionality, they offered a user authentication and key agreement mechanism inthis project. A user must present his identification and the appropriate password to the server in order to log into it. The danger and expense of maintaining and safeguarding the table will then be introduced. [3] Design of a multiserver environment impersonation attack-resistant mutually authenticated key agreement mechanism. Recent developments in wireless technologies and their limitations are the main reasons for growth of these schemes. They asserted that their protocol is effective and resilient to well-known security vulnerabilities. Authentication utilising avispa and

ban logic. The protocol is susceptible to the most common types of attacks, including man-in-the-middle and impersonation attacks against users and servers.[4] Effective one-way hashing without a verification table for multi-server authentication.There are more and more systems available to support network users online. Password- based security techniques have been frequently utilised to authenticate remote users. These are simple to construct, but the server must retain a verification table for these techniques. Attackers may pose as legitimate users in order to steal the server's verification table. This study suggests a different smart card-based multi-server authentication method. One-way hashing technique for multi-server authentication.[5] These are Gaining popularity because they make services accessible while preserving the confidentiality of communications over open networks. Nevertheless, the majority of the three-factor MAKA protocols in use today lack a formal security proof, making them vulnerable to anumber of attacks. Its challenging to swiftly eliminate fraudulent users.[6] This study suggests a circle-based remote password authentication technique. For the authentication of the user and server in this approach, we employ certain straightforward tangent theorems, such as secant tangent theorem. The tangentpoints that are situated are connected to the circle which gives the security. Authentication Method Using the Circle and the Tangent Theorem. Mutual authentication cannot be used, and users cannot change their passwords. [7] A biometrics-based authentication and cryptanalysis is the advancement for multi- server environments .Wang recently proposed a key agreement three-factor authentication technique and asserted that their system was impervious to a number of well-known vulnerabilities. Sadly, this research shows that their protocol is still susceptible to server spoofing, user impersonation, and privileged insider attacks. Moreover, their approach is unable to guarantee perfect forward secrecy. They suggest a biometrics-basedkey agreement and authentication approach for multi-serversituations as a fix.Hash function and a fuzzy extractor powered by biometrics.The plan falls short of offering absolute forward secrecy. [8] Li et al. recently offered an enhancement for enhancing its security and supporting session key agreement. Moreover, these systems are once the template fi is compromised, it is unsafe to use their biometric authentication. using remote user authentication based on biometrics. Attackers may bombard the server with a huge number of unauthorised access request messages during a DoS assault. *[9]* Comments on a smart card-based fingerprint identification system for remote users.Remote user authentication is a crucial aspect of security in computing settings. One such method for reliable remote user authentication combines smart cards with fingerprint verification. In this study, we cryptanalyze Yoon and Yoo's effective fingerprint-based remote user authentication technique from 2005 and propose a new, more efficient, and secure scheme.The Yoon-Yoo technique, which uses two secret keys and fingerprint verification, is nevertheless susceptible to numerous impersonation attacks. *[10]* A general architecture for three-factor authentication that protects dispersed systems' privacy and security. Many services and resources within distributed systems need to be secured against unauthorised use. Themost popular technique for confirming a distant client's identity is remote authentication.The transition from two-factor authentication to three- factor authentication is suggested using a general and safe architecture.Additionally, we believe that our framework is of independent importance because it preserves a number of the two-factor authentication's practice friendly features

[11] For brittle communications, strong multifactor authentication.User authentication in large-scale applications typically requires network support from a remote central authentication server. However, because of natural disasters or different cyberattacks on communication systems, the authentication service can be sluggish or unavailable. Systems that require strong authentication in emergency scenarios have expressed grave worries about this. This study makes two contributions . When compared to another generic protocol in the literature, the new proposal provides the same function with noticeable computing and communication improvements. [12]. Many of these solutions, however, are not sufficiently secure. First, we demonstrate through the use of an impersonation attack that it is insecure for use in medical applications. Then, we suggest a fresh AA scheme for WBANs and demonstrate its provably secure nature. Our thorough investigation shows that our suggested AA approach not only fixes the security flaws in earlier plans but also has comparable client-side computation costs. [13] Research investigating the prospect of a tight security reduction in the random oracle model has focused heavily on the Schnorr signature scheme, the most successful signature scheme based on the discrete logarithm issue. [14] With the use of a key agreement protocol, two or more parties can share a key, which can subsequently be used to achieve particular cryptographic goals. A system of authentication also makes sure that only the right people receive the keys. [15] Under the random oracle paradigm, it has been shown that this system is resistant to ID assaults and existential forgeries on adaptively generated messages.

PROPOSED SYSTEM

Ourproposed system has higher execution efficiency.Our proposed system prevents the attackers from stealing the resources and stops the attackers from grabbing users data too.Our proposed system has dynamic revocation mechanism Our proposed system has good execution and the cost for the computation is comparatively low when compared with existing system.



The fig.1 shows the image of the system architecture.

There are four modules in the project

A. *Users Registration Phase:*

In the first module, we try to develop the Users registration module, where the users who need to access the cloud server needs to get registered and then only able to login and access or upload their cloud files. The user registration is done by collecting the details of user name, password and other basic details.

B. *QR Code Generation:*

In this module a QR code will be sent to the user who needs to login through our website and the QR code that is generated is unique.

C. *Malicious User Revocation:*

In this module, we developed the system to identify the malicious user and also provide the option of user revocation. We try to develop the system with certain threshold where the user triesto bypass the QR code with wrong QR Code or fake QR code, thenthe malicious user is identified and blocked by us.

D. *Cloud Server :*

In this module, we developed the Cloud server module,where we design the system to upload the files in a free cloud server named DriveHQ. In this module we can store huge amount of encrypted data.

IV..RESULT ANALYSIS

The two-factor MAKA protocol have the following flaws Security vulnerabilities, Incomplete basic functions and High cost. Our system has more advanced features. Our protocol has a very good execution power and high computational power. The existing systems fails to provide formal security which results in attacks .MAKA protocol does not have a dynamic revocationfunctionality which results to various attacks. The existing systemstakes more time for computation hence it has more computational costThe existing system has no dynamic revocation mechanismwhich is very useful for privacy of data.Existing system cannotprovide security to the users.The flaws of the existing system are

removed in the proposed system.The below are the various screenshots from our proposed system and for each screenshot that is present below a detailed explanation is given under the image itself

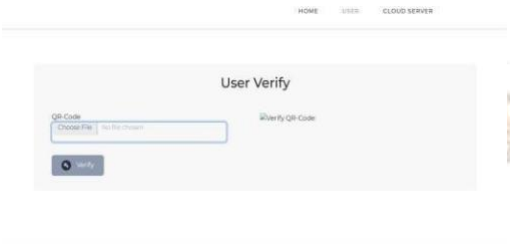


Fig 2: Verification of QR code.
fig 2.shows the QR code . Here the user can verify the qr code that he received to his gmail for the security purpose.

Fig 3: File upload.
fig.3 Users can upload their personal data in the form of files through our site

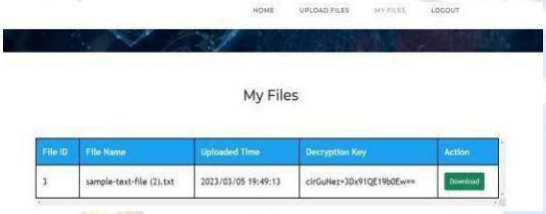


Fig 4:Downloading the file.
fig.4 users can see all their files by downloading their file using download button

Fig 5: Malicious user.
fig.5 users who are trying to enter to our site by giving fake credentials are treated as malicious users and they are blocked from entering to our site in the future too.

Fig 6: User analysis.
fig.6 users who are visiting our site are observed carefully and the graph is shown to identify the malicious users that have visited over the total number of users.

VI.CONCLUSION

To Resist The Exhaustion Of Password Attack On The Two-Factor Maka Protocols, A Large Number Of Three-Factor Maka Protocols Have Been Proposed. However, Almost All Three Factor Maka Protocols Don't Provide Formal Proofs And Dynamic User Management Mechanism. In Order To Achieve More Flexible User Management And Higher Security, This Paper Proposes A New Three-Factor Maka Protocol That Supports Dynamic Revocation And Provides Formal Proof. The Security Shows That Our Protocol Achieves The Security Properties Of Requirements From Multi-Server Environments.In the future, we want to enhance our system and make it more efficient in the next sprints and we like to improve the performance of our system too . In the future our project will provide security for 5G networks which enablenew cases for cloud computing . We are looking for differenttype of algorithms so that it boosts our project too.

XIII. REFERENCES

[1] L. Lamport, 1981Password Authentication with Insecure Communication.

[2]Wen-Shenq Juang, 2004. Efficient password authenticated key agreement using smart cards

[3] A. G. Reddy, E. J. Yoon, A. K. Das, V. Odelu, and K. Y. Yoo,2017Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multiserver environment.

[4] Jia-Lun Tsai,2008 Efficient multi-server authentication scheme based on one-way hash function without verification table.

[5] W. Tsaur, J. Li, and W. Lee, 2012 Secure Authenticated Key Management Protocol for Cloud Computing Environments: Design and Development.

[6] Y . Wang, J. Liu, F. Xiao, and J. Dan, 2009.Remote Login Password Authentication Scheme Using Tangent Theorem on Circle-A remote password authentication scheme

[7] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won,2012Cryptanalysis and improvement of biometrics-based authentication and key agreement scheme for multi-server environment.

[8] M. K. Khan and J. Zhang,2007Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards

[9] Youngkwon Lee and Taekyoung Kwon,2004Remarks on fingerprint-based remote user authentication scheme using smart cards.

[10] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng A generic framework for three-factor authentication: Preserving security and privacy in distributed systems.

[11] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, Robust multifactor authentication for fragile communicationsRobust multifactor authentication for fragile communications.

[12] D. He, S. Zeadally, N. Kumar, and J. Lee, Anonymous authentication for wireless bodyarea networks with provable security

[13] N. Fleischhacker, T. Jager, and D. Schroder On tight security proofs for schnorr signatures

[14] K. Y. Choi, J. Y. Hwang, D. H. Lee, and I. S. Seo, Id-based authenticated key agreement for low-power mobile devices

[15] J. C. Cha and J. H. Cheon, identity-based signature from gap diffie-hellman groups