ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

Proposing Genuine Protected Key Administration Procedure for Cloud Computing Backgrounds

[1] K. Venkateswarlu **[2]A. Anand**

[1] Assistant professor, Department of Master of Computer Applications, Narayana Engineering College, Gudur.

[2] PG Scholar, Department of Master of Computer Applications, Narayana Engineering College, Gudur.

Abstract: Earlier MAKA protocols are designed for single-server architecture. As Internet users grow exponentially, the number of cloud servers rendering different services has also grown significantly. For the single-server architecture, it is difficult for users to maintain a variety of passwords for each server. To improve user experience, many scholars propose more flexible MAKA protocols for multi-server environments. The works have shown that the password based MAKA protocols suffer from several attacks such as guessing password attack. To deal with these disadvantages, we intend a demonstrable lively revealed three-factor MAKA procedure that attains the consumer active organization using honor mark and afford official sanctuary evidence in the arbitrary oracle. Sanctuary scrutiny demonstrates that our procedure can gather a variety of anxiety in the multi-attendant environments.

Index Terms: Authentication, Bio ceramics, Protocols, Smart cards, Cloud Computing.

I. INTRODUCTION

IN the recent decade, cloud computing technology has been completely commercialized. It cannot only improve service efficiency but also reduce costs. More and more companies are putting their Services on the cloud platform for development, management and maintenance. This not only reduces the local maintenance burden for these enterprises, but also provides unified security and operation management for all services on the third-party cloud platform. Although third-party cloud platforms have more powerful technologies and more standard technical specifications to ensure that the servers run in a relatively secure environment, users and servers communicate in the public network.

Therefore, authentication and key agreement are critical for the communication security. The Use of mutual authentication and key agreement (MAKA) protocols not only prevent attackers from abusing server resources, but also prevent malicious trackers posing as the server to obtain the user's information. Therefore, the MAKA protocols have been extensively studied since Lamport Proposed a password-based authentication protocol. Earlier MAKA protocols are designed for single-server architecture. As Internet users grow exponentially, the number of cloud Servers rendering different services has also grown significantly.

The representation of Cloud service through its environment is as shown below. And it is the systematic procedural aspects of the cloud environment throughout the system analytics.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

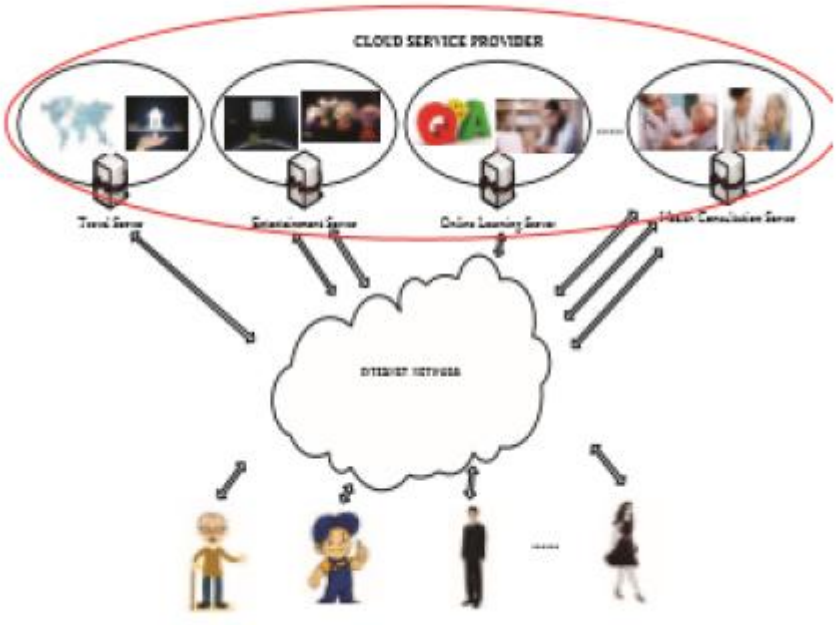


FIGURE.1: Cloud check background

II. RELATED WORK

In 2001, Li et al. introduced the concept of authentication protocol for multi-server environments and proposed the first password-based MAKA protocol using the neural network. Thanks to the complicated neural network. To improve efficiency, a MAKA protocol for multi-server architectures by using hashes functions and symmetric key cryptosystems. In the same year, protocol is flawed in terms of efficiency. They proposed a more efficient MAKA scheme for multi-server environments. To provide user anonymity, Das et al. proposed the first dynamic two-factor authentication scheme which uses dynamic pseudo-identities instead of a user's true identity.

Disadvantages of this work follows the protocol isn't suitable for smart devices with limited computing power, reduced efficiency. However, in their protocol RC shares system private key with all servers.

III. PROPOSED WORK

We design a three-factor MAKA protocol which implements three-factor security. And we show that the proposed protocol can meet the demands of multi-server architectures such as anonymity, non-traceability, resistance password guessing attack and smart card extraction attack, and so on. In our protocol, users can be dynamically revoked to promptly prevent

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

attacks from malicious users. Without a dynamic revocation mechanism, RC can't punish malicious users in a timely manner. This may result in such malicious users still active in the network to communicate with other servers. Advantages of this proposed work are: Our scheme achieves the user's dynamic management. Our protocol has good execution efficiency.

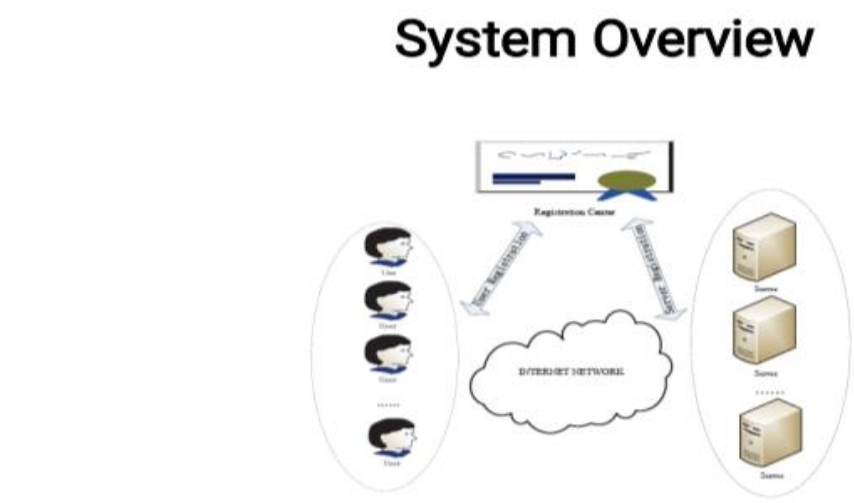


FIGURE.2: system overview

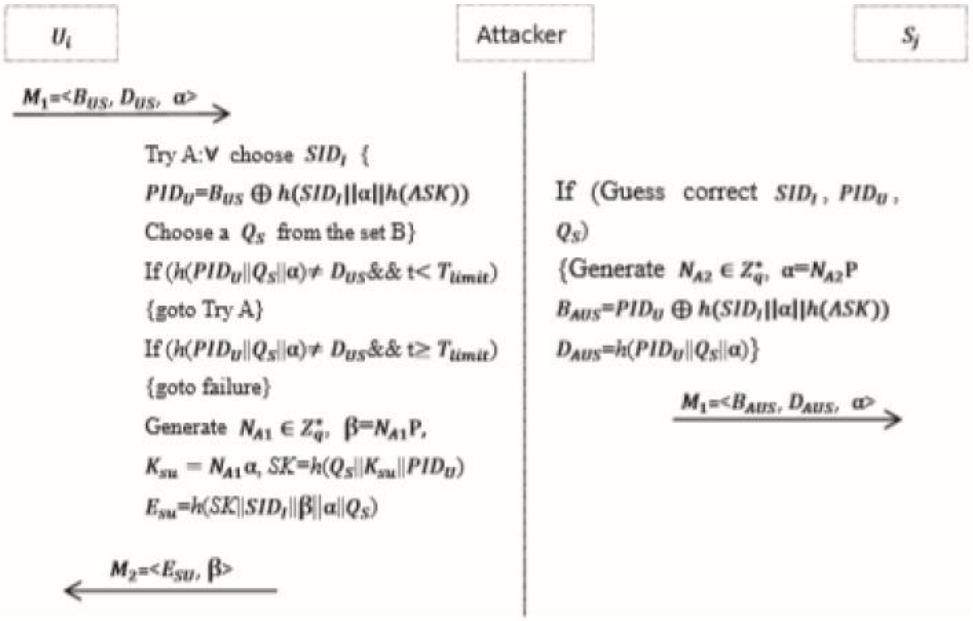
The above fig.2...represents the system over view of the cloud server management and its environment.

This proposed work follows the following algorithm:

Man in the Middle Attack algorithm: The attacker first uses the information extracted from the smartcard to complete the server's impersonation attack. At the same time, he used his successful guess of the information SIDI, PIDU and QS impersonation the user to complete. The authentication and key agreement with the real server Si. After that, the attacker can negotiate Session key with the server and the user respectively to seal communications between Ui and Sj.

Algorithm is as follows:

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020



PERFORMANCEANALYSIS:

In this part, we will examine the presentation of the projected 3DRMAKA procedure and the connected contrast system in terms of calculation time, announcement costs. As well as the necessary number of round-trip times (RTT). Depending on the system hold up the RTT time can develop into the leading price for a procedure. A new broad contrast can be get hold of to attain a dependable safety point of 1024-bits RSA algorithm.

IV. EXPERIMENT RESULTS

Our procedure has an important compensation intermsof customer computing instance and entire fee time. This allocate sour procedure to be organized one legant strategy that hasincompletecomputingauthority.Advancetheuniversalityoftheprocedure.Onthefurtherhand,thecomputationalcostofourprocedureontheattendantsideisslightlyseniorthanthatofthecorresponding comparisonschemesbutourschemeattainhighersafetyandmorecomprehensivefunctionality, soitbringsacertainservercomputingtimeascension.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

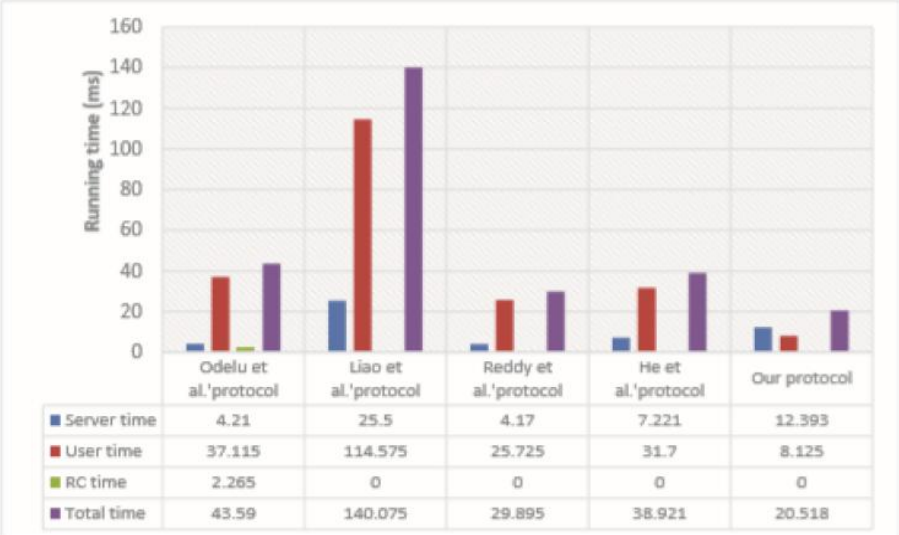
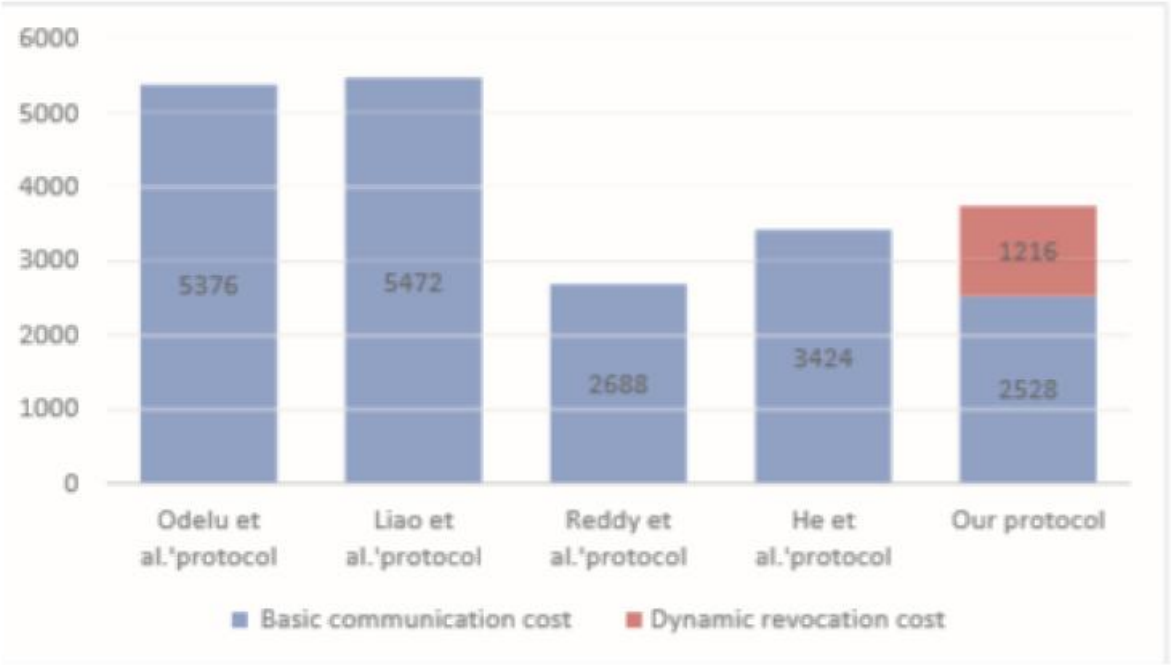


Figure.3: Graphical representation of Server time, user time, RC time.

The necessary numberofround-triptimesinthe procedure is as well as chief factoraffectingthe efficiencyoftheimplementation.Fewerthenumberofcommunicationstendtobemore efficient. Especiallyincomplex system environments.



In Odile et al.' protocol, since each authentication requires RC participation, it needs two extra connections than other procedure. In multifaceted system surroundings, numerous communications result in a significant increase in communication time. In the route of a complete contrast of implementation efficiencies, we terminate that our protocol has advantages over the pertinent protocols in conditions of computation time and statement cost.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

V. CONCLUSION

To oppose the tiredness of secret code assault on the two-factor MAKA procedures, several three-factor MAKA procedures have been projected. However, almost all three factor MAKA procedures don't afford official evidence and dynamic user management mechanism. In sort OF achieving more flexible user management and higher security, this paper proposes a new three-factor MAKA procedure that Supports dynamic revocation and provides formal proof. The security shows that our protocol achieves the security properties of requirements from multi-server environments. On the other hand, Through the comprehensive analysis of performance, our protocol doesn't sacrifice efficiency while Improving the function. On the contrary, the proposed protocol has great advantages interms of the Total computation time.

REFERENCES

1. L.Lamport,"Password authentication within secure communication," Communications of the ACM, vol.24,no.11,pp.770–772,1981.
2. X. Huang, Y.Xiang,A.Chunk,J.Zhou,andR.H.Deng,"Agenericframeworkforthree-factor authentication: Preserving security and privacy in distributed systems," IEEE Transactions on Parallel and Distributed Systems,vol.22,no.8,pp.1390–1397,2011.
3. X.Huang,Y.Xiang,E.Bettino,J.Zhou,andL.Xu,"Robustmultifactorauthenticationforfragilecommunications,"IEEETransactionsonDependableandSecureComputing,vol.11,no.6,pp.568581,2014.[4]D.He,S.Feudally,N.Kumar,andJ.Lee,"Anonymousauthenticationforwirelessbodyareanetworkswithprovablesecurity,"IEEESystemsJournal,pp.1–12,2016.
4. L.Li,L.Lin,andM.Hwang,"Aremotepasswordauthenticationschemeformultimergerarchitectureusingneuralnetworks,"IEEETransactionsonNeuralNetworks,vol.12,no.6,pp.1498–1504,2001.
5. W.Juang,"Efficientmultiserverpasswordauthenticatedkeyagreementusingsmartcards," IEEETransactionsonConsumerElectronics,vol.50,no.1,pp.251–255,2004.
6. C.C.ChangandJ.S.Lee,"Anefficientandsecuremultiserverpasswordauthenticationschemeusingsmartcards,"inInternationalConferenceonCyberworlds,2004,pp.417–422.
7. J.L.Tsai,"Efficientmultiserverauthenticationschemebasedononewayhashfunctionwithoutverificationtable,"Computers&Security,vol.27,no.3C4,pp.115–121,2008.
8. Viswanth, V. S., Ramanujam, R., and Rajyalakshmi, G, "Application of MQL for Developing Sustainable EDM and Process Parameter Optimization using ANN and GRA Method". International Journal of Business Excellence, vol. 19, No. 1, 58-62, 2019.
9. Rajasekar, P. and Mangalam, D. (2016) Efficient FPGA implementation of AES 128 bit for IEEE 802.16e mobile WiMax standards. Circuits and Systems, 7, 371-380. doi: 10.4236/cs.2016.74032.
10. W.Tsaur,J.Li,andW.Lee,"Anefficientandsecuremultiserverauthenticationschemewithkeyagreement,"JournalofSystemsandSoftware,vol.85,no.4,pp.876–882,2012.
11. Viswanth, V. S., Ramanujam, R., and Rajyalakshmi, G, "A Novel MCDM Approach for Process Parameters Optimization in Eco-Friendly EDM of AISI 2507 Super Duplex Stainless Steel". Journal of Advanced Research in Dynamical and Control Systems - JARDCS, vol. 10, No. 7, 54-64, 2018.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

12. Y.LiaoandC.Hsiao,"Anovelmultiserverremoteuserauthenticationschemeusingselfcertifiedpublickeysformobileclients,"FutureGenerationComputerSystems,vol.29,no.3,pp.886–900,2013.

Author's profile:

K.Venkateswarlu has received his M.Tech from P.B.R Vits college-Kavali In (2011-2014).He is dedicated to teaching field for last 5 years. At present he is working as Assistant professor for the Department of MCA in Narayana Engineering College, Gudur, Nellore.

A.Anand has received his degree B.Sc Computers (2014-2017)from Dr.C.V.Raman degree College- Nayudupeta, which is Affiliated to VSU, Nellore. And now perusing MCA (2017-2020) at Narayana Engineering College–Gudur which is affiliated to JNTUA.

