Mechanism for Cloud Computing Environment's Reliable Authenticated Token Handling

GiriBabu Sadineni[1], Janardhan Reddy D[2], Adusumalli Niharika[3], Kommu Tejaswini[4], Golla Vandana[5], and Padmini Biyyapu[6]

[1]Associate Professor, Department of Computer Science & Engineering, PACE Institute of Technology & Sciences, Ongole, Andhra Pradesh, India
[2]Assistant Professor, Department of Computer Science & Engineering, PACE Institute of Technology & Sciences, Ongole, Andhra Pradesh, India
[3,4,5,6] UG Student, Department of Computer Science & Engineering, PACE Institute of Technology & Sciences, Ongole, Andhra Pradesh, India

ABSTRACT- Cloud computing (CC) has matured in terms of dependability and effectiveness, which has led to the migration of many applications to the cloud. Three-factor Multilateral Authenticity and Knowledge Acceptance (MAKA) mechanisms for multi-server systems are gaining a lot of interest for their convenience and security. Although there are many extant three-factor MAKA protocols, none of them give a rigorous secure guarantee, making them vulnerable to numerous assaults on other procedures in the chain. And most three-factor MAKA mechanisms lack adaptive cancellation mechanisms, preventing malevolent users from being quickly removed. We present a three-factor MAKA protocol with a proven adaptive reversible evidence in the arbitrary source to overcome these issues. This method uses Schnorr identities to enable vibrant administration by the client. In multi-server setups, our procedure is capable of meeting a wide range of requirements. For intelligent systems with low processing power, the suggested method is a viable option. The entire computation code demonstrates the system's viability.

KEYWORDS- Mechanisms, Adaptive devices, intelligent system, Computation, Acceptance.

I. INTRODUCTION

In the last century, CC has become a fully mainstream innovation. It has the potential to both increase operation quality and save expenses [1]. More and more businesses are placing their construction, administration, and support efforts in the cloud. Fig. 1 illustrates how the third-party cloud infrastructure offers integrated safety and operational administration for all applications on the infrastructure, reducing the load on these organizations [2]. Consumers and computers connect in the public internet even though third-party cloud systems have more advanced hardware and more standardized operational requirements to guarantee the computers function in a reasonably safe environment [3]. A secure telecommunication system relies heavily on identification and key negotiation. Aside from preventing virtual servers from being misused, MAKA standards also prohibit dangerous hackers from acting as the service in order to collect user data. Although Lamport suggested a password-based signature scheme [4], the MAKA technologies have been intensively investigated. For a sole player structure, the older MAKA technologies [5] were created.

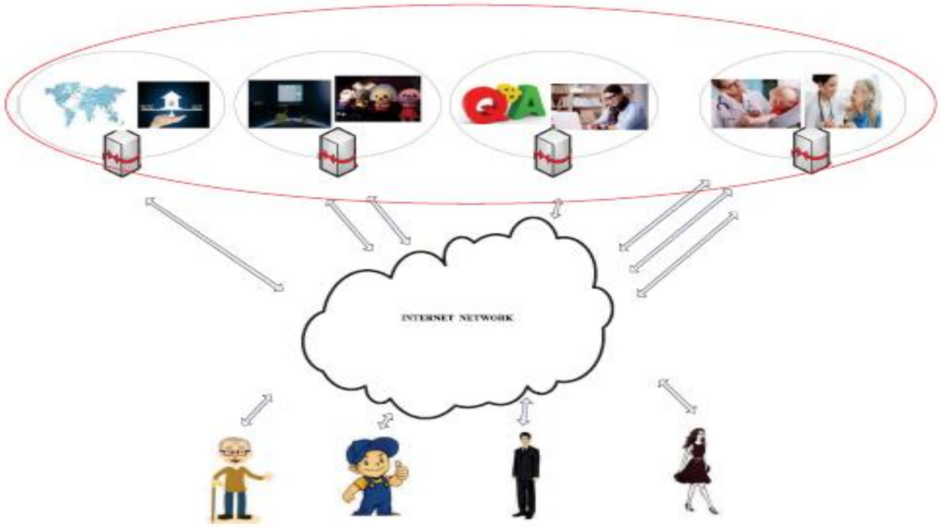


Figure 1: Cloud Operational Settings

II. RELATED WORKS

Increases in the number of cloud computers providing various applications have kept pace with the rise in Internet consumers [12-15]. Managing several credentials for every site in a solitary design is tough for customers. Several researchers have proposed more adaptable MAKA protocols for multi-server situations in order to enhance customer journey [16-20]. Using the internet product's integrated monitoring tools, such conventions may be easily implemented [21-28]. There is no requirement for customers or virtual machines to join at the enrollment centre (RC) in the methodology for multi-server topologies as depicted in Fig. 2. A multi-server identification mechanism was initially suggested in 2001 by Li et al. [5] who used a neural network (NN) and a passcode-based MAKA mechanism. Li et al protocol .'s is not suited for intelligent gadgets with low computational capacity because of the complex NN. By utilising checksums and key generation advanced encryption standard, Juang [6] created an efficient MAKA algorithm for multi network servers. A year later, Chang et al. [7] made the same observation about Juang's blockchain's effectiveness. For multi-server situations, they came up with a more economical MAKA system. RC, on the other hand, distributes the network secret key with all clients in their communication. As a consequence, there will be a plethora of system weaknesses. Improved protection has also been suggested for existing MAKA technologies [8], [9] via the use of block ciphers and geometric encryption algorithms." An identification mechanism for smartphone consumers that uses self-certified shared key and works across several servers was presented by Liao et al. [10] in 2013. A global data packet isn't established, and the transmission costs are prohibitive.

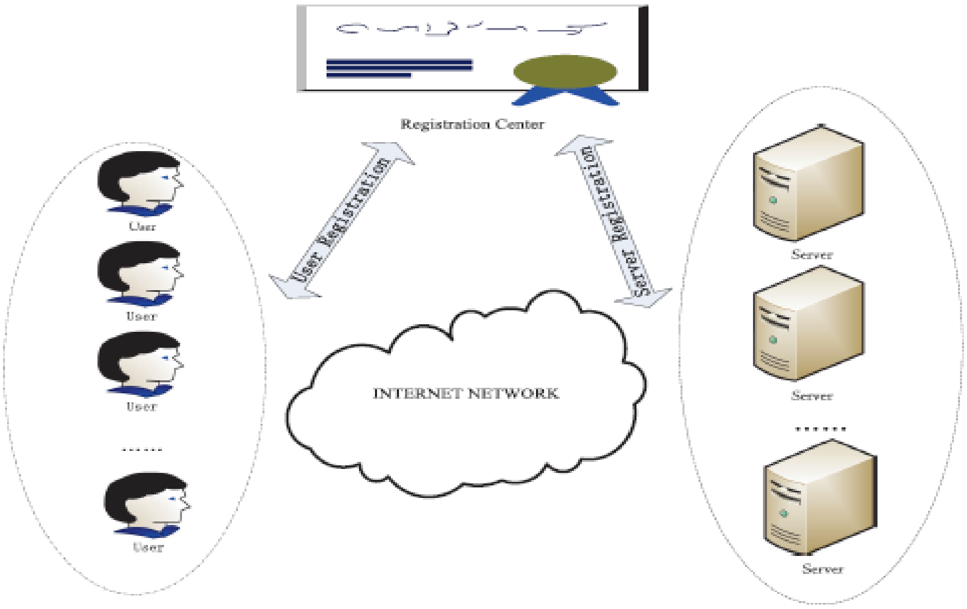
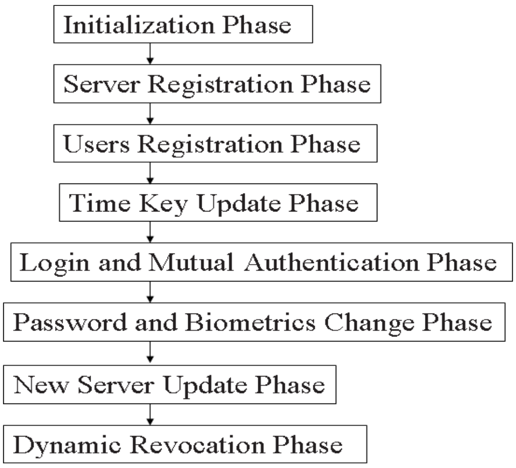


Figure 2: Protocol-Based Multi-Service Frameworks

III. PROPOSED METHODOLOGY

The MAKA technique is discussed in detail in this chapter. Figure 3 depicts the eight steps of the suggested technique. The RC initializes the network secret key and platform settings during enrollment. An approved internet connection must be registered in this step of the Server Enrollment process. To utilize the functions of a partner, a newbie should enroll with the RC during the User Enrollment stage in multi-server systems. To proactively control customers, the Time Key Upgrade Stage regularly changes the clock code for registered users. To begin, the user must enter their credentials for their contactless card. It is then possible to establish a shared key with the service once the visitor has authenticated themselves. Credentials and demographics may be changed without RC in the Password and Biometrics Alteration Stage, which relieves the client of the RC load. In the New Server Update Phase, a fresh service may connect to the system without requiring RC data to be entered. Having an effective cancellation process is an absolute need in the real world. Both avoiding and enhancing the effectiveness of RC administration may benefit from this. Reactive repudiation is now enabled by this method in two ways, including the cancellation of fraudulent accounts and user-initiated renunciation applications.



Initialization Phase

Server Registration Phase

Users Registration Phase

Time Key Update Phase

Login and Mutual Authentication Phase

Password and Biometrics Change Phase

New Server Update Phase

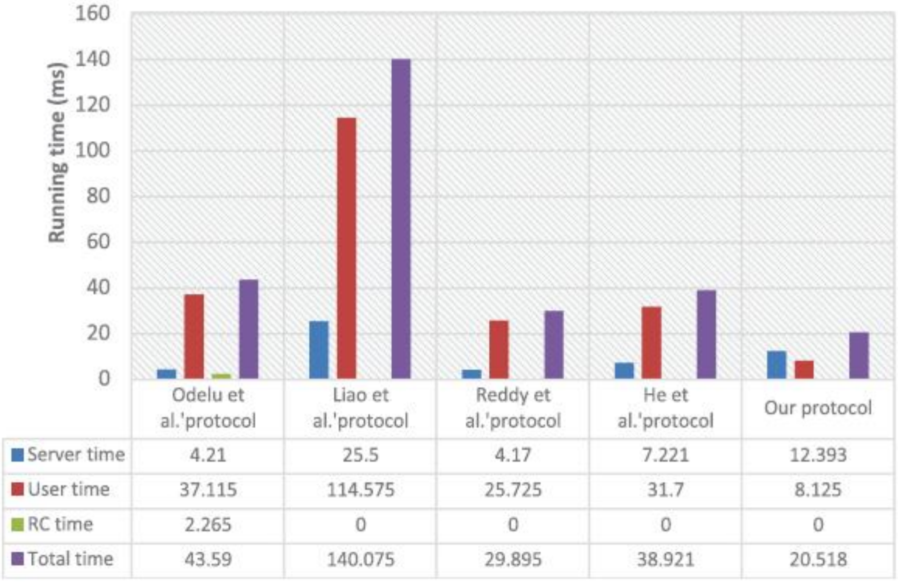
Dynamic Revocation Phase

Figure 3: Proposed Methodology

IV. RESULTS AND DISCUSSION

Analysis of suggested MAKA technique and associated comparability techniques in terms of computing cost will be carried out in this part. The Round Trip Times may become the primary expense of a communication based on the connection latency. Research [11] provides a much more thorough assessment. We use a Tate coupling and a super-singular curvature to reliably secure the RSA method at a 1024-bit scale. The quantity of procedures required to accomplish reciprocal verification and secret negotiation in our system and the [28] systems is summarized in Table 1 and Fig. 4. If RC and server both have the equal amount of processing capacity, we may proceed. Fig. 4 demonstrates that our approach has a considerable benefit in terms of the amount of consumer processing effort and overall cost duration. As a result, our method may be used on low-powered intelligent homes. The procedure should be made more ubiquitous. In contrast, the server-side processing burden of our approach is greater than that of the similar comparative systems [23, 28]. However, our system delivers stronger safety and more extensive capabilities, therefore it provides a considerable service processing cost ascent. Every identification and secret arrangement in [22] system requires RC's assistance, which puts RC under a lot of strain from the channel's many demands for this assistance. Additionally, the suggested method provides benefits when it comes to computing costs.

.



	Odelu et al.'protocol	Liao et al.'protocol	Reddy et al.'protocol	He et al.'protocol	Our protocol
🟦 Server time	4.21	25.5	4.17	7.221	12.393
🟥 User time	37.115	114.575	25.725	31.7	8.125
🟩 RC time	2.265	0	0	0	0
🟪 Total time	43.59	140.075	29.895	38.921	20.518

Figure 4: Cost Evaluations in Calculation

We begin by defining the essential terms:
T_{BP} denotes Bilinear-pairing time.
T_H: Hash time
T_{exp}: Exponentiation activity time.
T_A: addition activity time.
T_M: Multiplication activity time.
T_{SM}: Scalar multiplication activity time.
T_{ED} denotes encipher/ decipher time.
N_R denotes Not Required

Table 1: The Number of Operations

	[28]	[10]	[23]	[22]	Proposed
Client	$3T_M$ + $7T_{BP}$ +T_{ED}	T_{exp} + $7T_{SM}$ + T_A +$5T_H$	$9T_H$ + $2T_{SM}$	$4T_{ED}$ + $8T_{BP}$	$9T_H + 2T_{exp}$
Server	$7T_{SM}$ + $4T_A$	$8T_M + 2T_{exp}$	$7T_{SM}$ + $4T_M$	$3T_A$ + $2T_M$	$2T_{SM} + 4T_A$
RC	$5T_{exp}$ + $3T_{BP}$	N_R	N_R	N_R	N_R

V. CONCLUSION AND FUTURE SCOPE

Many three-step MAKA methods have been developed to combat the credential depletion assault on two-step MAKA systems. Most three-step MAKA mechanisms lack explicit justifications and account control mechanisms. This article presents a novel three-step MAKA mechanism that enables adaptive cancellation and gives rigorous evidence in order to offer more versatile account administration and improved protection. This proves that our approach meets the needs of multi-server setups in terms of safety and protection. In contrast to the other protocols, ours doesn't undergo degradation while enhancing the functionality. As a matter of fact, in terms of overall computing time, the suggested methodology offers a number of benefits.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] L. Lamport, “Password authentication with insecure communication,” Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.

[2] 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," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 8, pp. 1390–1397, Aug. 2011.

[3] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust multifactor authentication for fragile communications," IEEE Trans. Dependable Secure Comput., vol. 11, no. 6, pp. 568–581,Nov./Dec. 2014.

[4] D. He, S. Zeadally, N. Kumar, and J. Lee, "Anonymous authentication for wireless body area networks with provable security," IEEE Syst. J., vol. 22, pp. 1–12, 2016.

[5] L. Li, L. Lin, and M. Hwang, "A remote password authentication scheme for multiserver architecture using neural networks," IEEE Trans. Neural Netw., vol. 12, no. 6, pp. 1498–1504, Nov. 2001.

[6] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," IEEE Trans. Consumer Electron., vol. 50, no. 1, pp. 251–255, Feb. 2004.

[7] C. C. Chang and J. S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards," in Proc. Int. Conf. Cyberworlds, 2004, pp. 417–422.

[8] J.-L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table," Comput. Secur., vol. 27, no. 3C4, pp. 115–121, 2008.

[9] W. Tsaur, J. Li, and W. Lee, "An efficient and secure multi-server authentication scheme with key agreement," J. Syst. Softw., vol. 85, no. 4, pp. 876–882, 2012.

[10] Y. Liao and C. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," Future Generation Comput. Syst., vol. 29, no. 3, pp. 886–900, 2013.

[11] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Trans. Comput., vol. 51, no. 5, pp. 541–552, May 2002.

[12] D. Wang and P. Wang, Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards. New York, NY, USA: Springer International Publishing, 2015.

[13] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," Electron. Lett., vol. 38, no. 12, pp. 554–555, 2002.

[14] C. Lin and Y. Lai, "A flexible biometrics remote user authentication scheme," Comput. Standards Interfaces, vol. 27, no. 1, pp. 19–23, 2004.

[15] C. Chang and I. Lin, "Remarks on fingerprint-based remote user authentication scheme using smart cards," Operating Syst. Rev., vol. 38, no. 4, pp. 91–96, 2004.

[16] H. Kim, S. Lee, and K. Yoo, "Id-based password authentication scheme using smart cards and fingerprints," Operating Syst. Rev., vol. 37, no. 4, pp. 32–41, 2003.

[17] M. Scott, "Cryptanalysis of an id-based password authentication scheme using smart cards and fingerprints," Operating Syst. Rev., vol. 38, no. 2, pp. 73–75, 2004.

[18] M. K. Khan and J. Zhang, "Improving the security of 'a flexible biometrics remote user authentication scheme'," Comput. Standards Interfaces, vol. 29, no. 1, pp. 82–85, 2007.

[19] E. Yoon and K. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," J. Supercomputing, vol. 63, no. 1, pp. 235–255, 2013.

[20] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme," in Proc. Int. Conf. Comput. Sci. ppl., 2012, pp. 391–406.

[21] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," IEEE Syst. J., vol. 9, no. 3, pp. 816–823, Sep. 2015.

[22] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

[23] A. G. Reddy, E. J. Yoon, A. K. Das, V. Odelu, and K. Y. Yoo, "Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment," IEEE Access, vol. 5, pp. 3622–3639, Feb. 2017.

[24] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic id-based remote user authentication scheme," IEEE Trans. Consumer Electron., vol. 50, no. 2, pp. 629–631, May 2004.

[25] Y. Wang, J. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic id-based remote user authentication scheme," Comput. Commun., vol. 32, no. 4, pp. 583–585, 2009.

[26] K. Yeh, C. Su, N. Lo, Y. Li, and Y. Hung, "Two robust remote user authentication protocols using smart cards," J. Syst. Softw., vol. 83, no. 12, pp. 2556–2565, 2010.

[27] F. Wen and X. Li, "An improved dynamic id-based remote user authentication with key agreement scheme," Comput. Electr. Eng., vol. 38, no. 2, pp. 381–387, 2012.

[28] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 9, pp. 2052–2064, Sep. 2016.