TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 10493 - 10498

Design of Efficient Multi-Server Password Authenticated Key Management Protocol for Cloud Computing Environments

[1]V. Manjusha, [2]A. Gayathri, [3]K. Logu

[1]UG Scholar, Dept. of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India

[2]Associate Professor, Dept. of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India

[3]Assistant Professor, Dept. of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India

[1]manjuvadlamudi690@gmail.com, [2]gayathribala.sse@saveetha.com, [3]klogu.sse@saveetha.com

Article Info
Volume 82
Page Number: 10493 - 10498
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 19 February 2020*

Abstract

With the improvement of disseminated registering advancement to the extent trustworthiness and capability, incalculable organizations have moved to the cloud arrange. To worthwhile access to the organizations and guarantee the security of correspondence in the open framework, three-factor Mutual Authentication (MA) and Key Agreement (KA) shows for multi-server structures increment wide thought. In any case, most of the present three-factor MAKA shows don't give a formal security affirmation achieving various attacks on the related shows, or they have high estimation and correspondence costs. In addition, most of the three-factor MAKA shows haven't a dynamic denial segment (DDS), which prompts malicious customers cannot be speedily disavowed. To address these detriments, we propose a provable one of a kind revocable three-factor MAKA show that achieves the customer dynamic organization using Schnorr marks and gives a formal security proof in the subjective prophet. Security assessment exhibits that our show can fulfill various needs in the multi-server circumstances. Execution assessment demonstrates that the proposed arrangement is fitting for enrolling resource obliged smart contraptions. The full type of the reenactment execution shows the likelihood of the show.

Keywords: *Authentication, Cloud Computing, Dynamic denial segment, Password*

1. Introduction

In the progressing decade, dispersed processing development has been completely advanced. It cannot simply improve organization capability yet moreover decrease costs. A regularly expanding number of associations are putting their organizations on the cloud arrange for development, the administrators and upkeep. This not simply decreases the area upkeep inconvenience for these undertakings, yet what's more gives bound together security and action the officials for all organizations on the untouchable cloud arrange. Yet pariah cloud stages have even more prevailing developments and continuously standard specific points of interest to ensure that the servers continue running in a reasonably secure condition, customers and servers grant in the open framework. Along these lines, confirmation and key comprehension are essential for the correspondence security. The use of regular affirmation and key understanding shows not simply shield aggressors from abusing server resources, yet also foresee malicious aggressors acting like the server to get the customer's information.

2. Literature Survey

Conventions of client validation can guarantee the security of information transmission and clients' correspondence over shaky systems. Among different verified instruments run presently, the secret key based client confirmation, in light of its effectiveness, is the most generally utilized in various zones, for example, PC systems, remote systems, remote login, activity frameworks, and database the executive’s frameworks. Indeed, even as secret word is enriched with the property of basic and human critical, for which causes such an assault of savage power, for instance, the past works regularly endure disconnected secret phrase speculating assault. Subsequently, an ameliorative secret key based confirmation plot is proposed in this paper, accomplishing to oppose disconnected secret key speculating assaults, replay assaults, on-line secret key speculating assaults, and ID-burglary assaults. Considering security, the proposed plan is given acceptable practicability, significantly over unreliable system.

In huge scale frameworks, client confirmation for the most part needs the help from a remote focal validation server by means of systems. The verification administration anyway could be moderate or inaccessible because of catastrophic events or different digital assaults on correspondence channels. This has brought genuine worries up in frameworks which need vigorous validation in crisis circumstances. The commitment of this paper is two-overlap. In a moderate association circumstance, we present a protected conventional multifaceted verification convention to accelerate the entire validation process. Contrasted and another nonexclusive convention in the writing, the new proposition furnishes a similar capacity with huge enhancements in calculation and correspondence. Another validation component, which we name remain solitary confirmation, can verify clients when the association with the focal server is down. We examine a few issues in remain solitary verification and tell the best way to include it multifaceted validation conventions in an effective and nonexclusive manner.

3. Proposed System Design

Because of the fast improvement of science and methods, individuals can remotely get to PCs over the systems. Along these lines, client validation and key understanding become increasingly more imperative to guarantee the legitimateness of the client and the security of later interchanges, separately. Since the quantity of servers giving the offices to the client is generally more than one, the idea of multi-server conventions is presented.

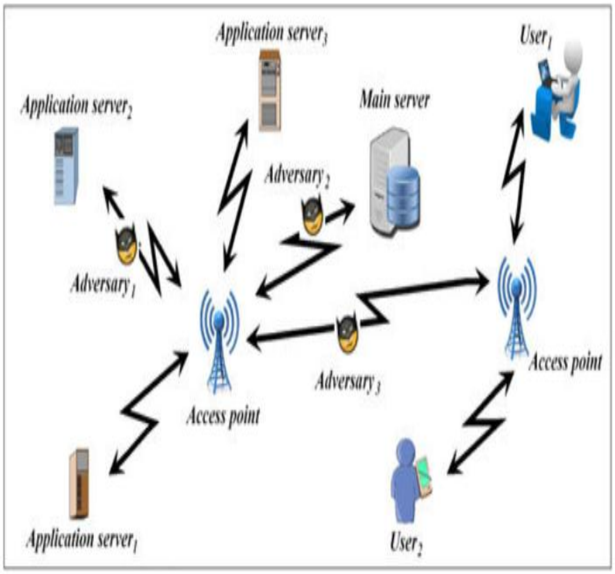


Figure 1.1: Multi Server Communications

Fig 1.1 shows the multiserver should communicate Access Point (AP) through the users.

On the Internet, every server typically gives different administrations, and each assistance gave by the server may not be gotten to by the client. Consequently, get to control is required in the multi-administration condition. In 2004, Juang proposed a multi-server validation plot with key understanding. Be that as it may, get to control isn't considered in Juang's proposed plan, so we propose an effective multi-server secret key validated key understanding plan with get to control in this article.

The significant job for the client is to move login window to client window. This module has made for the security reason. In this login page we need to enter login client id and secret key. It will check username and secret phrase is coordinate or not (substantial client id and legitimate secret word).

Patient Getting Admitted In Hospital

In this module, the client will get conceded in the medical clinic 1 because of some sickness issue. After that the client data with respect to the treatment accomplished for that ailment and the tablets given everything will be put away in the database.

Already Disease Attacked

In this module, the specialist will ask the patient whether the illness is already attack or not. Whenever assaulted, the specialist will ask in what emergency clinic you got conceded with this disorder.

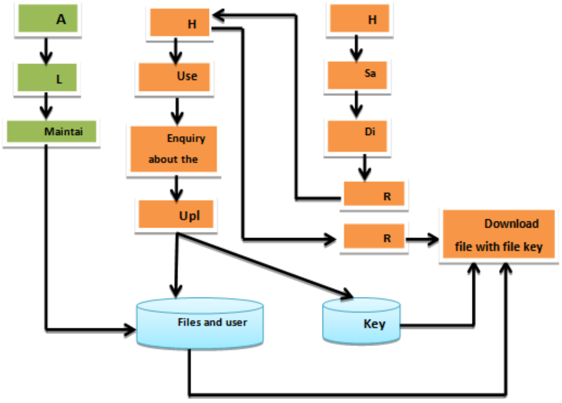


Figure 1.2: Flow Architecture for Key Management

Request Patient Data from Hosp1 to Hosp2

In this module, in the wake of realizing that the patient has conceded beforehand in emergency clinic 1 the specialist will demand the patient treatment information and the tablets given from the medical clinic 2.

Response from Hosp2

In this module, in the wake of mentioning the patient information from medical clinic 1, the emergency clinic 2 will be tolerating the solicitation from the clinic 1 to realize the treatment given to the patient.

Admin Maintaining the File

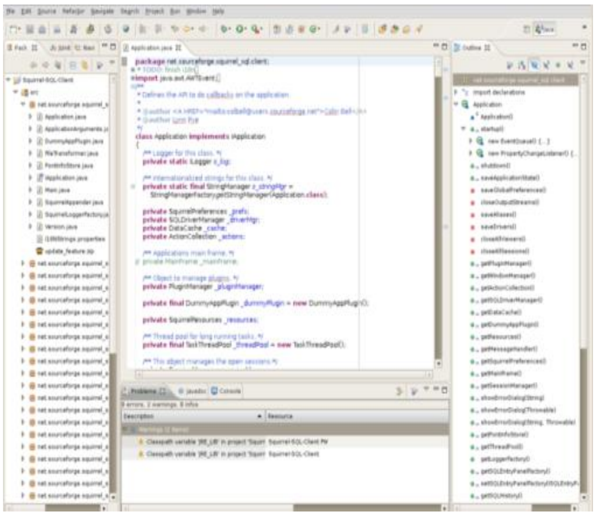
In this module, the administrator will keep up the database the patient subtleties and the medical clinic subtleties.

Download the File Using the Keys

In this module, the specialist from the emergency clinic 1 will have the option to download the document utilizing record key and the csp key gave to them and afterward the treatment will be begun for the patient.

A successful multifaceted verification instruments that utilizations vigorous combiners of quick hash capacities. Each hash work is determined dependent on preset key and the possibility of one-time secret phrase (OTP). Likewise, the hash work is applied to both the key and the message. Also, it proposes a period upgraded based one-time secret phrase (TEOTP) hash work that is executed in the base station/sink and IoT gadget to determine the issue of time synchronization in time sensitive one-time secret word (TOTP).

4. Simulation and Analysis



```
package net.sourceforge.squirrel_sql.client;
+ * TODO: finish ...
+import java.awt.AWTEvent;
/**
 * Defines the API to do callbacks on the application.
 *
 * @author <A HREF="mailto:colbell@users.sourceforge.net">Colin Bell</A>
 * @author Lynn Pye
 */
class Application implements IApplication
{
	/** Logger for this class. */
	private static ILogger s_log;

	/** Internationalized strings for this class. */
	private static final StringManager s_stringMgr =
		StringManagerFactory.getStringManager(Application.class);

	private SquirrelPreferences _prefs;
	private SQLDriverManager _driverMgr;
	private DataCache _cache;
	private ActionCollection _actions;

	/** Applications main frame. */
//	private MainFrame _mainFrame;

	/** Object to manage plugins. */
	private PluginManager _pluginManager;

	private final DummyAppPlugin _dummyPlugin = new DummyAppPlugin();

	private SquirrelResources _resources;

	/** Thread pool for long running tasks. */
	private final TaskThreadPool _threadPool = new TaskThreadPool();

	/** This object manages the open sessions. */
```

```
9 errors, 2 warnings, 8 infos
Description                                      Resource
Classpath variable 'JRE_LIB' in project 'Squirr  SquirrelSQL-Client Pl
Classpath variable 'JRE_LIB' in project 'Squirr  SquirrelSQL-Client
```

Figure 2.1: Eclipse IDE

Fig 2.1 to shows Eclipse IDE for connecting Amazon AWS cloud service to create a bucket without any interruption.

Figure 2.2: AWS Infrastructure

Fig 2.2 shows the AWS Global Infrastructure is designed and built to deliver the most flexible, reliable, scalable, and secure cloud data management system.

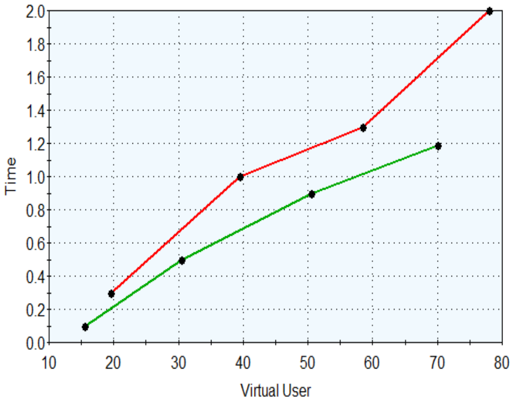


Figure 2.3: Average Collection Time

Fig 2.3 shows the larger response times seen below, but they correspond mainly with commercial spikes.

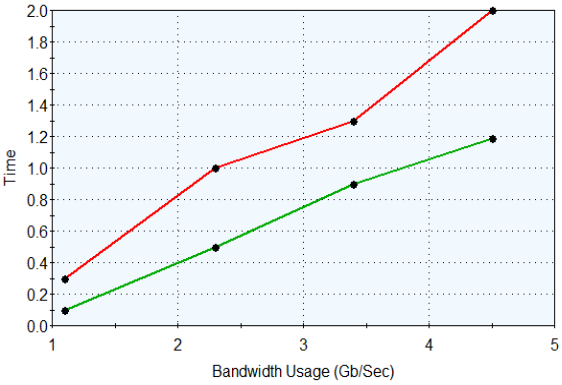


Figure 2.4: Bandwidth Usage

Fig 2.4 Bandwidth is a potential bottleneck that can become maxed out very quickly. This especially true if an application has large downloads, lots of page resources, or does not properly utilize aCDN.

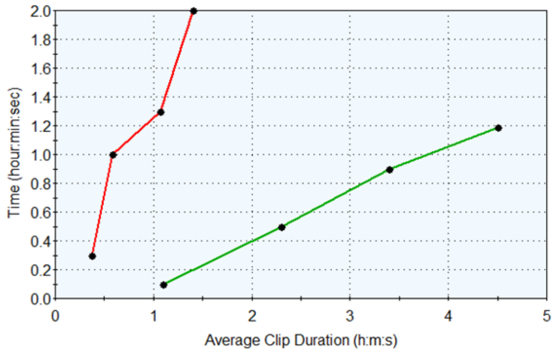


Figure 2.5: Average Clip Duration

Fig 2.5 shows the test execution itself incorporated spikes in traffic, which you can see accurately reflected in the chart at the corresponding times

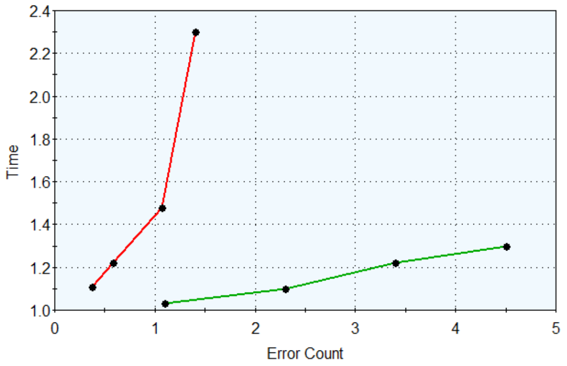


Figure 2.6: Error Count

Fig 2.6 shows the Errors consisted mainly of connection timeouts and HTTP 504, 502, 404, and 400 errors.

5. Discussion and Conculsion

To oppose the tiredness of mystery word ambush on the two-factor MAKA shows, incalculable three-factor MAKA shows have been proposed. In any case, for all intents and purposes every one of the three factor MAKA shows doesn't give formal confirmations and dynamic customer the official's instrument. In order to achieve progressively versatile customer the board and higher security, this paper proposes another three-factor MAKA show that supports dynamic disavowal and gives formal confirmation. The security exhibits that our show achieves the security properties of necessities from multi-server conditions. On the other hand, through the broad examination of execution, our show doesn't relinquish adequacy while improving the limit. Suddenly, the proposed show has mind boggling inclinations to the extent the outright estimation time.

References

[1] L. Lamport, "Password authentication with insecure communication," Communications of The 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 Transactions on Parallel and Distributed Systems, vol. 22, no. 8, pp. 1390–1397, 2011.

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

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

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

[6] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," IEEE Transactions on Consumer

Electronics, vol. 50, no. 1, pp. 251–255, 2004.

[7] C. C. Chang and J. S. Lee, “An efficient and secure multi-server password authentication scheme using smart cards,” in International Conference on Cyber worlds, 2004, pp. 417–422.

[8] J.-L. Tsai, “Efficient multi-server authentication scheme based on one-way hash function without verification table,” Computers & Security, 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,” Journal of Systems and Software, vol. 85, no. 4, pp. 876–882, 2012.