International Journal of Engineering & Technology, 7 (2.9) (2018) 109-114

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secure Data Access in Homogeneous and Heterogeneous Distributed Databases Using Effective Authentication Protocols

M. Natarajan [1*], R.Manimegalai [2]

[1*] *Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, Tamilnadu, India.*

[2] *Research Supervisor, Department of Information Technology, PSG College of Technology, Coimbatore, Tamil Nadu, India.*

Abstract

A distributed database is a group of several, understandably interrelated databases distributed over a computer system. Homogeneous and Heterogeneous databases are the two main classifications of DDBMS. In Homogenous distributed database system, the data is distributed but all servers run the same Database Management System (DBMS) software. In Heterogeneous distributed databases dissimilar sites run under the control of different DBMSs. The advantages of distributed database includes data duplication, low functioning costs, faster data operation and data processing, but security is still a major problem. In this paper, it's an effort to find the best security algorithms for homogeneous and heterogeneous database by comparing the proposed security algorithms called Key Computation based Secure Handshake Authentication Protocol (KCSHAP) and Key Agreement based Secure Kerberos Authentication Protocol (KASKAP) with some existing algorithms such as Multi-coefficient Secret Sharing (MCSS), Kerberos Authentication Protocol (KAP), handshake authentication protocol (HAP) in terms of computation complexity and number of access granted for the request. With the help of this best security protocol, the authenticated users can access the homogeneous and heterogeneous databases in a secure manner.

Keywords: Distributed DBMS, Homogeneous, Heterogeneous, Security, KASKAP, KCSHAP.

I. INTRODUCTION

A distributed database is a gathering of databases that are conveyed and saved on a few PCs (destinations) inside a lot of associations. The locales which are associated with the dispersed database have the full command over their database as far as dealing with the information. The destinations may likewise between work at whatever point required. A connection association in the database allows the hubs which are neighborhood to get to the information on a remote database. So as to begin these associations, every database in this framework must have a one of a kind name for the worldwide database in the system space. The name of the worldwide database distinguishes the database server particularly in a circulated framework. The appropriated information are administrated among neighborhood and worldwide exchanges. In nearby exchanges, the information can be gotten to just by the destinations where the exchange found, while a worldwide exchange is that the information have been gotten to in different locales [1]. The distributed database may arrange into homogenous and heterogeneous. A homogeneous distributed database has a similar programming and equipment running all databases occurrences, and may show up amid a solitary interface as though it were a solitary database. A heterogeneous conveyed database may have diverse equipment, working frameworks. An organization of appropriated database framework is neighborhood and worldwide exchange. A nearby exchange is alluded

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

as an information could be gotten to by the hub utilizing join association which is treated as a remote access [3].

1.1 Homogeneous Distributed Databases Management System

In homogeneous distributed database, all locales have indistinguishable programming and know about one another and consent to coordinate in handling the client demands. Each site surrenders some portion of its independence as far as directly to change construction or programming. A homogeneous DBMS appears to the client as a specific framework. The homogeneous framework is a lot simpler to propose and deal with. Figs 1.1 speak to the design of homogeneous database.

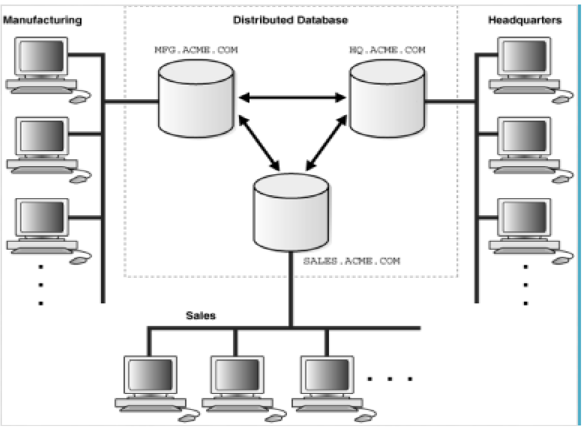

Fig 1.1: Homogeneous Databases Can Communicate Directly With Each Other

Properties of homogenous databases:

In a homogeneous appropriated database, every one of the destinations utilize indistinguishable DBMS and working frameworks. Its properties are

- The information structures utilized at every area must be same or good.
- The working framework utilized at every area must be same or all around coordinated.
- The database application (DBMS) utilized at every area must be same or good.
- The locales utilize much related programming.
- The locales utilize indistinguishable DBMS or DBMS from a similar seller.
- Each site knows about every single other site and participates with different locales to process client demands.
- The database is gotten to through a solitary interface as though it is a solitary database.

Homogeneous appropriated databases are characterized into two kinds. They are

- Autonomous – Each an each database is autonomous that capacities all alone. They are coordinated by a controlling application and use message going to share information refreshes.
- Non-self-sufficient − Data is distributed over the homogeneous hubs and a focal DBMS co-ordinates information refreshes over the destinations.

1.2 Heterogeneous Distributed Databases Management System

In a heterogeneous appropriated database, unique destinations may utilize diverse diagram and programming. Distinction in construction is a noteworthy issue for inquiry preparing and exchange handling. Locales may not know about one another and may give just constrained offices to participation in exchange preparing. In heterogeneous frameworks, diverse hubs may have distinctive equipment and programming and information structures at different hubs or areas are likewise unsuited. Distinctive PCs and working frameworks, database applications might be utilized at every one of the areas. For instance, one area may have the most recent social database the board innovation, while another area may store information utilizing regular records (old) of database the executives framework. Also, one area may have the Windows working framework and another may have UNIX. Heterogeneous frameworks are generally utilized when singular locales utilize their very own equipment and programming. On heterogeneous framework, interpretations are required to permit correspondence between various destinations (DBMS) [4]. In this framework, the clients must almost certainly make asks for in a database dialect at their nearby locales. Normally the SQL database dialect is utilized for this reason. In the event that the equipment is extraordinary, the interpretation is troublesome, in which PC codes and word-length is changed. The heterogeneous framework is regularly not actually or sensibly plausible. In this framework, a client at one area might almost certainly read yet not refresh the information at another area. The heterogeneous database engineering speak to in Fig 1.2

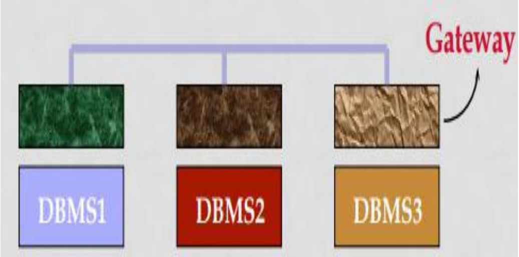

Fig 1.2: Heterogeneous Databases Communicate with Gateway Interfaces

Properties of heterogeneous database:

In a heterogeneous dispersed database, diverse locales have distinctive working frameworks, DBMS items and information models.

• Different destinations utilize divergent blueprints and programming.

• The framework might be gathered of an assortment of DBMSs like social, organize, various leveled or item situated.

• Query handling is confounded because of disparate patterns.

• Transaction handling is intricate because of disparate programming.

• A site may not know about different destinations thus there is limited co-activity in handling client demands.

There are two kinds of heterogeneous conveyed databases:

• Federated − The heterogeneous database frameworks are free in nature and incorporated together so they work as a solitary database framework.

• Un-united − The database frameworks utilize a focal planning module through which the databases are gotten to.

Security implies assurance of data and data framework from unlawful access, alteration and abuse of data [5]. The reason for dispersed database security is to manage shielding information from individuals or, programming having pernicious intension. Conveyed framework has four principle security parts, security validation, approval, Encryption, and staggered access control [6].

In area II, the calculations utilized for security of DDBMS have been talked about. Area III examines the test results and Section IV closes with end [7].

II. ALGORITHMS

In this section, the main algorithms viz., KASKAP and KCSHAP are used in this paper for security analysis of homogeneous and heterogeneous databases are discussed.

2.1 KASKAP

This proposed algorithm of mine is already explained in detail in the paper [8]. Here just stated the overview of this algorithm Kerberos validation [9] convention is checking the honesty, secrecy and approval of the whole hub over the conveyed system for anchored exchange utilizing the key assention. Key assention has a common confirmation which enhances the safe exchange around the appropriated condition. Kerberos with key assention calculation as pursues [10]

Algorithm

Step 1: Request from the client to the database

Step 2: Runs the trusted node with key agreement

Step 3: response from the database to the client [11]

2.2 KCSHAP

This proposed algorithm of mine is already explained in detail in the paper [2]. Here just stated the overview of this algorithm. A Secure database model is considered in this system where the global database is partitioned into a collection [13] of local databases and distributed over N sites connected via a network [12]. An independent processor has been equipped with each site, which has been connected through a secured communication link to other sites. Each site consists of a n number of client nodes and a trusted node. The trusted node processes the user requests from the client nodes. The combines the results from concerned distributed databases and forward it to the authenticated user. The trusted node authenticates the user based on the Key Computation based Secure Handshake Authentication Protocol (KCSHAP).

Algorithm:

Step 1: choose the websites in distributed database management system

Step 2: Assign a trusted node to the website

Step 3: For *every* nodes in the websites, Assign Private Security Number PSN for the node, which is a prime number of size 1024 bts

Step 4: A group key GK is randomly selected and it should satisfy GK > PSN assigned to the nodes

Step 5: every nodes in the websites **Compute** the message pair and password

III. RESULTS AND DISCUSSION

The proposed algorithms for homogeneous and heterogeneous like KASKAP and KCSHAP are evaluated by using the Network Attached Storage (NAS), which one of the popular distributed storage system. [14]. The computational problem is solved with some complexity can be defined in terms of power utilized with respect to time and it can be given as follows

$$\text{Computation complexity} = \text{Power utilized} \times \text{time}$$

Table 3.1 shows the Security analysis of Homogeneous database [15] using the proposed security algorithm KASKAP, KCSHAP with HAP, KAP and MCSS in terms of access granted with respect to access request from n number of users. For 50 access requests from the 50 users in the system, the KASKAP granted 40 access requests by denying 10 requests, while the MCSS granted 44 access requests by denying 6, HAP granted 46 by denying 4, KAP granted 43 by denying 7 and KCSHAP granted 42 by denying 8. It is clear that the proposed KASKAP performs better security than the stated algorithms [16].

Table 3.1 Security analysis of Homogeneous database

No of nodes	Computation complexity (Js)				
	KASKAP	HAP	KAP	MCSS	KCSHAP
10	700	970	900	1000	840
20	1100	1700	1800	1500	1200
30	1300	1500	1600	1900	1400
40	1600	2000	2300	2100	1800
50	2000	2300	2700	3000	2200

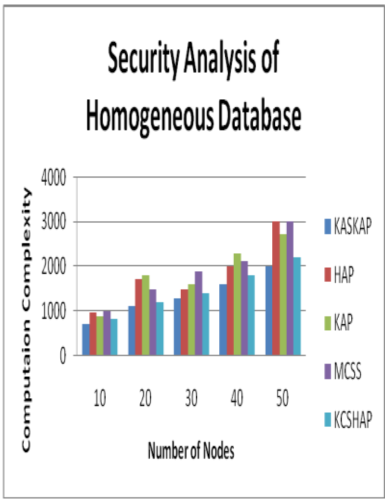

Fig.3.1Analysis of homogeneous database in terms of computation complexity

From the Fig 3.1 it clearly shows that the computation complexity of KASKAP is minimum compare to other security algorithms. KASKAP gives the better security access of the homogeneous databases in distributed data access.

Table 3.2 shows the Security analysis of Heterogeneous database using the proposed security algorithms KCSHAP, KASKAP with HAP, KAP and MCSS in terms of access granted with respect to access request from n number of users. For 50 access requests from the 50 users in the system, the KASKAP granted 42 access requests by denying 8 requests, while the MCSS granted 44 access requests by denying 6, HAP granted 46 by denying 4, KAP granted 43 by denying 7 and KCSHAP granted 40 by denying 10. It is clear that the proposed KCSHAP performs better security than the stated algorithms.

Table 3.2 Security analysis of Heterogeneous database

No of nodes	**Computation complexity (Js)**				
	KASKAP	**HAP**	**KAP**	**MCSS**	**KCSHAP**
10	800	1300	1200	1000	600
20	1000	1400	1300	1300	800
30	1400	1600	1800	1700	1200
40	1500	1700	2000	1900	1300
50	1700	1800	2200	2000	1500

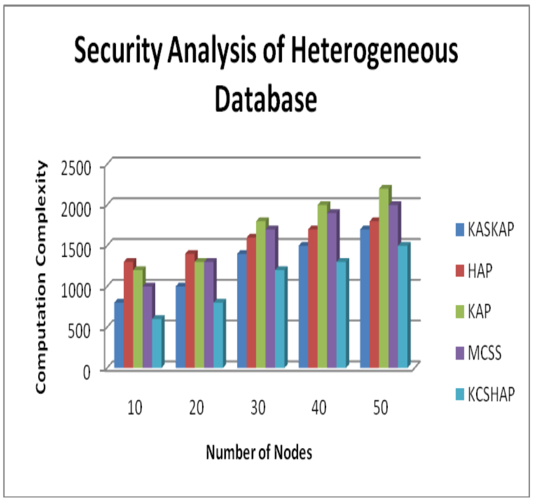

Fig 3.2Analys is of heterogeneous database in terms of computation complexity

From the Fig 3.2 it clearly shows that the computation complexity of KCSHAP is minimum compare to other security algorithms. KCSHAP gives the better security access of the heterogeneous databases in distributed data access.

IV. CONCLUSION

This paper analysis the security of homogeneous and heterogeneous databases in distributed databases by comparing the proposed security algorithms called Key Agreement based Secure Kerberos Authentication Protocol (KASKAP) and Key Computation based Secure Handshake

Authentication Protocol (KCSHAP) with some existing security algorithms such as Multi-coefficient Secret Sharing (MCSS), Kerberos Authentication Protocol (KAP), handshake authentication protocol (HAP) in terms of computation complexity and number of access granted for the request. According the experimental results, the KASKAP performs better security in homogeneous databases compared to other security algorithms in terms computation complexity and KCSHAP performs better security in heterogeneous databases in terms of low computation complexity and high authentication. With the help of this proposed best security algorithms viz., KASKAP and KCSHAP, the authenticated users can access the homogeneous and heterogeneous databases in a secure manner.

REFERENCES

1. M. Natarajan and R. Manimegalai, “Key Computation based Secure Handshake Authentication Protocol (KCSHAP) for Secured Distributed Database Access”, IJCTA, 9(40), 2016, pp. 183-189

2. Shakeel PM, Baskar S, Dhulipala VS, Mishra S, Jaber MM., “Maintaining security and privacy in health care system using learning based Deep-Q-Networks”, Journal of medical systems, 2018 Oct 1;42(10):186.https://doi.org/10.1007/s10916-018-1045-z
3. Shakeel PM, Baskar S, Dhulipala VS, Jaber MM., “Cloud based framework for diagnosis of diabetes mellitus using K-means clustering”, Health information science and systems, 2018 Dec 1;6(1):16.https://doi.org/10.1007/s13755-018-0054-0
4. *M.Natarajan, R.Manimegalai, “*Key Agreement based Secure Kerberos Authentication Protocol (KASKAP) for Distributed Database Access in Secured Manner”IJET,7(2.9).2018,pp 24-27.
5. Mohamed Firdhous, “Implementation of Security in Distributed Systems – A Comparative Study”, *International Journal of Computer Information Systems,*vol. 2, issue 2, 2011
6. Sridhar KP, Baskar S, Shakeel PM, Dhulipala VS., “Developing brain abnormality recognize system using multi-objective pattern producing neural network”, Journal of Ambient Intelligence and Humanized Computing, 2018:1-9. https://doi.org/10.1007/s12652-018-1058-y
7. Kun Fang, “TRUST Management Model in Distributed GIS”, 2008 IEEE.
8. Min Zhang, Desheng Zhang, Hequn Xian, Chi Chen, Dengguo Feng, “Towards A Secure Distribute Storage System”, *International Conference on Advanced Communication Technology, Gangwon-Do, IEEE*, vol 3, pp 1612 – 1617, 2008.
9. P. Mohamed Shakeel; Tarek E. El. Tobely; Haytham Al-Feel; Gunasekaran Manogaran; S. Baskar., “Neural Network Based Brain Tumor Detection Using Wireless Infrared Imaging Sensor”, IEEE Access, 2019,vol 7,issue 1, Page(s): 1
10. Shakeel, P.M., Tolba, A., Al-Makhadmeh, Zafer Al-Makhadmeh, Mustafa Musa Jaber, “Automatic detection of lung cancer from biomedical data set using discrete AdaBoost optimized ensemble learning generalized neural networks”, Neural Computing and Applications,2019,pp1-14.https://doi.org/10.1007/s00521-018-03972-2
11. MD.TABREZ QUASIM, “Security Issues in Distributed Database System Model”, COMPUSOFT, An international journal of advanced computer technology, 2 (12), December-2013 (Volume-II, Issue-XII)
12. Dr.Mohmad Kashif Qureshi “Security Aspects of Distributed Database”, IJAIR(2013)pp197-212.
13. Parul Tomar and Megha, “ An Overview of Distributed Databases”, International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 2 (2014), pp. 207-214.
14. Dr.C.Sunil Kumar,2 J.Seetha, S.R.Vinotha, ”Security Implications of Distributed Database Management System Models” International Journal of Soft Computing And Software Engineering (JSCSE) e-ISSN: 2251-7545 Vol.2, o.11, 2012.
15. Baskar, S., et al. "An Energy persistent Range-dependent Regulated Transmission Communication Model for Vehicular Network Applications." Computer Networks (2019).
16. Ranjana Thalore, Partha Pratim Bhattacharya, Manish Kumar Jha, “Performance Comparison of Homogeneous and Heterogeneous 3D Wireless Sensor Networks”, Journal of Telecommunication and Information Technology (2017).