*International Journal of Engineering & Technology*, 7 (2.9) (2018) 24-27

International Journal of Engineering & Technology

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

***Research paper***

# Key agreement based secure Kerberos authentication protocol (KASKAP) for distributed database access in secured manner

**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, TamilNadu, India*
**Corresponding author E-mail: natrajanm944@gmail.com*

## Abstract

Distributed database is a collection of multiple databases that can be stored at different network sites. It acts as an important role in today's world intended for storing and retrieving huge data. The implementation of distributed database advantages such as data replication, low operating costs, faster data transaction and data processing, but security is still a significant problem. In this paper make clear to explain security issues of distributed database and give the suggestion to improve security of distributed database. Subsequently, secured distributed database design in light of trusted node is proposed. The design contains a unique node in a system called a trusted node for each site through which every single other node will get to the database. Trusted node process client demands, joins the outcomes from concerned distributed databases and forward it to the confirmed client. The system adjusted by the trusted nodes keeping in mind the end goal to give authentication is Key Agreement based Secure Kerberos Authentication Protocol (KASKAP). Hence authenticated users can only access the database.

***Keywords***: *Trusted Node; Distributed Database; Authentication; Security; KASKAP.*

## 1. Introduction

Today data is a kind of important source considered in information system. Data source is an essential part of core capability of enterprise [1]. Whereas increasingly highly developed infrastructure, continuous advance of their applications, facility of enterprises and data acquisition. Therefore growth rate of information system is faster when compared with other category of data. Due to that reason the traditional storage system does not satisfy the requirement of large scale storage [2]. Consequently, the computer storage technology travels to the distributed database system for rapidly growth of data. Distributed database system is a collection of databases which are distributed and organized in more than a few computers (nodes) among the network. Distributed system has an extensibility of data, effectiveness of processing, storage of large scale data, good robustness and concurrency transmission [3]. An administration of distributed database system is local and global transaction. A local transaction is referred as a data could be accessed by the node using link connection which is treated as a remote access [4]. Whereas the global transaction is referred as the data have be multiple nodes. While the data across multiple nodes then the data security could not be an ensured. Therefore the security is a one of the issue in distributed database system until now. Therefore the global transaction process using an intermediate for improving the security from the hackers which is called as trusted node [5]. Trust node process takes requests from the users and forward to the distributed database after that transitory the response from database to client using authentication. Authentication is a form of identification which is confirming the certainty between the client and the distributed nodes. Though, the key identification is one type of authentication for improving the security. Early of the database technology have client based key identification which have some drawback therefore move to the mutual authentication in distributed storage system. Key established the both sites such as client and the distributed node then the transactions are effectively executes between the client and the node in secured manner.

In this paper proposed Key Agreement based Secure Kerberos Authentication Protocol (KASKAP). Here develop a distributed authentication system for secured data access in efficient manner. Every node has a trusted node for authenticate the user belonging to the global transaction. The trusted node passing the request from the user to distributes database by using other trusted node in the network and forward the response from the database to the authorized client.

Remaining of the paper is organized as follows section 2 contains a related work. The proposed Key Agreement based Secure Kerberos Authentication Protocol (KASKAP) is clearly explained in section 3. The experimental results and discussion explained in section 4. Section 5 contains the conclusion of the work.

## 2. Related work

Maria Moloney [6] presents a trusted based security in MANET by combining the security management and context aware computing. Which could established suitable trust level for each and every situations. A priori trust relationship between router and the client which is identify every router before access to the network. The proposed system is successfully improves the computation of trust node and provide a strong and additional complete security in the

MANET. The system is overcome the weakness of MANET. Shao-Hua Liu [7] presents a genetic algorithm to improve the fuzzy c-means clustering algorithm for classifies the data. Simulation result of improved algorithm is fined the optimum query execution plan in a short period of time and also improves the query efficiency. Experimental result shows the performance of improved genetic algorithm which is better than the novel genetic algorithm. The novel genetic algorithm is using multi join query of distributed database optimally. Improved algorithm is setting the crossover and the mutation of genetic using in fuzzy c-means clustering.

Kun Fang [8] introduce the safety management patter which is a model of distributed computing. Client need to access some data in the web by using node in spite of there is no authenticate. This paper is to solve the above problem using trust management. The experimental results solve the good way of issue in distributed GIS. Qiao Sun, Lan-mei Fu, Bu-qiao Deng [9] explained challenges of transaction in heterogeneous environment. Every sub transaction need to local and global manager. Implements super text pre-treatment language for distributed transaction processing. This is to resolve the above mentioned problem. In this work is XA interface using PHP and MySQL for distributed process. The proposed method improves the reliability of transaction process, realization of distribution and power of modern information system.

Min Zhang, Desheng Zhang, Hequn Xian [10] proposed a secure network storage architecture which adds a layer for managing from node to the users. This is able to provide a reliable storage and secure data service while the storage servers. The architecture sufficiently reduces the scope of large scale storage and provides a access control flexibly. It ensures the privacy, integrity, scalability, efficiency, flexibility and availability of the distributed database system. The architecture presents a most important security function and key escrow format and an access control method. It amazingly enhancing the security of open storage system by provides a trusted execution environment.

## 3. Methodology

In this paper considered a secure distributed database system. The distributed database is collection of database where the global database is partitioned into a local database and distributed more than N nodes associated through a network. Every node has an N amount of client nodes as well as trusted nodes. The trusted node process is receives the request from the client and send to the database. After that the trust node forwards the response from distributed database to the authenticated client. The trusted node enables mutual authenticates based on the Key Agreement based Secure Kerberos Authentication Protocol (KASKAP). The architecture of the proposed system is shown in figure 1.

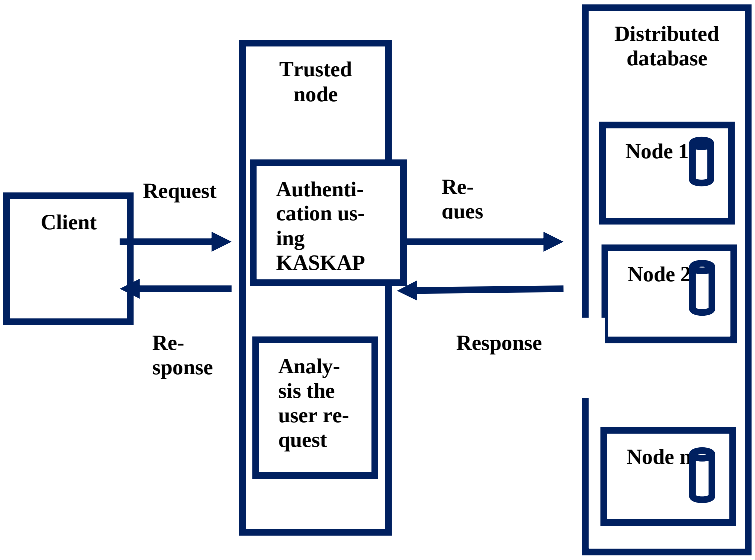

**Fig. 1**: Proposed System Architecture.

### 3.1. Key agreement

A key agreement protocol [11-12] enables the mutual authentication between client and database. Initially authentication verify between client and trust node and the same verification process followed between trust node and database as follows

Algorithm 1

Step 1: To generate random integer is defined as$r_a$, $k_a$is defined as ephemeral key from the time interval of [1, n-1] and process is defined as $Q_a$ and $V_a$ the request on P such as

$$Q_a = r_a.P \text{ and } V_a = -k_a.P \tag{1}$$

Client sends request $V_a$ to trust node.

Step 2: Trust node selects an integer randomly is defined as$r_b$, $k_b$is defined as ephemeral key from the time interval of [1, n-1] and process is defined as $Q_b$ and $V_b$ the request on P such as

$$Q_b = r_b.P \text{ and } V_b = -k_b.P \tag{2}$$

Trust node process is $E_b = H(x_{Q_b}, x_{V_b}, x_{V_a}, ID_b, ID_a)$ (2) and

$$d_b = r_b + e_b k_b + e_b s_b \tag{3}$$

Where $x_{Q_b}$is defined as x-coordinate of$Q_b$, $x_{V_b}$ is defined as x-coordinate of$V_b$ and $x_{V_a}$ is defined as x-coordinate of$V_a$. Trust node sends$V_b$, $E_b$ and $d_b$ to client.

Step 3: client process the request $U_b$ is defined as $U_b = d_b.P + e_b.V_b + e_b.Y_b$ and verify $e_b + H(x_{U_b}, x_{V_b}, x_{V_a}, ID_b, ID_a)$ it does not hold then client terminates the execution. Otherwise

$$e_a = H(x_{Q_a}, x_{V_b}, x_{V_a}, ID_b, ID_a) \tag{4}$$

$$d_a = r_a + e_a k_a + e_a s_a \tag{5}$$

Where $x_{U_b}$an x-coordinate of is$U_b$ , $x_{V_b}$ is defined as x-coordinate of$V_b$, $x_{V_a}$ is defined as x-coordinate of$V_a$ and $x_{Q_a}$is defined as x-coordinate of$Q_a$. Client process the request $k_a$ as follow

$$k_a = -k_a.V_b \tag{6}$$

And sends$e_a$, $d_a$ to trust node.

Step 4: trust node process the request $U_a$ such as $U_a = d_a.P + e_a.V_a + e_a.Y_a$ and verify $e_a = H(x_{U_a}, x_{V_b}, x_{V_a}, ID_b, ID_a)$. It does not hold then trust node terminates the execution. Otherwise

$$k_b = -k_b.V_a \tag{7}$$

Shared secret is request $k = k_a = k_b$.

Similarly above mentioned steps are followed to verify the authentication between trust node and database. Here to implement a mutual authentication protocol [13] using key agreement for privies a high security in the distributed database system. If the mutual authentication combines with the Kerberos as follows.

### 3.2. Key agreement based secure Kerberos authentication protocol (KASKAP)

The distributed authentication service is one of the challenging processes therefore travel to the Kerberos authentication. Contribution of the Kerberos authentication protocol is verifying the integrity, confidentiality and authorization of the entire node across the distributed network for secured transaction using the key agreement. Key agreement has a mutual authentication which improves the secure transaction around the distributed environment.

Kerberos with key agreement algorithm as follows

Algorithm 2

Step 1: Request from the client to the database which defined as

$$tgs_{req}: \{ts, \ldots\}\ K_{c,tgs}\{T_{c,tgs}\}K_{tgs}, V, Time_{exp}, n \tag{8}$$

Where $K_{c,tgs}$ is defined as key of the client node and tags, $Time_{exp}$ is defined as a time interval of request.

Step 2: Runs the trusted node with key agreement which is explained above in the section 3.1

Step 3: response from the database to the client is defined as

$$tgs_{rep}: \{K_{c,v}, V, Time_{exp}, n, \ldots\}K_{c,tgs}, \{T_{c,v}\}, K_v \tag{9}$$

Where $K_{c,v}$ is defined as key of the database and response tags, $Time_{exp}$ is defined as a time interval response

Initially client sends a request to the trusted node with the ID then the trusted node fined the request tag, where is located in the distributed environment. After that the connection will established from client to database. Second stage is generates the key for client and as well as the tags using key agreement because in this paper proposed mutual authentication. After that the authenticated client request pass to the database and the replay of database will forward to the client using Kerberos protocol because which is an efficient protocol of distributed environment. The proposed Key Agreement based Secure Kerberos Authentication Protocol provides an efficient high secure data transaction via the distributed database system.

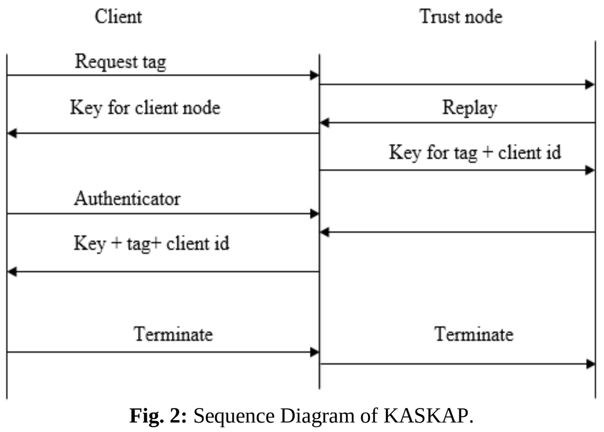

**Fig. 2:** Sequence Diagram of KASKAP.

## 4. Result and discussion

The experimentation of proposed KASKAP is using the Network Attached Storage (NAS) which is a most popular distributed database system. The configuration of experimental system is dual-core 2.01GHz Pentium processor, 4GB RAM and Windows 8. The experimental is passed out maximum 50 nodes and 50 requests. The proposed protocol is compared with existing protocol like tradition Kerberos Authentication Protocol (KAP), handshake authentication protocol (HAP). KASKAP has provides an efficient computation complexity. The computation problem is solved in terms of utilization of power with time utilization as follows

$$\text{computation complexity} = \text{power} \times \text{time} \tag{10}$$

Table 1 shows the computation complexity of proposed work and figure 3 shows the graphical representation of computation complexity.

Database

Check it in database

Response key + tag+ client id + DB id

Key + tag+ client id

Terminate

**Table 1:** Computation Complexity of Proposed Work

| 10 Request/Min | | | | | | |
|---|---|---|---|---|---|---|
| No. nodes | Time | | | Power | | |
| | KASKAP | HAP | KAP | KASKAP | HAP | KAP |
| 10 | 7 | 10 | 10 | 700 | 970 | 970 |
| 20 | 11 | 18 | 15 | 1100 | 1800 | 1500 |
| 30 | 13 | 15 | 18 | 1300 | 1500 | 1800 |
| 40 | 16 | 20 | 23 | 1600 | 2000 | 2300 |
| 50 | 20 | 23 | 27 | 2000 | 2300 | 2700 |

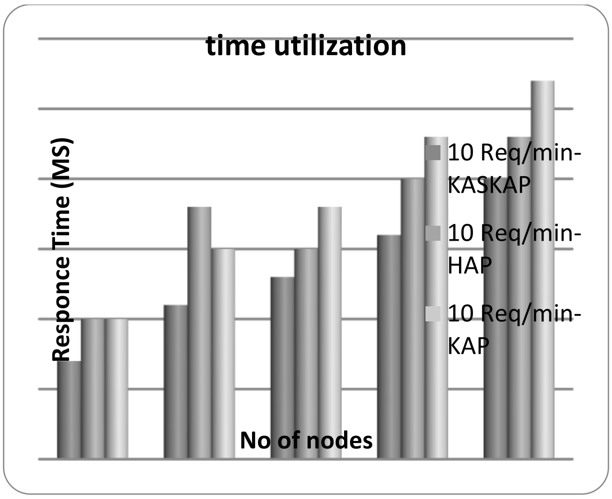

**Fig. 4:** Time Utilization.

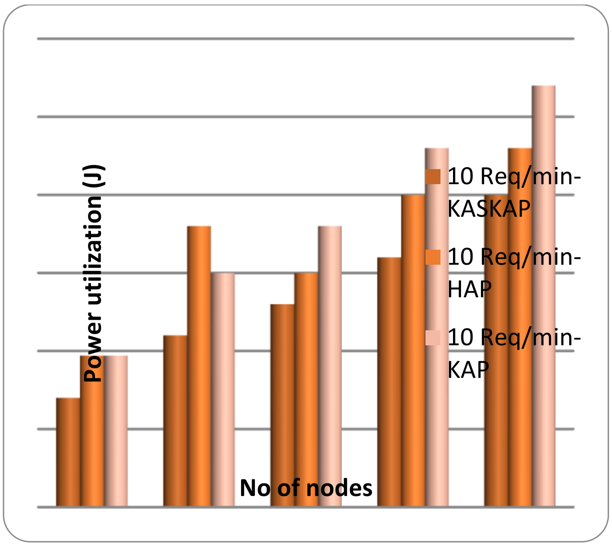

**Fig. 5:** Power Utilization.

From the analysis report of figure 3 and 4 describes the proposed work is achieved the low power and less time utilization because using the trusted node which compared to an existing protocol like tradition Kerberos Authentication Protocol (KAP) and handshake authentication protocol (HAP).

## 5. Conclusion

Security is a one of the considerable area in distributed database system therefore in this paper proposed a Key Agreement based Secure Kerberos Authentication Protocol (KASKAP) using trusted node for increasing the security when access the global transaction. Trusted node has an intermediate node between client and the database. Key agreement is a mutual authentication in both ends such as client and database tags which is process in trusted node. The trusted node is passing the request from client to database and forward the response from the database to client using Kerberos authentication protocol. Kerberos protocol is used for transferring the data around the distributed network efficiently. Therefore, the combination of Key Agreement based Secure Kerberos Authentication Protocol achieved very low computational complexity which is compared with existing protocol.

## References

[1] Yao Hongyu. Big data and cloud computing [J]. Information technology and standardization of big data and cloud computing, 2013 (5):21-22.

[2] J. Kubiatowicz, D. Bindel et al: OceanStore: An Architecture for global-scale persistent storage, ASPLOS, 2000. https://doi.org/10.1145/378993.379239.

[3] Avishay Traeger, N.Joukov, J.Sipek, E.Zadok, Using Free Web Storage for Data Backup, StorageSS'06, Oct 2006.

[4] Mohamed Firdhous, "Implementation of Security in Distributed Systems – A Comparative Study", *International Journal of Computer Information Systems*,vol. 2, issue 2, 2011.

[5] Gulhane, Bodkhe, S, "DDAS using Kerberos with Adaptive Huffman Coding to enhance data retrieval speed and security", *International Conference on Pervasive Computing (ICPC), Pune, IEEE*, pp 1-6, 2015

[6] Maria Moloney, Stefan Weber, "A Context-aware Trust-based Security System for Ad Hoc Networks", 2005 IEEE.

[7] ShaoHua Liu, Xing Xu, "Distributed Database Query Based on Improved Genetic Algorithm", 2016 IEEE. https://doi.org/10.1109/ICISCE.2016.84.

[8] *KunFang, "*TRUST MANAGEMENT MODEL IN DISTRIBUTES GIS*",* 2008 IEEE.

[9] Qiao Sun, Lan-mei Fu, Bu-qiao Deng, Jiasong Sun, "An Efficient Transaction Processing Method on the Distributed Database", 2016 9th International Congress on Image and Signal Processing, Bio-Medical Engineering and Informatics(CISP-BMEI 2016), IEEE.

[10] Min Zhang, Desheng Zhang, Hequn Xian, Chi Chen, Dengguo Feng, "Towards A Secure Distribute Storage System", Hi-Tech Research and development program (863) of china, Feb 2008.

[11] Bellare, M., P. Rogaway (1994). Entity Authentication and Key Distribution. *In Advances in Cryptalogy CRYPTO'93*, pp. 341-358. https://doi.org/10.1007/3-540-48329-2_21.

[12] Menezes, A., M. Qu, S. Vanstone (1995). Key Agreement and the need for authentication. PKS'95, Toronto, Canada.

[13] Law, L., A. Menezes, M. Qu, J. Solinas, S. Vanstone (1998). An efficient Protocol for Authenticated Key Agreement. *Technical Report CORR98-05*, Department of CO, University ofWaterioo.

[14] Menezes, A., M. Qn, S. Vanstone (1995). Some new key agreement protocols providing mutual implicit authentication. *Workshop on Selected Areas in Cryptography (SAC'95)*, pp.22-32.

[15] 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. https://doi.org/10.1109/ICACT.2008.4494090.