Addressing the Security Issues of Kerberos Method using RAID Level 5

Mousumi Hasan Mukti, Sabina Zaman, Khalil Ahammad, and Chowdhury Shahriar Muzammel

Abstract—Cloud computing is being considered as a revolutionary technique in the field of enterprise hardware and software design and development. As the popularity of cloud computing is increasing day by day and it's the mostly used technique in the online and automated business system, so the security of the stored data in the cloud and the accessing method of the data through the network must be ensured. Among the various types of server and network authentication protocol Kerberos is the latest and robust network protocol. For authentication, Kerberos is badly in need of a hosted server which has to be remaining running 24*7 and the access point should be a single server (centralized authentication service). Besides these, if the single server gets down, there is possibility of more attack as Kerberos can’t function its job. These are the major hindrance of Kerberos. This research paper has tried to overcome these security issues, accessing and recovering data by using the RAID level. RAID 5 is the most appropriate technique to recover from failure and in correcting the erroneous data by minimizing redundancy as well as mitigating data loss. Also, RAID 5 can be used in case of distributed data. So, a model has been proposed to configure RAID 5 to ensure better security of cloud storage by overcoming the limitations of Kerberos.

Index Terms—Cloud Storage; Cloud Computing; Distributed Data; Kerberos; RAID Level 5; Security.

I. INTRODUCTION

At the beginning of 21st century a word CLOUD and then CLOUD COMPUTING then CLOUD STORAGE has become the real buzzwords in the world. Customers have get involve in cloud computing of cloud storage as cloud computing gives various services like service on call, provides huge storage of data, allows users to access data on demand at anytime from anywhere and a reduces amount of administration [1]. All these services are provided by cloud computing in a package. So IT professionals get interested to cope up with this new technology, to be increase their dynamic skill they are also running after cloud based data, service and computing. As a whole by several years the amount of data in cloud storage are getting higher and higher with the popularity of cloud computing. For the growing vast service and millions of associated users and organizations the security of cloud based services is now the most prime concern. Both organizations and customers can access cloud data just by connecting by the internet. Kerberos network authentication protocol is the mostly used overall network protocol to give the authentication service by allowing the users encrypting their private data. Kerberos eliminates the use of remembering multiple authentication information by allowing user single sign key. For providing all these secured services Kerberos needs a dedicated centralized server which should remain running continuously. If the server is down the whole system will be stopped and thus the network security of users will be compromised. And for centralized data authentication, recovery from failure is quite impossible. Through this research work it has been tried to solve these security problem of Kerberos by configuring RAID 5 on a previously configured Kerberos server. RAID 5 allows block interleaved distributed parity [2]. Hence by using RAID 5 in Kerberos server the data for authentication can be stripped in more than 3 disks. This technique can diminish the centralized sever authentication and allow a way of recovery after failure.

II. CLOUD COMPUTING AND CLOUD STORAGE

Different cloud service providers like Microsoft Azure, Amazon web services, IBM define cloud computing as IT standard which provides result of computation, database storage on demand, and many other IT services via internet by means of payment from organizations who are taking the cloud services.

Cloud storage is a model of cloud computing. In it data is usually stored on remote sites/ servers which can be accessed by users through internet/cloud. Maintenance, operating and management are provided by vendors or cloud storage provider. Data center is the representation of cloud storage. It is implemented on virtual environment and gives scalability to application through which users access the data storage. Users can get access of data through API. From the definition of cloud computing and cloud storage users can be identified. The users of cloud computing can be classified into two. One the organizations who are renting cloud computing service from the cloud provider and or vendors and second the users who are actually using the cloud computing services. Maintaining the huge IT infrastructure like data center is always not possible for many organizations and even many of the companies are not interested to maintain it. From this necessity the Cloud storage technology arises. As in recent years the usage and popularity of cloud storage has grown higher and higher so as the cloud computing. Users can access the stored data in cloud and make reliable transactions and performance simply by connecting internet in a high speed as well as can avail the data continuously. This may tend to the topic cloud computing.
III. KERBEROS

MIT introduced a network authentication protocol named Kerberos by using symmetric-key cryptography to provide network services eliminating the need of sending passwords over the network. Kerberos uses strong cryptography so client can prove his identity to a server through an insecure network connection. To assure privacy and data integrity client and servers can use Kerberos to encrypt all their communication and also to identify them. Within a network system integrity and security can be cumbersome. Administrators can be busy a long duration just in tracking of what services are being run on the network and the way the services are used. At that time, the used technique by the protocol is in danger to identify authenticated users. Protocols those allow insecure methods of authentication Kerberos is the means of eliminating those and thus increasing overall network security. Kerberos has tried to ensure that every single user who are connecting and using the cloud server can generate and apply special information for high level security [3]. Kerberos Authentication is done by the method of ticket Granting server. Kerberos V5 authenticates users by the following steps [1].

![Fig. 1. Steps of Kerberos Authentication [1]](image)

A. Importance of Kerberos in Cloud Storage and Cloud Computing

The cloud storage and the cloud computing both are technology based on internet. Thus the security concern arises high to ensure the security level in cloud computing. Thus arise, the network authentication issue for both the customer and the organization taking the cloud storage and computing services from cloud service provider and vendor. Among the various number of network authentication protocol, Kerberos and thus its versions are the latest network authentication protocol. By Kerberos customer, service provider and the organization buy or rent cloud storage can connect to each other by encrypting their personal data [4]. Many protocols like, DIAMETER, CHAP, EAP, PAP and RADIUS are not for overall authentication protocol for the network. One may concern to identify server and other may works to authenticate user’s password only. But Kerberos is the authentication protocol for the complete network.

B. Major Hindrance of Kerberos

Though Kerberos the highest used and most secure and better performed network authentication protocol but there are some major holes which may be the hindrance for Kerberos are as follows:

1. Kerberos requires a dedicated centralized server which can be said as a “Single point of Access” for continuous availability or authentication. New users cannot log in if the Kerberos server is down
2. Replay Attack [5].
3. Platform dependency and password guessing attack [6].
4. The whole community who are communicating with each other should use Kerberos else no one.
5. In RFC 3244 it is described that Kerberos administration protocol varies between server implementation and is not standardized also. All four drawbacks stated above are not the main concern of this research. Here the first one Centralized Server is main drawback on which the paper has worked for.

IV. PROBLEM FORMULATION OF THE RESEARCH

From the limitations and drawbacks of Kerberos it’s clear that Kerberos system has several drawbacks. A central server is required to be available in 24*7 hours. A user cannot login if the Kerberos server is down. The problem has been addressed by using N-Kerberos (multiple Kerberos) [7]. In this project work, it has shown how single point of failure could be removed to solve or to minimize the first drawback of Kerberos stated in the section of Major hindrance of Kerberos. Here Raid level 5 is used to remove the drawback and this proposed system is implemented in a baking network infrastructure.

V. METHODOLOGY USED TO ADDRESS THE FORMULATION PROBLEM

Each drawback has different solution approaching different methodologies and formulation and also same problem can be solved in various ways. This research has tried to address and finally to solve the security, recovery and error correcting and detecting issues of using dedicated single server by Kerberos. Hence we used RAID level 5 and configured RAID 5 on Kerberos server.

A. RAID and RAID Levels

To improve reliability via redundancy and to improve performance via parallelism of database hence for stored data the concept of RAID (Redundant Array of Independent Disks) has introduced. There are 7 types of RAID level which are named as RAID0 –RAID6. Though the letter R of RAID indicates Redundancy but all RAID levels don’t support redundancy. Zero redundancy, Disk mirroring, ECC, bit-interleaved parity, block interleaved parity, block interleaved distributed parity and P+Q redundancy scheme are used in different levels of RAID [8]. For the purpose of this research RAID 5 has been selected and configured over Kerberos server.

B. Choosing factors of RAID Level

Factors behind choosing of a RAID level are crucial issues. Availability, application performance, capacity, cost, monetary cost and performance should be taken into
account. Performance in failure and in rebuilding of a failed disk is also important choosing factors of RAID level.

C. Reason for choosing RAID Level5

For increasing performance DISTRIBUTED parity is used in RAID level 5. It’s called Block Interleaved Distributed Parity [8]. In RAID 5 parity bits are partitioned and distributed across N+1 Disks. This mechanism let all the disks to participate in read operation. There is parity block in RAID 5. But it doesn’t store the parity in the same block but stored them in distributed manner. Thus in disk failure and in data loss it’s recoverable by RAID 5 [8]. This is the main reason of using RAID5 over other RAID levels. Previously it has been mentioned that the Kerberos server requires a single dedicated server which tends to a single socket for failure and no data recovery. By configuring RAID5 over Kerberos has solved these short coming of Kerberos server in a great deal. But for this the performance has been sacrificed a bit. For research a small amount of cloud storage has been parched and among that storage only 25% is used for redundancy.

VI. CONFIGURING RAID LEVEL 5 IN KERBEROS SERVER

Solution may be simple but tricky or broad and complex and the combination of simple, tough and complexity. In this research it’s also not tough to configure the RAID 5 in Kerberos server rather the main point was to identify the problem and then find a proper solution. In this purpose we purchased small volume of cloud storage from cloud service provider then set up Kerberos network authentication protocol to identify and encrypt information of the users who has used our demo system hosted in cloud server. After setting up Kerberos in cloud server RAID 5 has configured over it. There are two possible ways to configure RAID 5 in a server. First one is configuring RAID 5 using Kerberos Server 2008 Disk Management and other is using the Disk Part command in command prompt.

A. Configuration RAID 5 Using Kerberos Server 2008

Disk Management

The Disk Management snap-in is used to configure Windows Server 2008 RAID 5. This can be accessed either from Computer Management tools or from the Server Manager. Disk Management Tools are found in the storage Category in all scenarios. In previous section it has been stated that minimum number of 3 disk drives are mandatory for RAID 5 implementation. The configuration window is given here as figure [2].

In total four disks have been created after partitioning. Disk 0 to Disk 3. Among these four disks, disk 0 has been used as system disk and has not been included to configure the RAID 5. But as at least 3 disks are required to configure it so the other three disks: Disk 1, 2 and 3 are added to store the users’ personal information by block interleaved distributed parity mechanism.

B. Configuring from command prompt

Another way of configuring the RAID 5 on Kerberos server is using the Disk Part command. It has to be done from the command prompt. By typing <diskpart> on Run dialog or by entering command prompt DiskPart can be initiated. After initializing the command prompt the following commands are typed and executed sequentially to configure RAID5. Following Five steps are used to configure RAID5 from command prompt are given in figures [3] to [7].

Fig. 2. Configuring RAID 5 Using Kerberos

Fig. 3. Listing all disks

Fig. 4. Converting into dynamic disk

Fig. 5. Adding disks for RAID5
VII. CONCLUSION

Cloud Storage is designed to ensure extreme scalability, and to manage storage systems easily. This research gives a summarized preface to cloud storage. We have found that to ensure continuous secured cloud storage and cloud computing services Kerberos has great importance. After finalizing the problem statement of Kerberos authentication protocol, the paper has tried to solve/minimize the major limitations of Kerberos that is single point failure of Kerberos authentication protocol to recover after failure. But RAID Level 5 gets down if parity disk fails. To make the proposed system more efficient, other drawbacks of Kerberos should be solved.

REFERENCES