Construction of Information Security Evaluation Model Based on Information Ecology

Tian Ru Jun

Information Engineering University, Zhengzhou, Henan, 450001, China

Keywords: Security private cloud network, Information security evaluation model, Information ecology

Abstract: In this paper, the author researches on the construction of information security evaluation model based on information ecology. The traditional static security defending system, such as firewall, data encryption, identification authentication, admission control and operate system reinforced technology, can't completely satisfy the need of the security condition. According to the complexities and diversifications of the attack methods and means, the intrusion detection technology, become a new hot issue in the field of the information security. By using Bayesian topic modeling to capture the intrinsic structure of atomic activity and interactions in the NAS security private cloud network, we effectively tune model parameters to detect as quickly as possible, the transition from normal to abnormal behavior. The experiment result shows the proposed method can improve the overall system performance substantially.

1. Introduction

The Internet technology, the Internet began to spread to various industries and fields, "Internet plus" affects people's knowledge system and way of life. The "Internet+" as a hot word that widely spread as the prime minister's government work report during the period of NPC and CPPCC. As a concept, it is not a new word, it be noticed and discussed in the Internet industry before being rose to national level. As a kind of semi-structured concept, the lack of another subject shows that it has a lot of space behind the "+". With what method to add, and what kind of bonus effect will reach, it is not entirely within the estimate. The popularity of "Internet+" is a direct reflection of Social development trend. That is, the Internet as an infrastructure that equally important with water, electricity and other energy sources, is gradually changing people's work and life. For the media industry, the attitude towards the Internet is mixed. Today, people's attention is attracted by a great deal of information that generated by the kinds of Internet community.

The DAS direct connection, storage space can solve the single server scalability, high performance transmission and external demand, single storage system capacity, has never come to 1TB, to 2TB, with the introduction of large capacity hard disk, a single external storage capacity will rise. Prior to the emergence of NAS and SAN, DAS has been in the storage market occupies an absolute share. But with the continuous growth of user data, especially for hundreds of GB or more, the recovery in the backup and disaster recovery, expansion, and other issues become increasingly troubled by the system administrator [1-3]. Direct attached storage on the server host operating system for IO read and write data and storage management, data backup and recovery requirements using the resource of the host server (including CPU, IO, tape machine system) data streams need to return to the host server is connected with the (Library), data backup server resources usually occupied by 20-30%, so direct attached storage leads to more amount of data backup and recovery, time is long, the server hardware dependence and influence is greater, which has become the bottleneck of the development of the most deadly DAS. According to the data show that by 2003, the market share of DAS products has been more than NAS and SAN products.

  DOI: 10.25236/iccem.2021.056

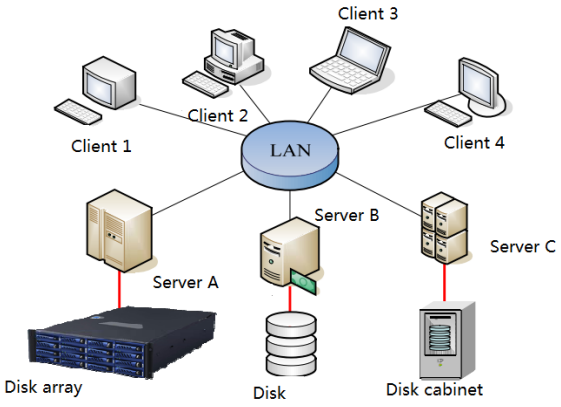

Fig.1 Schematic Diagram of Das Network Topology

A NAS includes a processor, a file service management module, and a plurality of hard drives for data storage. NAS can be used in any network environment. The main server and client can be very convenient access to any format on the NAS file, including SMB format, NFS format and CIFS format, etc. NAS system can be based on server or client computer instructions to complete the internal file management. Moreover, the NAS system can be directly connected to the network via Hub or switch, and is a plug and play network device. Again, there is no need for the primary server because it is independent of the primary server. This can greatly reduce the cost of investment in the main server. Finally, NAS has better scalability and flexibility. Storage devices are not subject to geographical constraints can be connected at different locations through physical connections and network connections [4-5].

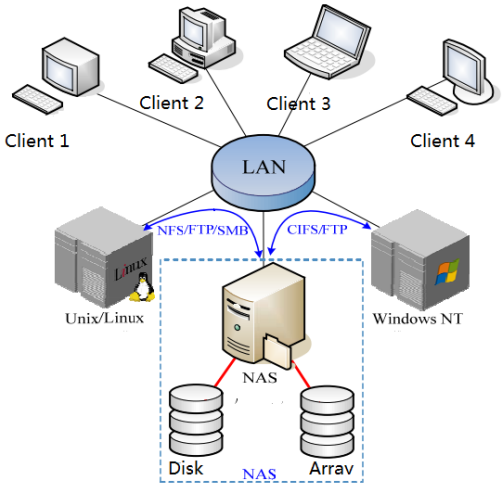

Fig.2 Schematic Diagram of Nas Network Topology

2. Research on File System of Information Security Evaluation Model

With the network speed, access data faster than the read speed from the local hard disk from the network node memory; and each node in the cluster memory can be gathered together to form a single node is much larger than memory, these premises makes Cooperative Cache become reality. Cooperative caching is to make full use of the cache on the client, so that the data access to a new level can reduce the number of actual disk data read and write, thereby improving the efficiency of the file system. In order to solve this problem, we need to design a uniform protocol. Generally speaking, the nodes in the cluster have the probability of failure, and the data in the file system may be damaged or lost in the process of the system. The failure of hardware or software will make the service provided by the system fail. In this case, continuing to ensure the availability of data, disaster recovery and recovery occurs when the fault becomes the main problem of data fault tolerance and high availability of the system, the CIFS protocol diagram shown in Figure 3.

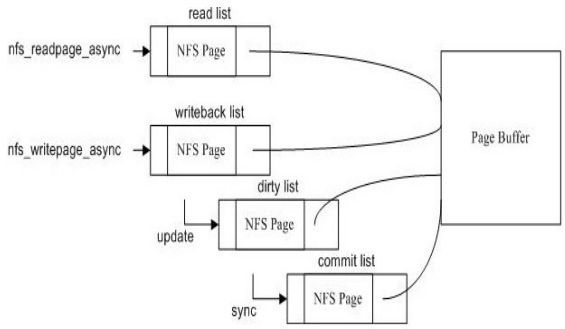

Fig.3 Schematic Diagram of Cifs Protocol

For a parallel file system in a distributed environment, file metadata also includes the following [6]. The difference is that the physical distribution of the file includes not only the location of the files on the disk, but also the location of the disks in the system. Therefore, metadata information should be more. In order to improve the performance of the I/O file to read and write file data parallel file system is usually not stored in a single device, but these data will be evenly distributed across multiple nodes, even if it is separate file slice storage may. It is the most important metadata in the parallel file system to describe the parameters of the data location or file segmentation. In order for an application to transparently use a parallel file system, it is necessary to manage the data that has been split. One of the key elements in the design of parallel file system is the management of metadata.

Secondly, the access performance of metadata affects the performance of parallel file system. In the parallel file system, the access of metadata is very frequent, and the metadata file is usually very small. When the metadata and user data are stored separately, the design logic is clear, the metadata access flow and the data access flow are separated, and the control is simple. Distributed metadata management can achieve good access parallelism, and easy to achieve load balancing. But its control and implementation of complex, need to maintain consistency of metadata, the overhead is relatively large, good consistency protocol design reduces this overhead, improve the performance of metadata is the main research content, metadata structure diagram is shown in Figure 4.

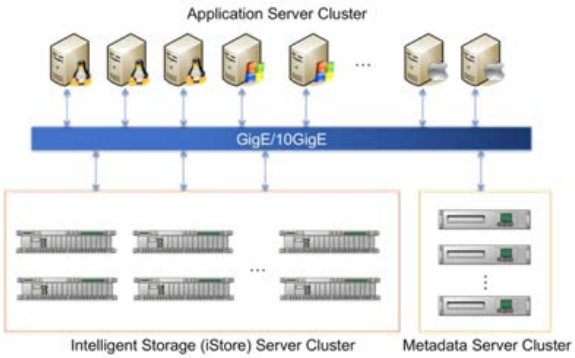

Fig.4 Schematic Diagram of Metadata Storage Structure

NAS is difficult to avoid the appearance of “information island”, if there is more than one NAS in an enterprise, is likely to be in a NAS data also appear in another NAS, and at the same time, all NAS do not communicate with each other, mutual sharing of resources. A single NAS can be used on the market structure of commercial PCRAID card + multiple hard drives, using RAID5 algorithm, so that a single NAS capacity can reach to T units, a plurality of NAS storage system can form a massive. The architecture of the system is shown in Figure 5.

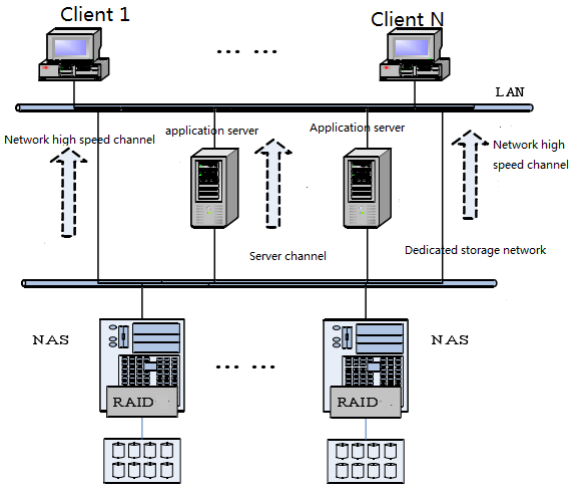

Fig.5 Cluster Nas System Structure Diagram

3. Design of Nas System

The NAS system is in an operating system platform file system level by SMB/CIFS, NFS and FTP protocol to provide file sharing services between heterogeneous systems; and make users and user groups, shared folders, file system and logical volume resources, user quota, and user authentication, user access control management of the shared folder the state monitoring system of storage; at the same time, the normal operation of maintenance services, to provide relevant and timely log records and e-mail warning system. The NAS system can be deployed to provide open file sharing services for the entire Internet in the public network nodes, deployed in the internal network node enterprises can, especially the active directory domain within the enterprise internal organization of enterprise internal network provides limited file sharing service [8]. The active directory domain by the main domain controller is responsible for the management and maintenance of domain users and groups, as well as related user authentication, active directory domain for NAS system Samba service sharing mode. NAS system is a shared service and storage management system. The NAS system mainly realizes the user and group management, management of the shared folder, logical volume resource management, user quota management, Samba service management, NFS service management and FTP service management and other functions. The core of the system is NAS storage management, service and other NAS system construction elements and resources sharing management. Such as providing shared services network file system is based on external system storage management system, we can use the software system of open source or commercial building external systems rely on NAS system.

When the upper down command, first search in the cache content already exists, if present, will immediately return to the corresponding content, if the requested object is not in cache, the command sent to the lower level of CNS (Client Name Space) module, and according to a certain algorithm, reading part in order to improve the system, the cache hit rate, and improve the performance of the performance. The same SC module (Server Cache), is mainly located in the storage node cache, the working principle of CNS is similar to. The CNS module (Client Name Space) and SNS (Server client module namespace Name Space) server namespace module, CNS and SNS is the core unit of file system metadata management and metadata are designed in this paper is implemented in most of the two modules [9]. CNS is mainly responsible for the above CC layer down command analysis, find out the access object which belongs to a storage node, and when SNS receives the SN pass up the order, carries on the analysis to find out the real access to the command, the command of physical objects, and will continue to upload commands to the SC layer. The CN module (Client Network) client network module and SN module (Server Network), is mainly responsible for all the command or response were packed, finally through the network to send out. Local FS module (Local File System) is a storage server's local file system, finally all commands will be executed in the layer, and through hardware heterogeneous local file system

layer can shield the entire storage server, providing a good scalability.

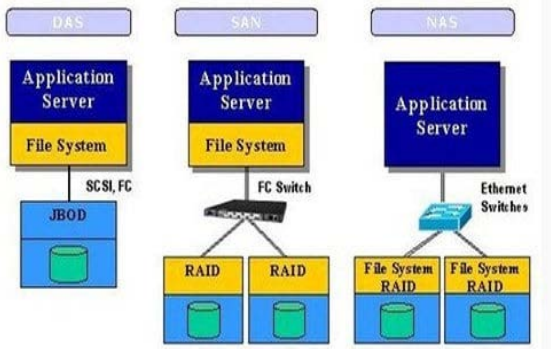

Fig.6 Schematic Diagram of Nas System

The whole system is not responsible for the metadata server, metadata of the whole system is made by different local configuration information stored on the server are integrated into a global configuration information. Each storage server is only responsible for the management of their own local configuration information, the application server in the first connection storage server, will automatically request global configuration information, which will construct a complete metadata tree. The metadata NAS cluster file system is divided into 2 levels, respectively, by the NCFS metadata management module at the bottom and top of the metadata management host. An example is given to illustrate the hierarchical model of NCFS metadata from theory and practice. The hierarchical model of metadata diagram as shown in Figure 8, first explain the 2 unique concept here: local node, node distribution; assumption in the logical view (see user view), node 2 is the node of the B node; if 2 nodes corresponding to the physical node is B on the physical node the child nodes, and control sub attribute node 2 (mainly refers to the metadata information related to the safety of property and physical control) corresponding to the same B node, the node 2 is called the local node, on the contrary, it is called distribution node. The metadata manager of the NAS file system is responsible for managing the metadata of the distributed nodes. For a local node, its primary metadata is managed primarily by the host file system. Through the coordination of the host file system and NCFS to form a complete metadata tree, and the whole system has the global name space, still to view the user logic 8 as an example, in this case, if the root node, a, B, C and 5 node distribution node, D, 1, 2, 3 4 and 6 nodes is the local node, to assume the root node and the a node belonging to the storage server 1, B and C nodes belonging to the storage server 2, and 5 nodes belonging to the storage server 3, configuration information, will be in the 1 configuration information stored in the metadata server stored in the root node and the a node in the same way, file service 2 containing B and C node configuration properties, and the storage server 3 contains 5 node configuration file information, build a node data structure, configuration information of each node can then heartbeat manager each storage server receives the configuration information, and sends his own configuration information storage server and then form a unified global configuration information, through the global configuration file system, each storage server is to construct a unified global metadata tree [10].

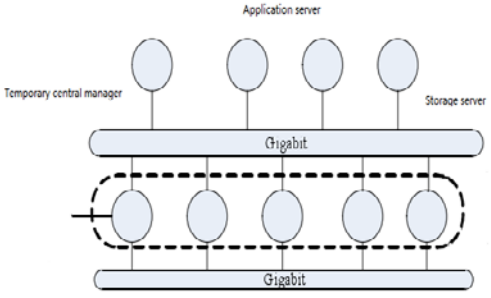

Fig.7 Schematic Diagram of the Architecture of Ncfs System

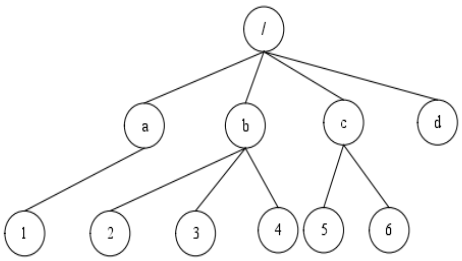

Fig.8 Schematic Diagram of Hierarchical Model of Metadata

Father attribute weighted value: creating objects of the parent node the server where the father attribute is 1.2, the other 1 nodes, in this way, can guarantee the parent node where the server has a priority, so as to facilitate the data correlation between father and son nodes; storage capacity weighted value: consider a proportion of storage capacity set the value of the current node; storage of spare capacity: the storage node idle capacity; the total idle storage capacity: total idle current storage capacity; load weighted value: considering the severity of the CPU load and a proportion of the value set. Because the parallel strategy, in order to achieve a large number of read and write parallel strategy, so this part of process until after the parallel access strategies in detail [11]. Rename command is the most complex in the entire command metadata basic operation, mobile data in the same file system implementation is usually the rename operation, in the system, because the global namespace, the user does not know in which files are stored on the storage server which has a specific position, therefore, when the user moves for an object, probably from the storage server attached to another storage server, therefore, in order to minimize the invalid data in the mobile network, typically, not real data across the server mobile, just by adding a distribution node or modify the metadata information distribution node of the old inside, so as to complete the rename operation, data processing flow diagram as shown in Figure 9.

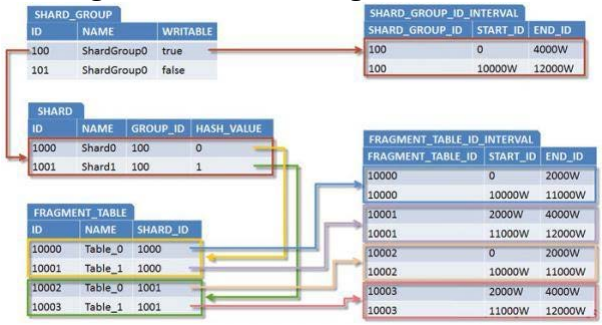

Fig.9 Metadata Processing Flow Diagram

4. Implementation of Metadata Management in Information Security Evaluation Model

In the disk array, by allowing several disks in parallel so as to improve the performance of I/O system, at the same time, the use of certain redundancy, to increase the security of the system, such as in RAID5, when there is a disk failure, can check the failure recovery disk data using redundant disk. In view of the idea of RAID, in the NCFS system we introduced the idea of RAID, we realize the idea is the hot files respectively stored in different storage node, so when the hot file access the application server, will first visit the judged data blocks belong to the storage node, and then modify the offset, and finally to the store the corresponding access node. Step one: the hot file judgment and segmentation (1) when the storage node is running, by which judge the current hot module file for the hot files; (2) the hot files in judgment, calculated to provide a storage node parallel service, calculated by the heartbeat protocol module in other storage nodes CPU minimum of load N-2 storage nodes (N is the total number of storage nodes), if the whole system there are only 2 storage nodes are automatically set another storage node can provide parallel services; (3) the documents are not allowed to temporarily lock, writing to the file, then the file. Storage to storage nodes in N-

1. The storage node 1 through the heartbeat module, respectively, second, N+1 block, 2N block, 3N-1 block in the 4N-2 block, and so on to calculated second, third, fourth, N-2 of the storage node. To put a file stored separately to the 4 storage nodes as an example, the distribution of the final document as shown in figure 10.

The total number of RAID nodes: the file is stored separately to several storage nodes, combined with the use of this parameter and the current RAID node number, when the RAID node points for a total of 0 or 1, said the document did not adopt the parallel access strategy, the RAID node of the current number parameter must be 0. The current RAID node number: for parallel file, local storage in several parts of the file in parallel file note sorting is based on the beginning of 0, 0 is the first storage node, 1 said second storage nodes, Tongli turn down. Note: in order to support future expansion of RAID algorithm is more likely to represent the RAID level, adding a new parameter, it is also possible to reduce the amount of communication between modules is possible through the heart, the parallel attribute into a parameter, based on the identification of some bits of the parameters to judge the level of RAID, RAID node the total number of nodes in the current number, RAID. In the application server, when the user requests to read file requests, IFS generates a read request, read and fill some parameter in the command, and then ordered to send the CC layer, CC layer when accepting orders, find the command request data from the cache, if present, will immediately return the requested data. If not, the command is sent to the CNS, when the CNS received the order, immediately in the metadata tree search read request object, if the read request object is a node metadata tree, and parallel nodes are calculated to ask parallel operation, data block which belongs to a server, and according to the number RAID, offset correction, if the requested data block is the first memory, do not need cheap correction, if the first storage node is then corrected Should the amount, to the storage node can correctly locate the data block, and then CNS the command sent to the CN layer and CN layer through the TCP/IP protocol to send commands to the storage node, when the storage node SN receives the command, then the command sent to the SNS layer, SNS layer according to the user logic in the command in the metadata tree when the search to search the corresponding metadata node, then modify the command request object name to the real file real corresponding to the local file system, then the command is sent to the SC layer when the SC layer receives the command, first find the cache, if the command request data in cache, and then return to the command data [12].

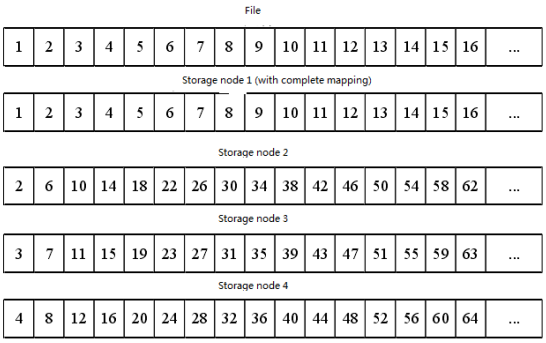

Fig.10 Schematic Diagram of Parallel File Distribution

5. Conclusions

In this paper, the author researches on the construction of information security evaluation model based on information ecology. The traditional static security defending system, such as firewall, data encryption, identification authentication, admission control and operate system reinforced technology, can't completely satisfy the need of the security condition. According to the complexities and diversifications of the attack methods and means, the intrusion detection technology, become a new hot issue in the field of the information security. Combining the advantages of traditional NAS and SAN system, aiming at the limitation of the above NAS and SAN system and the lack of a NCFS system based on SAN, NAS and SAN have both advantages and disadvantages of the two techniques can overcome the system design, system structure is used

for SAN storage network, and each storage node using NAS equipment, using NAS cluster technology, using multiple NAS to form a large capacity, high availability, high performance and high expansion of storage system. The experiment result shows the proposed method can improve the overall system performance substantially. From several basic functions, static performance, reliability and other aspects of quantitative specification of the functional verification and testing of the NAS system, and from the two aspects of shared services and storage management functions and other commercial NAS systems or products are analyzed, given the NAS system in this paper is a cheap and practical systems.

References

[1] Mehran R, Oyama A, Shah M. Abnormal abnormal environment behavior detection using social force model. 2009:935-942.
[2] Popoola O P, Wang K. Video-Based Abnormal Human Behavior Recognition-A Review. IEEE Transactions on Systems Man & Cybernetics Part C, 2012, 42(6):865-878.
[3] Devroye L, Wise G L. Detection of Abnormal Behavior Via Nonparametric Estimation of the Support. Siam Journal on Applied Mathematics, 1980, 38(3):480-488.
[4] Li C, Han Z, Ye Q, et al. Visual abnormal behavior detection based on trajectory sparse reconstruction analysis. Neurocomputing, 2013, 119(16):94-100.
[5] Wang B, Ye M, Li X, et al. Abnormal abnormal environment behavior detection using high-frequency and spatio-temporal features. Machine Vision & Applications, 2012, 23(3):501-511.
[6] Xiong G, Cheng J, Wu X, et al. An energy model approach to people counting for abnormal abnormal environment behavior detection. Neurocomputing, 2012, 83(7):121-135.
[7] Ermis E B, Saligrama V, Jodoin P, et al. Motion segmentation and abnormal behavior detection via behavior clustering. 2008:769-772.
[8] Riboni D, Bettini C, Civitarese G, et al. Extended Report: Fine-grained Recognition of Abnormal Behaviors for Early Detection of Mild Cognitive Impairment. 2015, 199(3):149-154.
[9] Zhang Y, Qin L, Yao H, et al. Abnormal abnormal environment behavior detection based on social attribute-aware force model. 2012:2689-2692.
[10] Wang B, Ye M, Li X, et al. Abnormal abnormal environment behavior detection using size-adapted spatio-temporal features. International Journal of Control Automation & Systems, 2011, 9(5):905-912.
[11] Mousavi H, Mohammadi S, Perina A, et al. Analyzing Tracklets for the Detection of Abnormal Abnormal environment Behavior. 2015:148-155.
[12] Bussler L, Davis E. Information Systems: The Quiet Revolution in Human Resource Management. Journal of Computer Information Systems, 2016, 42(2):17-20.