

# A Research Paper of Well Developed Safekeeping Issues Implement with Analytic Approach in Distributed File System

Ajmal Faizy<sup>1</sup>

<sup>1</sup> School of Technology & Sciences,  
Alakh Prakash Goyal Shimla University,  
Shimla (HP)

Mr. Aman Kumar<sup>2</sup>

<sup>2</sup> Schools of Technology & Sciences,  
Alakh Prakash Goyal Shimla University,  
Shimla (HP)

**Abstract**— We have developed a plan to check arrange joined limit systems against various sorts of attacks. Our system uses strong cryptography to conceal data from unapproved customers; someone expanding absolute access to a circle can't get any significant data from the structure, in addition, fortifications should be conceivable without allowing the super client access to decoded data. While renouncing of-organization attacks can't be envisioned, our system recognizes delivered data. The structure was made using a rough plate, and might be fused into typical report systems. We notice the arrangement and security tradeoffs such a coursed archive structure makes. Our arrangement watches against both remote interlopers and hence the people who increase physical access to the plate, using just enough security to thwart the 2 sorts of attacks. This security is regularly practiced with little discipline to execution. We watch the wellbeing errands that are principal for each very action, and demonstrate that there's nevermore any clarification to not consolidate strong encryption and check in arrange report structures. Conveyed record frameworks (DFS) give a crucial reflection to area straightforward, perpetual capacity. they permit conveyed procedures to co-work on progressively sorted out information past the life-time of every individual procedure. the incredible intensity of the document framework interface exists in the unquestionable truth that applications don't should be changed so on utilize appropriated capacity. Then again, the general and simple record framework interface makes it famously hard for a circulated document framework to perform well under a determination of changed remaining burdens. This has cause the present scene with kind of famous dispersed document frameworks, each custom-made to a particular use case. Early circulated recording framework s simply executes document framework approaches a far away server, which limits versatility and strength to disappointments. Such confinements are enormously decreased by present day procedures like conveyed hash tables, content-addressable capacity, disseminated accord calculations, or eradication codes. inside the daylight of up and coming logical information volumes at the Exabyte scale, two patterns are rising. In the first place, the already solid plan of dispersed record frameworks is decayed into administrations that freely give a various leveled namespace, information get to, and conveyed coordination. Besides, the isolation of capacity and figuring assets respects stockpiling engineering during which each register hub likewise takes part in giving constant stockpiling.

**Keywords:** *Distributed system; Hadoop; Blobseer; concurrency; speculation.*

## 1. INTRODUCTION

In the front line world, there is a developing necessity for joint exertion amongst topographically segregated social events. Stages and businesses that assist such joint exertion are in improbable intrigue. Flowed Conferencing System

(DCS) is a push to supply a segment to clients to work supportively frequently in an appropriated circumstance. The device depends upon an incredible, continually unfold shape and gives get the threat to manage document organization, cautioning, invulnerable correspondence and gadgets for agreeable choice making [1]. DCS offers central scattered synergistic contraptions (content apparatuses, outlines editors, etc) and can in addition toughen untouchable applications. The designing of DCS is deliberate to be flexible. Another imperative association goal is adjustment to internal disappointment. The device is predicted to manipulate type out dissatisfactions and shape crashes by using restoring from fortifications and arriving at quite a number desires for the most bleeding area information. Archive the board is vital in any exceeded on system. Record constructions in appropriated situations want to deal with problems now not considered elsewhere. A key request is the way are reviews and inventories displayed to the purchaser [2] Another request is what takes place when a couple of clients regulate a related archive at the equal time [2]. It is additionally critical to make certain that records is not rendered blocked off with the aid of the mistake of a few structures [3]. Record approvals are in like manner essentially logically pissed off [2]. Finally, execution have to be one of the desires of a dispersed file shape [2] The quintessential interpretation of (DCS v1) gave honestly constrained corporations to targeted endeavors. One of its drawbacks used to be that it had now not a lot of employments and solely clients in the voter occupation ought to pick selections [1]. Furthermore, it relied upon UNIX approvals for safety [5] The ensuing shape (DCS v2) offers greater groups and higher correspondence locals. Likewise, it helps all the moreover throwing a vote casting structure framework and confined Role Based Access Control (RBAC) [4]. DCS v2 modules have higher help for archive/object types. The massive agencies gave via DCS are depicted under [6] Distributed File System (DFS) offers document dealing with administrations to DCS clients. It is supposed to allow document sharing and simultaneous get admission to of documents. It moreover offers straightforwardness [2]. Furthermore, it utilizes the Access Control Service gave with the aid of DCS to put in force file get to authorizations [4] Conference Control Service (CCS) This module manages the Collaborative Group (Cog). It is the predominant assist of be impelled and fires up every different module. It makes use of invulnerable advising to empower customers to login and communicate with organizations. This module additionally

handles workout routines like splitting and becoming a member of events/Cogs/goals, receives the risk to manage requests and contain consumer requests. It is obligated for making and eradicating Cogs Database Service (DBS): DBS continues up all tables in DCS space. It makes use of a Database Managements System (DBMS) as the backend. Tables are taken care of as to some diploma imitated, flowed databases and social tournament multicast is used to make sure inescapable consistency. Notice Service (NTF): NTF offers unusual tournament cautioning to enlisted customers. Despite positive events, NTF empowers clients to painting new events. NTF maintains up a global and shut by using database to organize occasions to enrolled customers, close by the transport approach Decision Support Service (DSS): DSS energizes the goals of troubles by way of a social event of human beings with the joint dedication in regards to them. It continues up selection positions consequently. It offers creation, exchange and execution of designs. In case a layout requires a vote amongst a terrific deal of customers, DSS will contact the customers, get their votes and return the end result Security is one of the traits of AFS. It makes use of a puzzle key cryptosystem to enhance an ensured channel amongst Vice and Virtue. The secret key is used with the aid of the two machines to set up a assembly key, which is used to sport format the secure RPC. The route towards maintaining the purchaser is consistently baffling. The exhibit used for this reason for existing, is gotten from the Needham-Schroeder exhibit [17]. An Authentication Server (AS) outfits the purchaser with suitable tokens. These are used to advance his/her character. Access manipulate data are used to manage approvals to reviews and files. The Vice document servers confederate files with archives so to speak. Records do not pass towards manipulate records. LBFS is anticipated for frameworks with low alternate velocity and excessive latencies [22]. LBFS works on the opportunity that a kind of an archive shares a good deal for all plans and purpose with its previous interpretation. It in like manner acknowledges that there are resemblances between data made through a similar application. The methods used via LBFS can be used recognized with the methodologies used by way of different coursed document constructions (like Coda) to enhance safety from prepare riding forces LBFS works by way of preserving up a outstanding save at each the customer and the server. Records are indifferent into variable measurement knots. As a long way as viable are directed through Rabin fingerprints, situation to decrease and furthest cutoff points. A Rabin novel imprint is the polynomial depiction of the records modulo a predestined unchangeable polynomial. Right when the low-demand thirteen bits of a zone's one of a form imprint proportionate a picked worth, the location consists of a breakpoint. Tolerating sporadic data, the regular piece dimension is  $2^{13} = 8192 =$  eight Kbytes. This association ensures that modifications to an irregularity have an effect on solely that piece and its neighbors. LBFS archives portions the use of their SHA-1 hash [24]. If the piece is reachable in each the server and the client, honestly its hash is sent. Something different, the whole rectangular is transmitted. All statistics despatched on the framework is compacted the use of gzip. LBFS offers similar assembly semantics as AFS. Records are flushed to

the server on close. LBFS makes use of ephemeral archives to execute atomic updates. All stays in contact with the archive occur on a quick report which is then renamed. This ensures synchronous creates can failing to carry about clashing reports. This is in checked multifaceted nature to NFS. The patron that shut the document closing will overwrite the moves of the others.

## 2. LITERATURE REVIEW

Writing Survey: As inspected by Pallickara et al. (2007) and Shehab et al. (2010), the critical examination issues in flowed structures are security moves close. The unprecedented fragments of passed on structure security look like affirmation, encryption, endorsement and system confirmation as commented by Anderson (2010). Then again the security the officials condition (Bai (2008)) which used to be established on single force systems is right now used with bundles shared obligations. The Appropriated System get the chance to control parts have been considered by Koshutanskai (2009) and the activity based access instruments have been discussed in detail by Chadwick et al. (2003). For expressive economy the term security is used to address the two its standard significance similarly as those thoughts passed on by the term security as commented via Seamons and Winsbotough (2002). An outline of dispersed framework design is typically given and utilized as a system for resulting examination. The significant security assaults issues, for example, spying, disguising and message treating (changing the substance of the message), replaying the message and refusal of administrations have been examined by Oppliger et al. (1999). Security Based on Authentication Shehab et al. (2010) have proposed a way check framework. On demand way disclosure estimation has been investigated to make talented spaces to securely deliver courses in the common condition. Pallickara et al. (2007) made a vehicle approach for following the openness of components in scattered systems. As inspected by Xiaoyong et al. (2011), heterogeneous scattered structures are fantastically significant in different applications, like stock articulation update systems, electronic trade planning structures, which need a significantly capable amalgam of approval, uprightness and protection. Xiaoyong et al. (2011) have excessively developed a significant security driven arranging designing. This strategy hasbeen delivered for Direct Acyclic Graph (DAG). The made thought capably surveys the trust of each center point the affirmation of remote client is an essential exploration domain in the appropriated systems. Critical arrangement issues are the cryptographic counts, synchronization and proportion of trust. A confirmed mystery word based approval with an accepted untouchable is proposed by Seung and Souhan (2006). A remarkable approval show, called Kerber OS is the base of this procedure. Security Approaches Based on Trust Li and Singhal (2007) has developed a trust based model for applications like P2P structures. Trust models expect huge occupation in the age of security structures in scattered applications. A widely inclusive D-S speculation based trust model (ExDSTM) has been made and executed by Jiang et al. (2012). Other D-S speculation models are executed by Huang et al. (2010), Wang and Sun (2009) and Yu and Singh

(2002). A dynamic and setting fragile trust based security part has been proposed and executed by Ding et al. (2012).[18] A peril the officials has been facilitated into security by using a trust model as proposed by Lin and Varadharaan. This model shows that the hazard the board can be applied to amplify the use of the circulated frameworks. The model has the utility to assess the trust, moreover.

Security Approaches Based on Policy Hamdi and Mosbah (2009) have developed a course of action based scattered structure security instrument. This procedure gives specific security approaches and self-sufficient of essential structure. This technique relies upon zone express language for affirmation, detail close by the execution of appropriated system security courses of action and approaches. Hamdi et al. (2007) discussed the certifiable coordination of security approaches with scattered systems. The security game plans are structured truly and maintained to the dispersed system thusly. Yao and Fidelis (2003) have developed a methodology based framework.

Security Approaches Based on Quorum As discussed by Zhou et al. (2010), greater part based security systems are unimaginably used in handling the issue of data consistency in passed on issue open minded structures. The Intrusion – Tolerance Quorum System [ITOS] of crossbreed time model taking into account Trust Timely Computing Base (TTCB) has been proposed and executed by Zhou et al. (2010). A vocation based access control model has been made by Tomoya and Makoto (2000). [21]The Role Ordering (RO) schedulers are introduced close by synchronization control reliant on significance of occupations given out to the trades.

### 3. PROBLEM FORMULATION and PROBLEM STATEMENT

We observe under positive problems and difficulties in the enchantment of tightly closed circulated frameworks.

1. Advancement of strategy which surmised the safety stage in a framework.
2. Investigating the framework security.
3. Proposing the protection measurements.
4. Joining the methodologies like Cryptography and so on for impervious circulated statistics Correspondence.
5. Utilization of core product in conveyed framework security.
6. Utilization of internet advantages in safety purposes. In a Hadoop bunch condition, records is organized any vicinity belongings are accessible, upheld by using massively parallel calculation. This is very special in relation to the unified engineering of a accepted social facts store. Hadoop's appropriated sketch makes a state of affairs that is highly defenseless in opposition to assault at specific focuses, as an alternative of the unified storehouses that are strong and less difficult to verify. Information interior Hadoop bunches is liquid, with a number of duplicates shifting to and from quite a number hubs to assurance extra and flexibility. [19] Information can likewise be reducing into portions that are shared over more than a few servers. These characteristics encompass new intricacy, and request an alternate way to deal with records security.

### 4. OBJECTIVE

The main principle objective or goals of safety in DFS framework are:

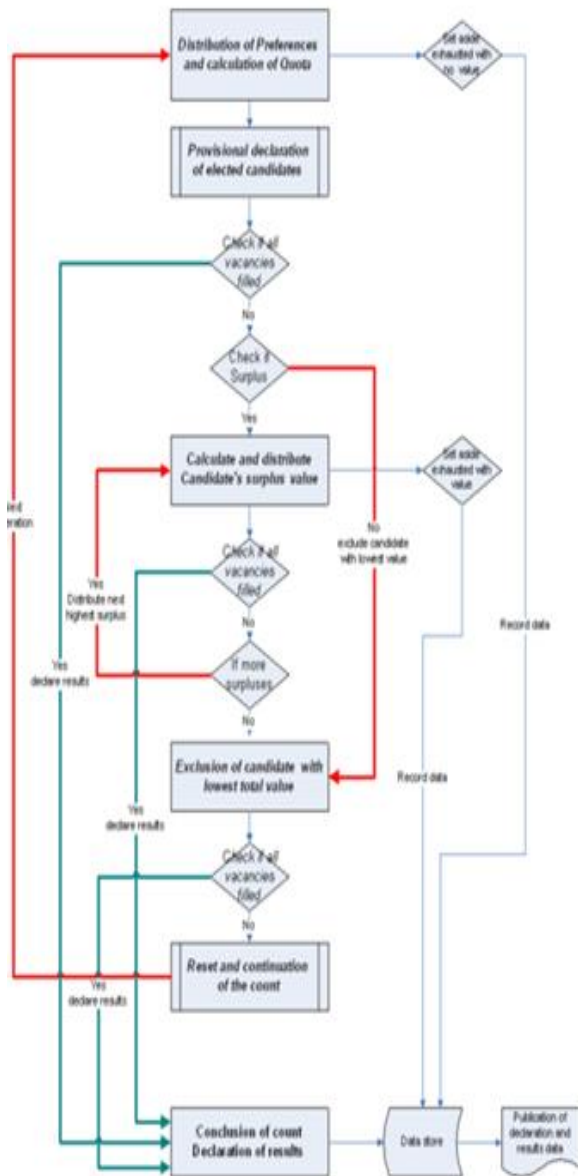
- The evidence scheme should give a consistent name space.
- Files and records should be section clear and province self-ruling.
- Concurrency control should authorize customers to alter as well as records, without losing changes made by any customer.
- The steadiness semantics should be obvious. Record migration and replication must be reinforced to improve openness and execution.
- Novel servers must be allowed to join the social event without shutting it down. Development of servers should not alter customer experience belligerently.
- The record structure should give an interface to empower customers and applications to convey beneficially.

### 5. RESEARCH METHODOLOGY

The general technique for this investigation was to perform tests where we can control the earth and factors that could influence the result of the examinations. Further, we play out a subjective examination where an investigation would yield information that would not be helpful, as the outcomes would prompt a probabilistic answer (i.e., totally, in part or not satisfying the perspectives). There are other methodological methodologies that were thought about, at the end of the day, they sometimes fell short for our necessities. Area 0 location why these methodologies were not applied in more detail.

#### 5.1 Shared trial settings for Scalability and Performance

The preliminary setting for both adaptability and execution was run on the working structure CentOS on machines with Intel Xeon W3550 (Intel, 2009) and 24GB RAM in a non-GUI condition. For all investigations, the item adventure go-ipsfs v0.4.13 (Benet, 2014a) was used for the record moves. Further, the IPFS adjustment of the IPFS center points was also v0.4.13. The exploratory plans for IPFS share the identical environmental diversion, where arrange transmission limit hindrances are executed, and different centers are run on one machine. While picking the replication apportionment, the python 3 library subjective was used, or even more expressly, unpredictable model (Python Software Foundation, 2018). The completed imperatives are that all centers are limited to 100 megabits for consistently (100 Mbit/s). This control was picked with the motivation that the Swedish government hopes to meet the target that 95% of private and companions affiliations should have at any rate 100 Mbit/s by 2020 (Regeringskansliet, 2016). In like manner, these requirements were sensible since by and large private and companions areas will have 100 Mbit/s inside 2 years, as of forming this examination. These obstacles are completed by using a



mechanical assembly called stream. The gathering contains various center points, where at any rate one center points fill in as sections for moving toward requesting. All center points in the gathering are totally related, inferring that all centers think around each other and can interface with any center in the pack. This is a reasonable setting for a local pack, for instance, a gathering passed on at an association, since an association would more likely than not orchestrate a set number of centers and in a perfect world, these centers would think around each other.

## 5.2 Method Implementation

This passage portrays the execution subtleties and how the presentation tests are completed. Trial subtleties in this methodological procedure for execution are to direct a test. The examination is an ecological reproduction performed on IPFS, NFS (adaptation 4) and ext4. The test settings are imparted to the adaptability explore and depicted in area These are the factors utilized in the investigation that differs between arrangements.

**Record framework :** The document framework that is utilized for the examination, the three potential arrangements are ext4, NFS and IPFS

**Store utilization:** If reserve is dynamic or inert during the examination. As ext4 doesn't bolster it, it is consistently dormant.

**Replication utilization:** If the documents utilized for the analyses can be found on more than one hub. Just IPFS has local help for it, in this manner it is just present in the IPFS try. It is constrained to replication on 10 hubs out of 100.

There are several risks that are associated with distributed file systems; These risks consist of Leakage, which includes Eavesdropping, Tampering which includes Masquerading, Message Tampering

```
#include "ns3/core-module.h"
#include "ns3/netanim-module.h"
#include "ns3/internet-module.h"
#include "ns3/point-to-point-module.h"
#include "ns3/applications-module.h"
#include "ns3/point-to-point-layout-module.h"
// Network topology (default)
using namespace ns3;
NS_LOG_COMPONENT_DEFINE ("Star");
int
main (int argc, char *argv[])
{
// Set up some default values for the simulation.
//
Config::SetDefault ("ns3::OnOffApplication::PacketSize",
UIntegerValue (137));
??? try and stick 15kb/s into the data rate
Config::SetDefault ("ns3::OnOffApplication::DataRate",
StringValue ("14kb/s"));
// Default number of nodes in the star. Overridable by
command line argument.
uint32_t nSpokes = 8;
CommandLine cmd;
cmd.AddValue ("nSpokes", "Number of nodes to place
in the star", nSpokes); cmd.Parse (argc, argv);
NS_LOG_INFO ("Build star topology.");
4 PointToPointHelper pointToPoint;
pointToPoint.SetDeviceAttribute ("DataRate", StringValue
("5Mbps"));
```

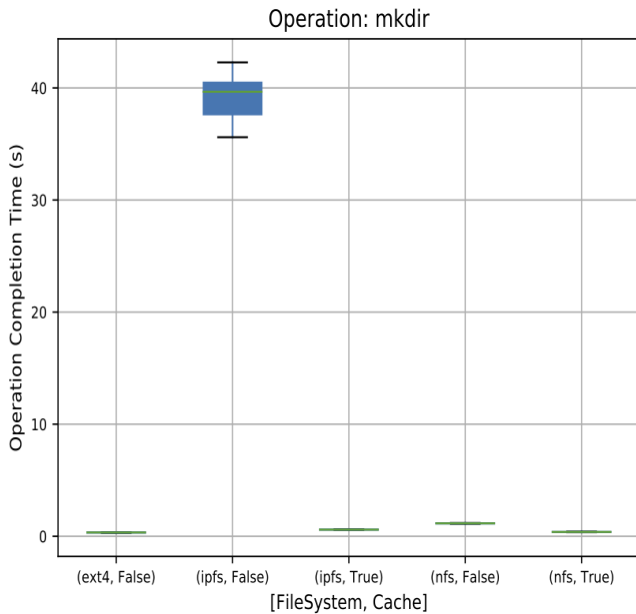


Figure Completion time in seconds for Make directory with file system and cache

```

pointToPoint.SetChannelAttribute ("Delay", StringValue
("2ms"));
PointToPointStarHelper star (nSpokes, pointToPoint);
NS_LOG_INFO ("Install internet stack on all nodes.");
InternetStackHelper internet;
star.InstallStack (internet);
NS_LOG_INFO ("Assign IP Addresses.");
star.AssignIpv4Addresses (Ipv4AddressHelper ("10.1.1.0",
"255.255.255.0"));
NS_LOG_INFO ("Create applications.");
uint16_t port = 50000;
Address hubLocalAddress (InetSocketAddress
(Ipv4Address::GetAny (), port));
PacketSinkHelper packetSinkHelper
("ns3::TcpSocketFactory", hubLocalAddress);
ApplicationContainer hubApp = packetSinkHelper.Install
(star.GetHub ());
hubApp.Start (Seconds (1.0));
hubApp.Stop (Seconds (10.0));
Create OnOff applications to send TCP to the hub, one on
each spoke node.
OnOffHelper onOffHelper ("ns3::TcpSocketFactory",
Address ());
onOffHelper.SetAttribute ("OnTime", StringValue
("ns3::ConstantRandomVariable[Constant=1]"));
onOffHelper.SetAttribute ("OffTime", StringValue
("ns3::ConstantRandomVariable[Constant=0]"));
ApplicationContainer spokeApps ;
for (uint32_t i = 0; i < star.SpokeCount (); ++i)
{ AddressValue remoteAddress (InetSocketAddress
(star.GetHubIpv4Address (i), port));
onOffHelper.SetAttribute ("Remote", remoteAddress);
spokeApps.Add (onOffHelper.Install
(star.GetSpokeNode (i)));
} spokeApps.Start (Seconds (1.0));
spokeApps.Stop (Seconds (10.0));
NS_LOG_INFO ("Enable static global routing.");
    
```

```

// Turn on global static routing so we can actually be routed
across the star.
Ipv4GlobalRoutingHelper::PopulateRoutingTables ();
NS_LOG_INFO ("Enable pcap tracing.");
// Do pcap tracing on all point-to-point devices on all
nodes.
pointToPoint.EnablePcapAll ("star");
NS_LOG_INFO ("Run Simulation.");
Simulator::Run ();
Simulator::Destroy ();
NS_LOG_INFO ("Done.");
return 0;
}
    
```

and Replaying, and Vandalism which includes Denial of Service. Each risk is described in detail in Coulouris *et al.* (2011, p. 466-467), and these are risks associated with distributed systems, not only distributed file systems.

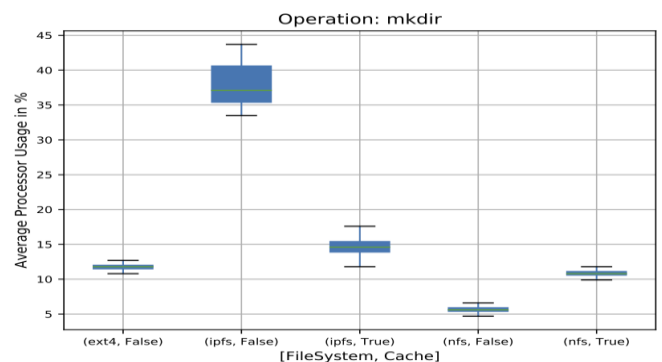


Figure Processor usage in percent for Make directory with file system and cache

**Leakage** – Leakage refers to the risk of having unauthorized users gaining access to classified information via a sort of leak in the organization, for example a whistle blower or a data leak.  
**Tampering** – Tampering is the risk of having unauthorized party editing/altering information that said party should not be able to edit or alter.  
**Vandalism** – Vandalism is when an unauthorized party actively interferes with the operation of a system without any

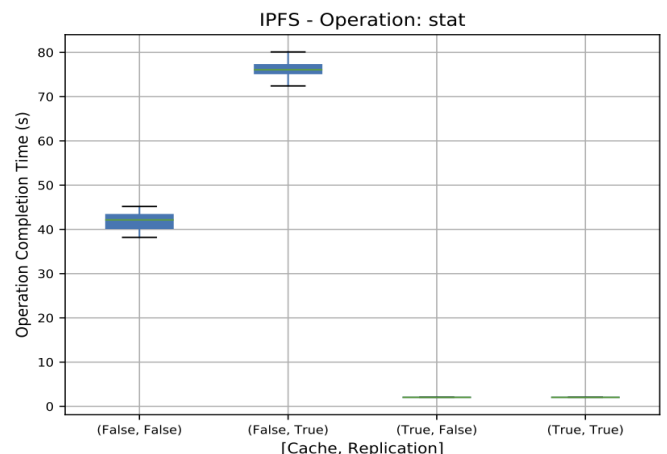


Figure Completion time in seconds for Copy with file systems and cache. This graph is the gain to themselves. same as Figure 2.

**Eavesdropping** – Eavesdropping is the unauthorized copying of messages being sent between two parties.

**Masquerading** – Masquerading is when a malicious entity is assuming the identity of another principal to send messages with.

**Message Tampering** – This is the act of intercepting messages being sent, and then altering them before sending them on to their destination.

**Replaying** – Storing the intercepted messages to use at a later date, for example could be used for replaying messages for bank transactions. These intercepted messages work well even for authenticated and encrypted messages.

**Denial of Service** – Flooding a channel with messages in order to overload it and take it down and prevent others from accessing it.

**Distributed Denial of Service** – Distributed Denial of Service is very similar to a regular Denial of Service. The big difference between the two is the magnitude of the attack possible. A Distributed Denial of Service attack makes use of entire networks of compromised devices to flood channels with much more traffic than is possible with a regular Denial of Service.

**IPFS and NFS** : A qualitative analysis on both IPFS and NFS is performed, and then compared to the baseline, and graded in Table 4, on how they handle the risks, or if they possibly make it worse.

**Analysis of Security related transparency:** The following transparencies are important when it comes to securing a system. When securing a system, it should not add any more steps than necessary for the user. It should also not cause any issues in operation, such as lowering performance to the point where it is noticeable to the user.

Therefore, the following transparencies will be analyzed in regard to how they are currently handled in both NFS and IPFS, and any planned solutions to improve it.

- Access Transparency
- Migration Transparency

**Access Transparency** : In regard to security this means that the resource in question should be able to be accessed even while being secured, without having to add extra steps for the users. Ideally the user should not have to be aware that the item they are accessing is secured at all.

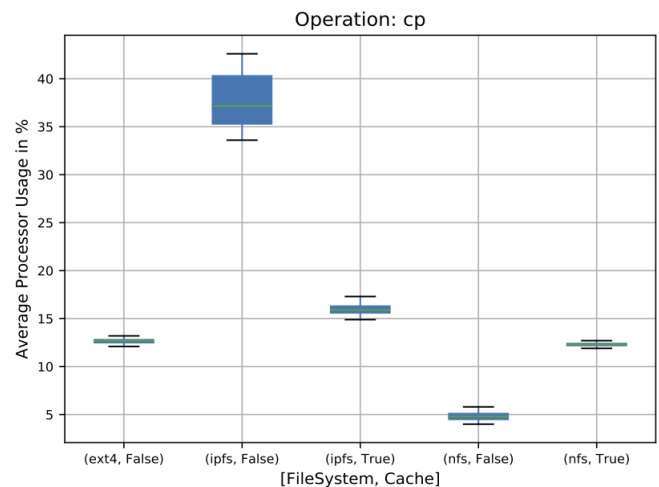
**Migration Transparency:** Migration Transparency in regard to security means that users should be able to move around the system and be able to move resources that they have permissions for, without being negatively affected by the chosen security implementations.

## 6. RESEARCH METHODOLOGY

**Figure** Completion time in seconds for Stat Operation in IPFS with cache and replication DFS gives a uniform call space to all information inside the gathering. Actually, it's far potential to increase it to provide a international namespace. In this regard, it's far like Coda. The subsequent purpose is completed by means of giving a File Information Table (FIT). [22]The FIT goes approximately as a mapping desk and

interprets among the clever call of the file and its actual region. The everlasting forming framework in DFS ensures

that simultaneous adjustments made to a report don't overwrite one another. Changes made by clients are spared as new paperwork. This ensures composes don't meddle with one another and data in no way lose modifications. DFS file consistency is unsurprising and configurable. Clients can see the most current modifications by means of indicating their approach. The semantics are very close to session semantics.



## 7. COMPARISON BETWEEN THE OLD MODELS AND THE PROPOSED MODEL:

The main comparison between old and proposed model are given in the following table:

Sr. No.	Old Model	Proposed Model
1	Security approaches are physically arranged in model proposed by Hamdi also, Mosbah (2009).	The Security approaches are naturally designed in the proposed model by FKBS execution.
2	The real based security model proposed by Shehab et al. (2010) employments manual arrangement of substances.	The Proposed model naturally outlines the status of elements utilizing distinctive trust esteems.
3	The Client protection isn't well actualized in the model proposed by the Theang et al. (2011).	The customer protection is kept up by Notoriety factor in the proposed model.
4	Seung and Souhan (2006) has proposed model that utilizations secret key based confirmation which is poor in the point of powerful security.	In the proposed model a safe framework has been created utilizing Notoriety Factor and Tri Facilities required for proposed work.

## 8. CONCLUSION

The motivation driving a spread report structure (DFS) is to permit different clients of really flowed PCs to share information and breaking point assets by utilizing a regular record framework. A normal methodology for a DFS is a mix of workstations and united PCs related by a region A spread record structure is a client/server-based application that grants clients to access and strategy data set aside on server as if it were isolated computer. Ideally, an appropriated archive system sifts through report and file organizations of an individual server into a [8]global library so remote data get to isn't region unequivocal yet it is vague from any client. All reports are open to all customers of the overall record system and affiliation is a dynamic and list based Dispersed

file framework is the new developed variety of record structure which is outfitted for overseeing data streamed across over different social occasions. Hadoop passed on chronicle framework (HDFS) is one of the most comprehensively saw known usage of DFS; paying little heed to the path that there are different executions like: Ceph, GlusterFS, and so forth. Purchase in with us to be told about our future article discharges which spreads centers will like:

- Future of DFS
- Brief presentation about DFS figuring
- Prologue to HDFS

#### REFERENCE

- [1] R. E. Newman, C. L. Ramire, and H. Pelimuhandiram, M. Montes, M. Webb, and D. L. Wilson, "A Brief Overview of the DCS Distributed Conferencing System," in *Proceedings of the Summer USENIX Conference*, Nashville, TN, June 1991, pp. 437-452.
- [2] A. S. Tanenbaum and M. Steen, *Distributed Systems: Principles and Paradigms*, Prentice Hall, Upper Saddle River, NJ, 2003. MA, 1997.
- [3] V. Manian, "Access Control Model for Distributed Conferencing System," M.S. thesis, University of Florida, Gainesville, FL, 2002.
- [4] L. Li, "File Services for a Distributed Conferencing System (DCS)," M.S. thesis, University of Florida, Gainesville, FL, 1995.
- [5] P. S. Yeager, "A Distributed File System for Distributed Conferencing System," M.S. thesis, University of Florida, Gainesville, FL, 2003.
- [6] R. Sandberg, D. Coldberg, S. Kleiman, D. Walsh, and B. Lyon, "Design and Implementation of the Sun Network Filesystem," in *Proceedings of the Summer USENIX Conference*, Portland, OR, 1985, pp. 119-130.
- [7] R. Srinivasan, "RPC: Remote Procedure Call Protocol Specification Version 2," Sun Microsystems, Santa Clara, CA, Request for Comments 1831, August 1995.
- [8] B. Callaghan, B. Pawlowski and P. Staubach, "NFS: Network File System Protocol Specification," Sun Microsystems, Santa Clara, CA, Request for Comments 1813, June 1995.
- [9] B. Callaghan, D. Robinson, R. Thurlow, C. Beame, M. Eisler, S. Shepler and D. Noveck, "NFS version 4 Protocol," Sun Microsystems, Santa Clara, CA, Request for Comments 3010, December 2000.
- [10] B. Callaghan, D. Robinson, R. Thurlow, C. Beame, M. Eisler, S. Shepler and D. Noveck, "Network File System (NFS) version 4 Protocol," Sun Microsystems, Santa Clara, CA, Request for Comments 3530, April 2003.
- [11] M. Satyanarayanan, "A Survey of Distributed File Systems," *Annual Review of Computer Science*, vol. 4, pp. 73-104, August 1990.
- [12] M. Satyanarayanan, "Scalable, Secure, and Highly Available Distributed File Access," *IEEE Computer*, vol. 23, pp. 9-21, May 1990.
- [13] M. Satyanarayanan, and M. Spasojevic, "AFS and the Web: Competitors or Collaborators," in *Proceedings of the Seventh ACM SIGOPS European Workshop*, Connemara, Ireland, 1996, pp. 89-94.
- [14] M. Spasojevic and M. Satyanarayanan, "An Empirical Study of a Wide Area Distributed File System," *ACM Transactions on Computer Science*, vol. 14, pp. 200-222, May 1996.
- [15] R. Needham and M. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," *Communications of the ACM*, vol. 21, pp. 993-999, June 1978.
- [16] Mar, Kheng Kok, et al. "Secure cloud distributed file system." *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2016.
- [17] Shetty, Madhvaraj M., and D. H. Manjaiah. "Data security in Hadoop distributed file system." *2016 International Conference on Emerging Technological Trends (ICETT)*. IEEE, 2016.
- [18] Mahmoud, Hadeer, Abdelfatah Hegazy, and Mohamed H. Khafagy. "An approach for big data security based on Hadoop distributed file system." *2018 International Conference on Innovative Trends in Computer Engineering (ITCE)*. IEEE, 2018.
- [19] Ramesh, D., Patidar, N., Kumar, G., & Vunnam, T. (2016, April). Evolution and analysis of distributed file systems in cloud storage: Analytical survey. In *2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 753-758). IEEE.
- [20] Botelho, Daniel Fiorese, Leonardo Willer de Oliveira, Bruno Henriques Dias, Camile Aredes Moraes, and Edimar Jose de Oliveira. "Distributed generation planning in distribution system with focus on reliability." In *2018 Simposio Brasileiro de Sistemas Eletricos (SBSE)*, pp. 1-6. IEEE, 2018.
- [21] Aldossary, Sultan, and William Allen. "Data security, privacy, availability and integrity in cloud computing: issues and current solutions." *International Journal of Advanced Computer Science and Applications* 7.4 (2016): 485-498.