NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 8, ISSUE 6, June. -2021

DEVELOPMENT OF AN ENHANCED CLOUD DEPLOYMENT MODEL FOR RESILIENT INTERNET DISASTER RECOVERY AND MANAGEMENT

Anigbogu Gloria N.
Department of Computer Science, Ebonyi State University, Abakaliki
*[1]gn.anigbogu@unizik.edu.ng

Ituma Chinagulm
Department of Computer Science, Ebonyi State University, Abakaliki
ichinagolum@gmail.com

Anigbogu, Sylavnus O.
Department of Computer Science, Nnamdi Azikiwe University, Awka
so.anigbogu@unizik.edu.ng

Karim Usman
Department of Computer Science, Benue State University, Markudi

ABSTRACT
Effective Internet disaster recovery and management is taking front burner consideration in organizations involved in Information Technology (IT) activities in order to safeguard their data and services on regular basis. When disaster, for instance knocks down the infrastructure of a single service provider, it usually will have ripple effect on the dependants that even a short period of down time can result in significant financial loss. Therefore, organizations may need disaster recovery plan or independent business continuity plan (IBCP) and backup policy that they can afford while at the same time achieving the primary aim of Recovery Point Objective (RPO) and Recovery Time Objective (RTO). This paper presents a hybrid of three Internet disaster recovery models of TAIJI, SECONDSITE and HS-DRT which can help organizations recover more quickly whenever Internet disaster occurred in their platforms. The system was developed using a combination of Structural System Analysis and Design Methodology (SSADM), Dynamic System and Development Methodology (DSDM) and Object Oriented and Design Methodology (OOADM). Java Enterprise (JEE) Technology in conjunction with NetBean1.0. Integrated Development Environment IDE were used at the front end, while MySQL server was used to implement the backend. The result obtained showed that a hybrid of Taji, SecondSite and HS-DRT which combined the features of; replication, duplication, server watch dog, check pointing, encryption, decryption, fragmentation, defragmentation and stateless services indicated an enhanced model for disaster recovery, since the deficiencies of each of those models hybridized were addressed through such features exhibited by the new model, which include; checksumming, compression and decompression

Keywords: Internet disaster; Cloud deployment; Disaster recovery, Business Continuity

INTRODUCTION
Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel or licensing new software. It extends information technology (IT) existing capabilities (Subashini and Kavitha 2011). Cloud computing paradigm is aimed at supplying virtualized and dynamically scalable resources. It also turns the computer into a virtual software or application image, which resides on some physical server in the cloud hosting environment (Velev and Zlateva 2011)
Organizations of all sizes require safeguarding of their data on regular basis, which makes disaster recovery and backup procedures, inescapable factors. Disaster recovery involves procedures to preserve continuation of business in case of a disaster (Brook *et al.*, 2015). Shaw (2018) opined that disaster recovery is a part of business continuity, which focuses more on keeping all aspects of a business running despite the disaster. And because IT systems these days are so critical to the success of the business, disaster recovery is a main pillar in the business continuity process.

Disasters often take place in vicinity of human livelihood. Disaster can either be natural or man - made. Most natural disasters come without warning and take lives of tens, hundreds and thousands of people. Natural disaster can destroy entire cities if precaution is not taken. The types are erosion, earthquakes, floods, tornadoes, hurricanes, lightning, landslide, tsunamis, wildfires and thunderstorms. The effects of natural disasters are very serious and the destruction caused may take a very long time to recover. The damages can equally take billions of dollars (Dimiter and plamena 2011). Some of the dangerous disasters in the history of mankind are Bhopal (India) gas accident of 1984, Chansala (India) mining disaster of 1975, September 11 terrorist attack (USA) 2001, Chernobyl (Russia) nuclear accident of 1986, Indian Ocean tsunami of 2004, Nepal earthquake (2005) and Fort McMurray (Canada) forest – fire (2016). Hurricane is one of the major natural disasters that affect countries like Canada, Bahamas, and USA etc. That of USA can be traced back since 1850's to 2019 and beyond with different name tag. The 2019 hurricane was named Dorian (Hauck, 2019).

Mohammad *et al.*, (2014) had noted that disaster recovery is a persistent problem in IT industries. It equally goes beyond IT industries and cut across every other industry. The society today depends mainly on computer system that even a short period of down time can result in significant financial loss or in some cases, can even put human lives at risk Wood *et al*., (2010)

In any business or organization, it is essential to have a backup plan in the event of a disaster which may happen at any time. A disaster recovery plan is a set process or a documented set of procedures which are created in order to retrieve the IT infrastructure of a business in the event of a disaster, and this is why it can also be referred to as an IT disaster recovery. A disaster recovery plan is a written document with specific steps and procedures set by the company or organization which should be followed when any kind of disaster happens. A good sample of a disaster recovery plan should state everything that should be done before, during and after a disaster occurs. And using the disaster recovery plan, data protection and service continuity are guaranteed for customers at different levels. Any enterprise main goal is business continuity which means resuming back services online after a disruption. Hence, Recovery Time Objectives (RTO) and recovery point objectives (RPO) are two important parameters which all the recovery mechanism should try to improve upon. And by minimizing RTO and RPO, business continuity can be achieved (Jangra and Bala, 2012)

Furthermore, Mohammad *et* a*l*., 2014) observed that disaster occurrence can affect the cloud, especially server locations. This problem is more crucial in cloud computing because cloud service providers (CSPs) have to provide the services to their customers even if the data center is down due to disaster.

In Nigeria, for instance many business concerns and relevant government agencies are yet to fully embrace this emerging technology (Cloud computing) in order to be able to enhance their profitability by reducing overhead cost on services, in the cause of hosting their services individually on the Internet. Furthermore, there is a palpable fear about the security of data of individual organizations when they are co- hosted in the cloud as the technology demands as well as associated disaster occurrences that are rampant today in the IT industry.

RELATED LITERATURES

We consider some of the related work done in disaster recovery and management in cloud computing environment

Caraman *et al.*, (2009) developed a model called Romulus. It is a disaster tolerant system based on kernel virtual machines. Romulus can tolerate failure in two situations; on the fly and failover. It uses new egress traffic buffer to replicate disk write after any checkpoint. It is operational within service provider premises even though their algorithms are accurate for disaster tolerant.

Again, Tamura *et al.*, (2008) designed a model called Kemari. It is a virtual machine synchronization for fault tolerance which provide a cluster system that synchronizes virtual machine for fault tolerance. Kamari used the primary backup approach so that any storage or network event that changes the state of the primary virtual machine must be synchronized in backup virtual machine. Unfortunately it is only operational within service provider premises.

Alazawi *et al.*, (2011) were of the view that Transportation and telecommunications play a critical role in disaster response and management in order to minimize loss of human life, economic cost and disruptions.

And therefore were concerned with developing emergency response systems for disasters of various scales with a focus on transportation systems which exploit ICT developments. The researchers, developed a system leveraging on Intelligent Transportation Systems (ITS) which include VANETs (Vehicular Ad hoc Networks), mobile and Cloud computing technologies in proposing an intelligent disaster management system. The system was intelligent because it is able to gather information from multiple sources and locations, including from the point of incident, and made effective strategies and decisions, that can propagate the information to vehicles and other nodes in real-time.

Nitesh and Bindu (2016) through their work noted that it was possible to realize a real time disaster management cloud where applications in cloud respond within a specified time frame. They were of the view that if a Real Time Cloud (RTC) was available; for the intelligent machines like robots, the complex processing can be done on RTC through request and response model. Therefore it would be possible to manage disaster sites more efficiently with more intelligent cloud robots without great loss of human lives waiting for various assistance at disaster sites.

Furthermore, Rodrigo De *et al.*, (2014) in their work observed that many corporations rely on disaster recovery schemes to keep their computing and network services running after unexpected situation, such as natural disaster and attacks. They also noted that corporations migrate their infrastructure to the cloud using the Infrastructure as a Service (IaaS) model. Hence Cloud providers need to offer disaster – resilient services. The work also provided guidelines for designing a data center network infrastructure to support a disaster – resilient IaaS Cloud. The guidelines described design requirements, such as the time to recover from disaster, and allow the identification of important domains that deserve further research efforts, such as the choice of data center site locations and disaster – resilient virtual machine placement.

Robinson *et al.*, (2014) in their white paper highlights Amazon Web Services (AWS) services and features that one can leverage for disaster recovery (DR) processes to significantly minimize the impact on data, system and overall business operations.

Chaowei *et al.*, (2017) in their work surveyed two frontiers of Big Data and Cloud computing. Again the work reviewed the advantages and consequences of utilizing cloud computing to tackling big data in digital earth and relevant science domains. From the work, the researchers were able to posit that:

i. Cloud computing and Big data enable science discoveries and application development
ii. Cloud computing provides major solutions for big data
iii. Big data, spatiotemporal thinking and various application domain drive the advancement of cloud computing and relevant technologies with new requirement.

Rajagopalan *et al.*, (2012) had earlier in their work developed a disaster tolerance system as a service, named SecondSite. SecondSite was designed to tackle three challenges which include; Reducing RPO, Failure detection and Service restoration using three techniques of Checkpointing, Quorum node and backup site

Zhu *et al.*, (2011) developed a disaster recovery system known as Taiji. Taiji is a Hypervisor – Based Fault Tolerant (HBFT) prototype which uses a mechanism similar to Remus. We recall that Remus was another hypervisor designed by Cully *et al.*, (2008). Taiji uses Network Attach storage (NAS) instead of separated local disk used in Remus. However, shared storage may become a single point and cause a weakness of this method

Ueno *et al.*, (2011) evaluated some results for a high security disaster recovery system using distribution and rake technology. The authors proposed an innovative file backup concept which makes use of an effective ultra-widely distributed data transfer mechanism and a high –speed encryption technology (HS-DRT). The HS-DRT system is based on the assumption that we can use a small portion of the storage capacity of a large number of PC's and cellular phones that are in use in daily life, to efficiently realize safe data backup at an affordable maintenance and operation cost.

Gharat and Mhamunkar (2015) in their work, proposed a Disaster Recovery as a Service (DRaaS) which was a nomenclature of cloud computing. This new approach of a DRaaS was a low cost service when compared to traditional disaster recovery systems. It was flexible in replicating physical or virtual data and provided facilities with consistent recovery for some working applications like SQL server. It has pre- built options for virtual recovery environments which include security, network connectivity and server failover when

continuously replicated among servers. When disaster occurs, disaster recovery backup will run all the applications until the primary site is resorted.

Furthermore, Machuca *et al.,* (2016) in their work gave an overview of different solutions in the context of technology-related disasters affecting communication networks and focused more on the importance of Software Defined Networking (SDN); its state of art on the resilience issues and approaches towards resilient SDN networks

Silva *et al.,* (2013) also in their work, presented dependability models for evaluating distributed cloud computing systems deployed into multiple data centers considering disaster occurrence. The approach was based on hybrid modeling technique which considered combinatorial and state-based models. The proposed technique allowed the impact assessment of disaster occurrence, virtual machine migration and data center distance on system dependability. Additionally, a case study was provided, considering a set of data centers located in different places around the world. The result demonstrated the influence of distance, network speed and disaster occurrence on system availability.

In the foregoing related work reviewed, it could be seen that many of them used the principle of server replication, combined with live VMs migration to create replicates of the primary servers from time to time and store them in backup servers.

Again, the storage services provided by one service provider may not be compatible with another service provider.

For instance, as noted by Basu *et al*., (2018); Popovic and Hocenski (2010), Microsoft cloud storage services is incompatible with google cloud storage. Consequently, it became very difficult for service users to transfer their application from one service provider to another in the cause of disaster occurring without losing a chunk of their sensitive data.

Therefore, this work was centered on providing an enhanced cloud disaster recovery model that integrated some of the functionalities across some selected disaster recovery models in order to address the problems of incompatibility of storage services by different service providers to their clients among other related issues.

METHODOLOGY

The methodologies adopted for this research were Structured System Analysis and Design Methodology (SSADM), Object Oriented Analysis and Design Methodology (OOADM) and Dynamic System Development Methodology (DSDM).

The SSADM was suited for a detailed design and analysis of an information system through which an improved system can be developed from an existing system. While the OOADM was adopted because it could be used to model a system as constituting of interacting objects in which each object was characterized in its class, state or behavior.

SYSTEM DESIGN

4.1 The design objectives of the new system were to:

i. create an enhanced disaster recovery system that drew operational features from SecondSite, HS-DRT and Taiji
ii. grant data center operators the privileges to configure their unique disaster recovery solution by hybridizing features selected from SecondSite, HS-DRT and Taiji to best fit into the company's budget on disaster recovery management.
iii. automatically generate backup files in accordance with the configuration patterns of companies.
iv. ensure that backup files are encrypted to protect them from Man- in -the -Middle attack while in transit.
v. ensure that the encrypted backup files are compressed to enhance its transmission over the internet.
vi. ensure that the compressed files are password protected to further enhance the security nature of the system.
vii. ensure that backup files are fragmented and each fragment transmitted through different routing process to enhance network overhead
viii. ensure that the backup files can be decompressed, decrypted and defragmented at recovery time only with the right keys

4.2 Main Menu/Control Centre

The functionalities of the system are logically grouped together in menu and submenu. Figure 1 shows the structural arrangement of the main menu.

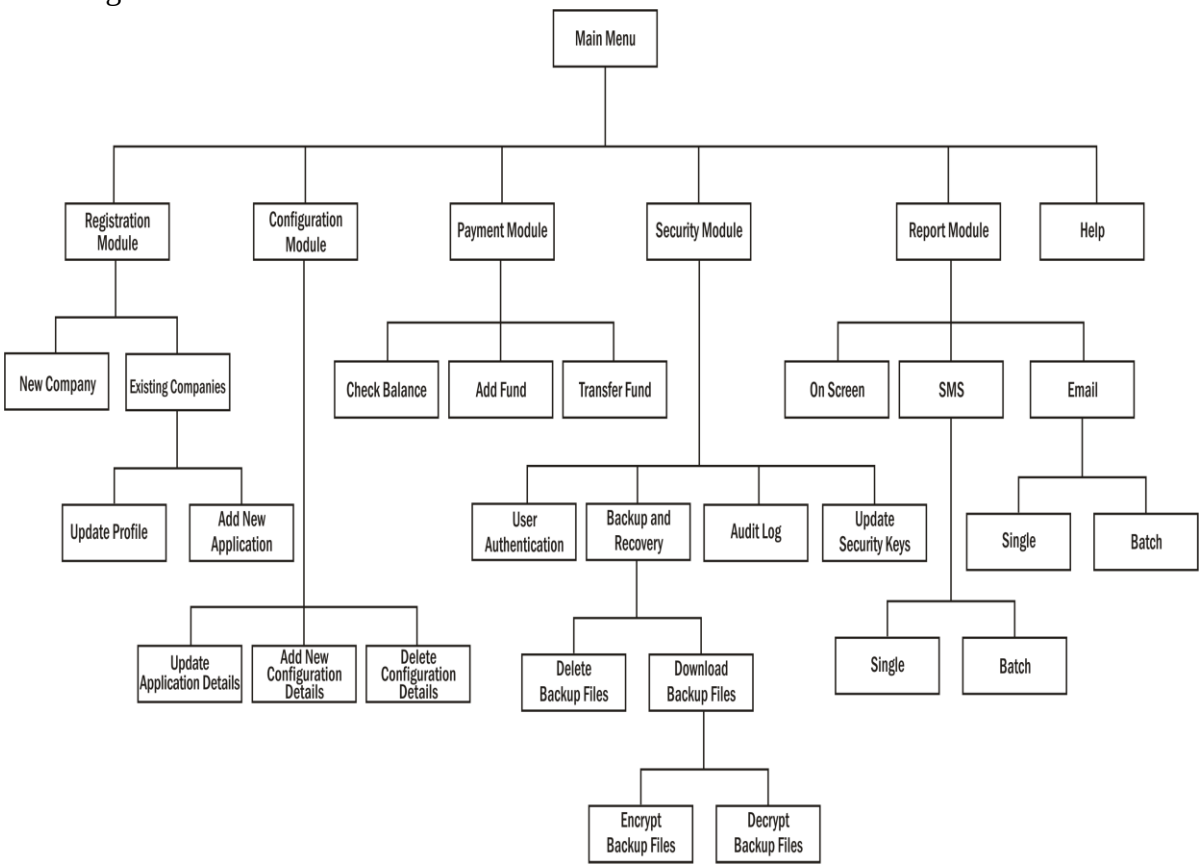


Fig. 1: Main Menu

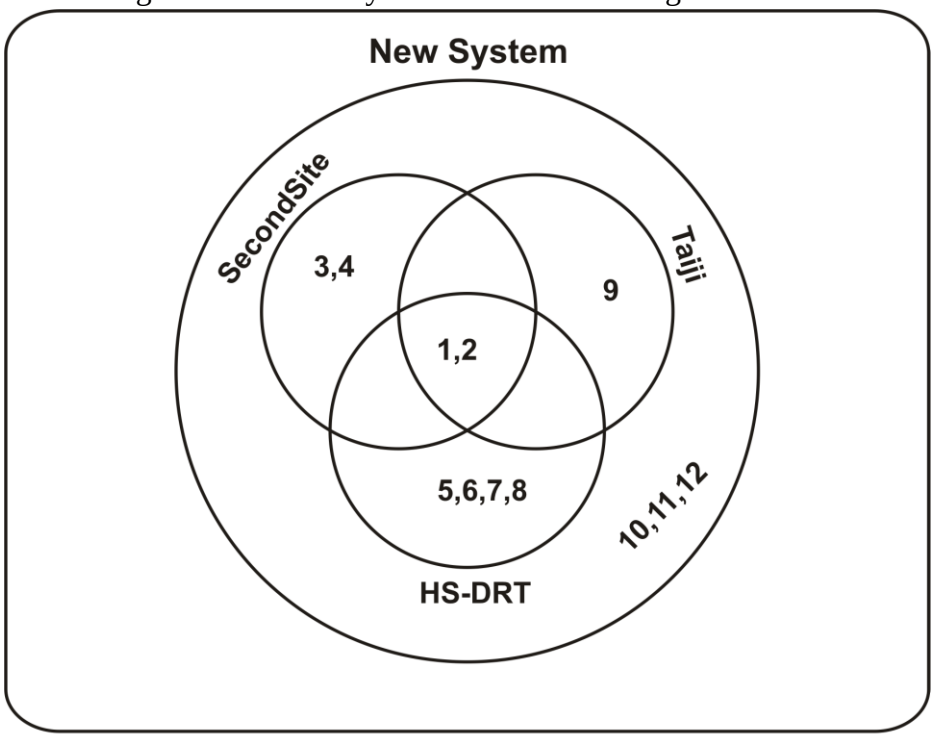
The new system was developed from a hybrid of SecondSite, Taiji and HS-DRT and implemented a total of twelve features selected from the three existing models under review. Table 1 showed the comparison between the three models and the new model.

Table 1: Comparison of Features

SN	Features	SecondSite	Taiji	HS-DRT	New System
1	Replication	V	V	V	V
2	Duplication	V	V	V	V
3	Server Watchdog	V	X	X	V
4	Check Pointing	V	X	X	V
5	Encryption	X	X	V	V
6	Decryption	X	X	V	V
7	Fragmentation	X	X	V	V
8	Defragmentation	X	X	V	V
9	Stateless Session	X	V	X	V
10	Checksumming	X	X	X	V
11	Compression	X	X	X	V
12	Decompression	X	X	X	V

Key
V stands for available features
X stands for unavailable features

The general architectural diagram of the new system is as shown in Figure 2.



Key

1. Replication	5. Encryption	9. Stateless Session
2. Duplication	6. Decryption	10. Checksumming
3. Server Watchdog	7. Fragmentation	11. Compression
4. Check Pointing	8. Defragmentation	12. Decompression

Fig. 2: Architectural Diagram of the Hybridized New System

System Implementation

The implementation of the new system was based on client/server architecture. Therefore, the minimum system requirements of the server machine in terms of software and hardware were quite different from that of the client system. In the light of this, the requirement of the client system is given separately from that of the server machine.

Hardware Requirements

i. **Hardware requirements of client systems:** The minimum hardware requirements for the client systems to effectively execute the new solution include:

a. 750MHZ processor speed
b. 128MB of RAM
c. 10 GB of Hard Disk Drive

ii. **Hardware requirements of server systems:** The minimum hardware requirements for the server machine to effectively execute the new solution include:

a. 2.00GHZ processor speed
b. 2GB RAM size
c. 500GB Hard Disk Drive

Software requirements

i. **Software requirements of client systems:** The client systems do not require any special software to execute the new system due to the fact that the new system is platform independent. All that is required of the client system is any graphical user interface (GUI) operating system and any web browser. However, for clients to execute the recovery module which is a standalone program written in Java, Java Development Kit (Java 1.8) or higher version is recommended. The system is compatible with virtually all operating

systems and all web browsers. As a matter of fact, the new system can even be executed on tablets and smartphones.

ii. **Software requirements of server systems:** The design system is hosted on the internet to give global access to our esteemed target users. However, it can equally be hosted on a local server for testing purpose. The minimal requirements of the local server in addition to GUI operating system and good browser include:

a. WildFly 10 Application Server
b. MySql Server
c. Java Development Kit (Java 1.8) or higher versions.
d. Any Good GUI Server Operating System
e. Web browser (Google Chrome, Mozilla Firefox, or any other one)

The researchers used a laptop with the following processor configuration: Intel(R) Core (TM) i7 CPU M 620 @ 2.67GHz, RAM of 6GB and Hard disk of 500GB to conduct experiments with a view of collecting some performance data from the system. The Operating System used in the experiments was Windows 10 64-bit. In the experiments, various sizes of remote databases were used and the backup files were encrypted, fragmented and compressed. The sizes of the backup files range from 64Kb to 20Mb.

Several performance metrics such as Encryption time, Compression size, CPU clock cycles and battery power were collatted. The encryption time was considered the time that an encryption algorithm took to produce a cypher text from a plaintext. Encryption time was used to calculate the throughput of an encryption scheme. It indicated the speed of encryption. The throughput of the encryption scheme was calculated as the total size of the plaintext in bytes encrypted; divided by the encryption time.

The CPU process time was the time that a CPU was committed only to the particular process of calculations. It reflected the load of the CPU. The more CPU time used in the encryption process, the higher was the load of the CPU. The CPU clock cycles were a metric, reflecting the energy consumption of the CPU while operating on encryption operations. Each cycle of CPU consumed a small amount of energy.

RESULTS AND DISCUSSIONS

5.1 ENCRYPTION TIME: A comparison was conducted between the results of the selected different encryption schemes in terms of the encryption time of five different encryption algorithm with ten different sizes of backup files in .sql format. The results are as shown in Table 2 and Figure 3;

Table 2: Comparison between DES, 3DES, BF, AES, and the Hybrid Encryption Time(s)

Input File Size (Kb)	DES (s)	3DES (s)	BF (s)	AES (s)	M-AES(s)
64.00	0.01	0.02	0.01	0.01	0.01
128.00	0.02	0.05	0.01	0.02	0.03
512.00	0.06	0.19	0.05	0.10	0.10
1,024.00	0.13	0.38	0.10	0.19	0.20
5,120.00	0.64	1.91	0.51	0.96	1.00
8,192.00	2.02	3.06	1.82	1.53	1.60
10,240.00	3.27	3.83	2.03	1.91	2.01
15,360.00	3.91	5.74	3.54	2.87	3.01
18,432.00	4.29	6.89	3.85	3.44	3.61
20,480.00	4.55	7.66	4.05	3.83	4.01

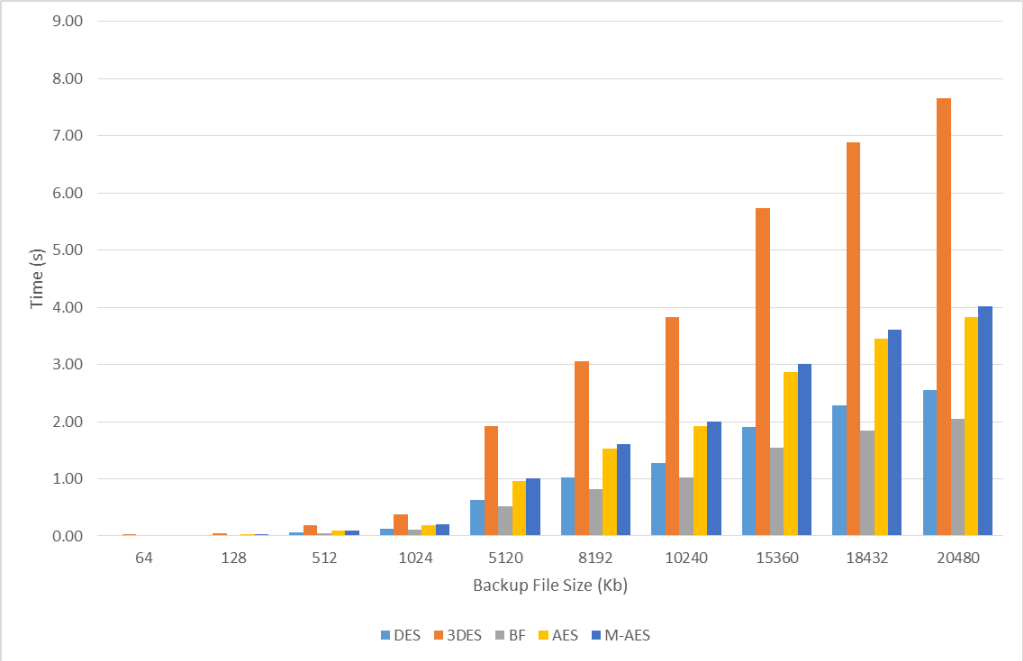


Figure 3: Bar chart of Input File Size versus Encryption Time for some encryption algorithms

The results were as expected. The Modified AES (M-AES) required more processing time than the Advanced Encryption Standard (AES) because of its key-chaining nature. The results as shown in Table 2 and Figure 3 indicated also that the extra time added was not significant for many applications, knowing that the new system was an enhancement over AES and that it was better in terms of file protection from Man -in –the- Middle (MITM) attacks.

5.2COMPRESSION SIZE: Again, in the work, the encrypted backup files were always compressed to enhance easy transmission of the files over network facilities. A modified version of Huffman Coding compression algorithm was used to compress backup files. A comparison was also conducted between the results of the selected different compression schemes in terms of the sizes of the compressed files of four different compression algorithms with ten different sizes of backup files ranging from 64 Kb to 20Mb. The results are as shown in Table 3 and Figure 4;

Table 3: Comparison between LZW, Huffman Coding, Shannon Coding and the M-Huffman

Input File Size (Kb)	LZW (Kb)	Huffman Coding (Kb)	Shannon-Fan Coding (Kb)	M-Huffman Coding (Kb)
64.00	36.57	18.29	18.82	16.00
128.00	73.14	36.57	37.65	32.00
512.00	292.57	146.29	150.59	128.00
1,024.00	585.14	292.57	301.18	256.00
5,120.00	2,925.71	1,462.86	1,505.88	1,280.00
8,192.00	4,681.14	2,340.57	2,409.41	2,048.00
10,240.00	5,851.43	2,925.71	3,011.76	2,560.00
15,360.00	8,777.14	4,388.57	4,517.65	2,800.00
18,432.00	10,532.57	5,266.29	5,421.18	2,800.00
20,480.00	11,702.86	5,851.43	6,023.53	2,800.00

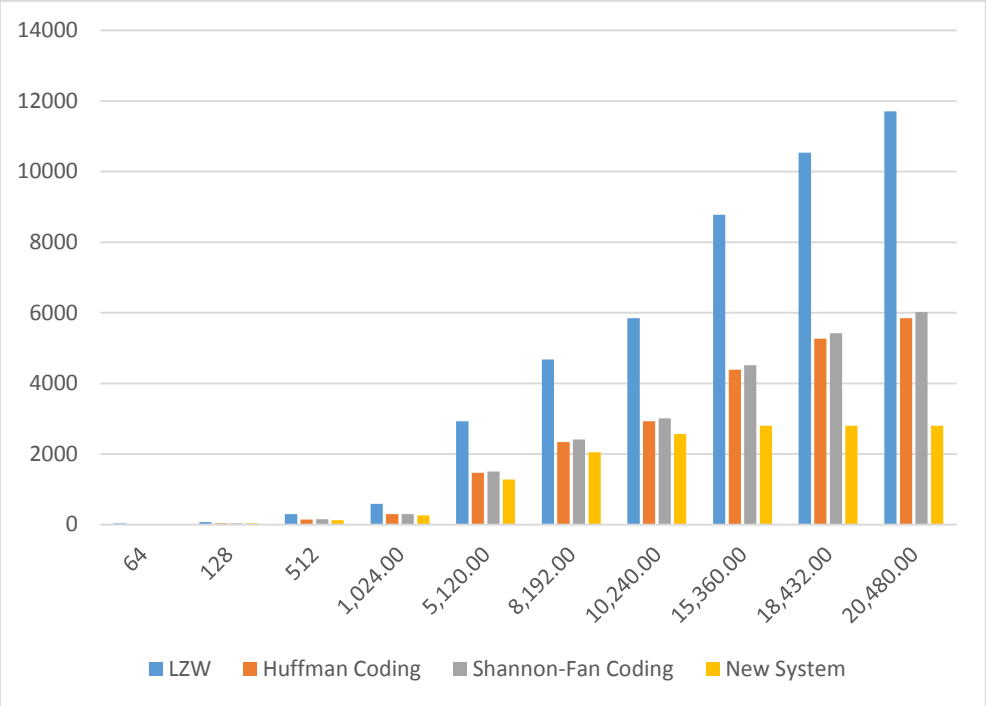


Figure 4: Bar chart of Input File Size versus Compressed Output File Size

The results from Table 3 and Figure 4 showed the superiority of the hybrid compression algorithm used in the work over other algorithms. Figure 4 also showed that as the size of input file increases, the output file size of the hybrid algorithm converges.

5.3 System Throughput: The throughput of an encryption scheme was calculated as the total size of the plaintext in bytes encrypted, divided by the encryption time. The higher the throughput values of an encryption scheme the better the algorithm. Using the same data set, the throughputs of the various encryption algorithms were captured and presented in table 4 and Figure 5;

Table 4: Throughput of DES, 3DES, BF, AES, and the Hybrid

DES	3DES	BF	AES	M-AES
8,238,161.04	2,739,484.17	10,224,146.29	5,478,968.34	5,228,787.14

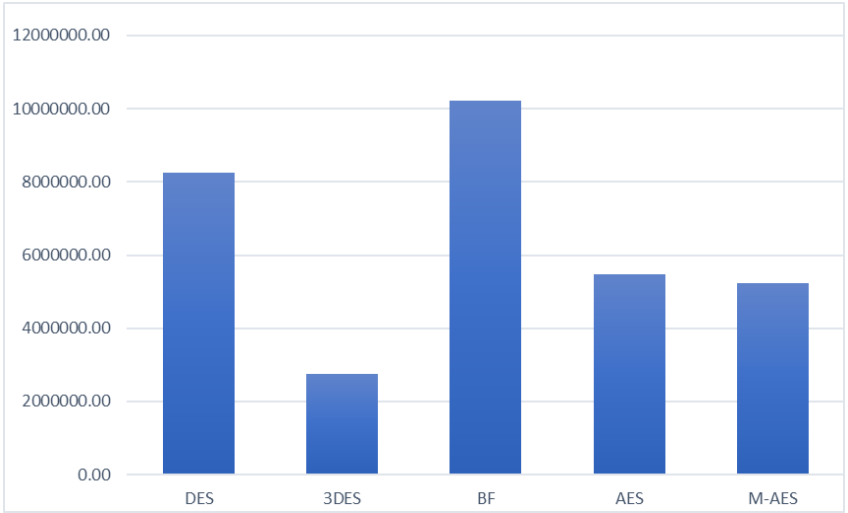


Figure 5: Bar Chart representation of System Throughputs of Some Selected Encryption Algorithms

The results were as expected. The Modified AES (M-AES) required more processing time than the Advanced Encryption Standard (AES) because of its key-chaining nature. The results shown in Table 4 and Figure 5 indicated that the little reduction on the throughput values was not significant for many applications, knowing that the new system was an enhancement over AES which was better in terms of file protection from Man-in- the- Middle (MITM) attacks.

5.4 COMPRESSION RATIO: Compression ratio was defined as the ratio between the uncompressed size and compressed size of compression algorithms (Al-Laham et al 2007). Using the same data set, the compression ratio of various compression algorithms was calculated and the results presented in Table 5 and Figure 6

Table 5: Comparison Ratio of LZW, Huffman Coding, Shannon Coding and the M-Huffman

Input File Size	LZW	Huffman Coding	Shannon-Fan Coding	M-Huffman Coding
64	1.7501	3.4992	3.4006	4.0000
128	1.7501	3.5001	3.3997	4.0000
512	1.7500	3.4999	3.4000	4.0000
1024	1.7500	3.5000	3.4000	4.0000
5120	1.7500	3.5000	3.4000	4.0000
8192	1.7500	3.5000	3.4000	4.0000
10240	1.7500	3.5000	3.4000	4.0000
15360	1.7500	3.5000	3.4000	5.4857
18432	1.7500	3.5000	3.4000	6.5829
20480	1.7500	3.5000	3.4000	7.3143

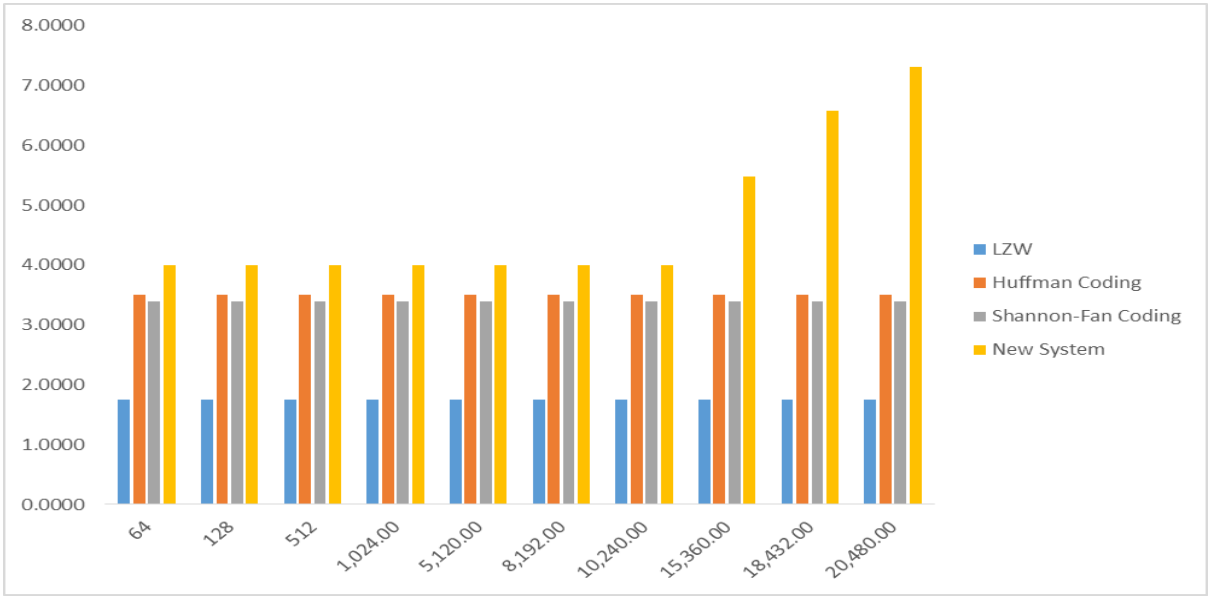


Figure 7: Bar Chart representation of Compression Ratio of Some Selected Compression Algorithms

It can be seen clearly from Figure 7 that the new system has better Compression Ratio compared with the other compression algorithms. Also worth of noting was the fact that the compression ratio of the new system increased exponentially as the size of the uncompressed files got larger than 15MB. This was in line with the fact illustrated in Figure 4 that the size of the compressed file converged as the size of the uncompressed file got larger than 15MB. Therefore, the denominator of Compression Ratio became constant while the nominator increased beyond 15MB. This explained why the compression ratio increased exponentially at the tail end of Figure 7

CONCLUSION

Over the years, organizations had found it very difficult to have complete features from one disaster Recovery Model that can satisfy their needs. Therefore deploying two or more Disaster Recovery Models to effectively handle their disaster recovery requirements was becoming a common practice. The hybridization of the three Disaster Recovery Models of SeondSite, Taiji and HS-DRT to produce an enhanced model was a contribution by the researchers that could help many data center operators and service providers to improve on the quality of service to their customers.

REFERENCES

1) Alazawi, Z., Abdijabor, M. B., Altowaijri, S., Vegni, A., & Mehmood, R., (2011): An Intelligent Cloud Based Disaster Management System for Vehicular Networks . 11th IEEE international Conference on ITS Telecommunication (ITST) August 23-25 2011 Pages 361-364
2) Al-Laham, M., & El Emary, I. M. (2007). Comparative study between various algorithms of data compression techniques. *IJCSNS International Journal of Computer Science and Network Security*, *7*(4), 281-291.
3) Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., ... and Sarkar, P. (2018, January). Cloud computing security challenges and solutions-a survey. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 347-356). IEEE.
4) Brook, C., Bedernak, M., Juran, I., & Merryman, J., (2012): Disaster recovery strategies with Tivoli Storage Management. IBM Corp. (retrieved on July 2018)
5) Caraman, M. C., Moraru, S. A., Dan, S. & Grama, C., (2012): Continous Disaster Tolerance in the IaaS clouds. 13th IEEE International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) pp. 1226-32. http://dx.doi.org/10.1109/OPTIM.2012.6231987(retrieved on Dec 2018)
6) Caraman, M. C., Moraru, S. A., Dan, S. & Kristaly, D. M., (2009): Romulus, Disaster Tolerant System based on Kernel Virtual Machines. 20th International DAAAM Symposium: Intelligent Manufacturing & Automatum: Theory. Practice & Education (pp. 1671-78)
7) Chaowei, Y., Qunying, H., Zhenlong, L., Kai, L., and Fei, H., (2017): Big Data and Cloud Computing: Innovation Opportunities and Challenges. International Journal of Digital Earth. Vol.10 issue 1 pp 1-35 (retrieved on July 2018)
8) Dennis, G., (2019): RTO vs RPO: Two means Towards the same End. https:www-cloudberrylab.com/resources/blog/rto-vs-rpo-difference/
9) Dimmter, V., & Plamena, Z., (2012): A Feasibility Study of Emergency Manageement with Cloud Computing Integration. International Journal of Innovation, Management and Technology Vol. 3 No 2 pages 188-193.
10) Gharat, A., & Mhamunkar, D., (2015): Disaster Recovery in Cloud Computing. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol. 4 Issue 5. ISSN: 2278-1323
11) Hauck, G., (2019): Lorenze Becomes The Most Powerful Hurricane To Make It So Far East In The Altantic. https:/www.usatoday.com/story/news/nation/2019/09/27/hurricane-lorenze-path–azores-strongest-eastern-a7858070021
12) Jangra, A., and Bala, R. (2012): A Survey on various possible vulnerabilities and attacks in cloud computing environment. International Journal of Computing and Business Research, 3(1), 1-13
13) Machuca, C.M., Secci, S., Vizarreta, P., Kuipers, F., Gouglidis, A., Hutchison, D., Jouet, S., Pezaros, D., Elmokashfi, A., Heegaard, P., & Ristov, S., (2016):Technology- related Disaster-resilient Software Defined Networks. 8th IEEE International Workshop on resilient Networks Design and Modelling. Sept 13-15,2016 Halmstad, Sweden Pages 35-42.
14) Mohammad, A.K., Azizol, A., Rohuya, L., Shamala, S., and Mohamed, O., (2014): Disaster Recovery in Cloud computing: A survey. Computer and Information Science journal vol.7, No.4 ISSN193-8989 pages 39-54
15) Nayak, T., Routray, R., Singh, A., Uttamchandani, S., & Verma, A.,(2010): End – to – end Disaster Recovery Planning: From Art to Science. IEEE/IFIP Network Operations and Management Symposium NOMS2010 Pages 357-364

16) Popovic, K., and Hocenski, Z., (2010): Cloud computing security issues and challenges. Paper presented at the MIPRO 2010 proceedings of the 33rd international convention.
17) Rodrigo, S. C., Stefano, S., Miguel, E. M., and Luis, H. K. C., (2014): Network Deisgn Requirement for Disaster Resilience in IaaS Clouds. IEEE Communication Magazine
18) Rajagopalan, S., Cully, B., Connor, R. O., & Warfield, A. (2012): SecondSite: disaster tolerance as a service. ACM SIGNPLAN Notices, 47(7), 97-107. http://dx.doi.org/10.1145/2365864.2151039.
19) Robinson, G., Narin, A., and Elleman, C. (2014): Using Amazon web Services for Disaster Recovery. Amazon Web Services. (retrieved on June. 2018)
20) Silva, B., Maciel, P., Tavares, E., & Zimmrmann, A., (2013): Dependability Models for Designing Disaster Tolerant Cloud Computing Systems 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). June 24-27. 2013 Washington USA. Pages 1-6
21) Subashini, S. & Kavitha, V., (2011): A survey on Security Issues in Service delivery Model of Cloud Computing. Journal of Network and Computer Applications Vol. 34 issue 1 pages 1-11 www.elsevier.com/locate/jnca.
22) Tamura, Y., Sato, K., Kihara, S., & Moriai,S., (2008): Kamari: Virtual Machine Synchronization for Fault Tolerance. Paper presented at the Proc. USENIX Annual Technology conference (Poster Session)
23) Ueno, Y., Miyaho, N., & Suzuki, S., (2011): Performance Evaluation of a Disaster Recovery System and Pratical Network Applications in Cloud Computing Envirnments. *International journal on Advances in Networks and Services* Vol.4 no 1&2, Pages 130-137.
24) Wood, T., Cecchet, E., and Ramakrishnam, K.K., (2010): Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Chanllenges. 2nd USENIC Workshop on Hot Topics in Cloud Computing (pp1-7)
25) Velev, D. and Ziatera, P., (2011): Principles of Cloud Computing Application Emergency Management. International Conference on E – Business, Management and Economic
26) Zhu, J., Jiang, Z., Xiao, V., & Lee, X., (2011): Optimizing the perfomance of vritual machine synchronization for fault tolerance. IEEE Transactions on Computers. 60(12). 1718-1729. http://dx.doi.org/10.1109/TC.2010.224