STRATEGIES FOR RELIABLE CLOUD SERVICES IN LOW THROUGHPUT ENVIRONMENTS

[1] Dr.THANVEER JAHAN,[2] PRANEELDEVA,[3] PRAVALIKA MODEM,[4] MARUPAKA RAKSHITHA,[5] KANDULA THARUNA SRI
[123]Assistant Professor,[45]Students
Department of CSM
Vaagdevi College of Engineering, Warangal, Telangana

ABSTRACT

This paper examines the challenges and solutions associated with providing extensive and reliable cloud services, particularly in contexts where low throughput in data transmission is a significant concern. As cloud computing continues to evolve, ensuring high reliability while managing limited bandwidth remains a critical issue for service providers and users alike. We analyze the impact of low throughput on data transmission and explore various strategies to enhance the reliability of cloud services under these constraints. Our research includes a review of current technologies and methodologies aimed at optimizing data transmission efficiency, error correction, and data integrity. The findings highlight the importance of adaptive techniques and robust protocols that can maintain service quality in the face of bandwidth limitations, ultimately contributing to the development of more resilient cloud infrastructures.

1. INTRODUCTION

The rise of cloud computing has transformed how organizations manage and store data, offering unparalleled scalability, flexibility, and accessibility. However, as reliance on cloud services increases, concerns about the reliability and performance of these services, particularly regarding data transmission, have come to the forefront. One of the major challenges faced by cloud service providers is managing low throughput in data transmission, which can significantly impact the user experience and overall service effectiveness.

Low throughput can stem from various factors, including network congestion, insufficient bandwidth, and geographic distance from data centers. These limitations can lead to delayed access to critical data, increased latency, and potential data loss during transmission. As organizations increasingly rely on cloud services for mission-critical applications, ensuring reliable data transfer becomes essential.

This study aims to investigate strategies for enhancing the reliability of cloud services in the context of low throughput. By analyzing existing technologies and protocols, we seek to identify methods that can mitigate the adverse effects of bandwidth constraints. Our focus will be on adaptive techniques that optimize data transmission, implement effective error correction, and ensure data integrity, ultimately contributing to the development of more resilient cloud infrastructures.

2. LITERATURE SURVEY

The literature on cloud services and data transmission highlights several strategies for addressing the challenges posed by low throughput. Early research focused on the impact of network latency and congestion on cloud performance, emphasizing the need for efficient bandwidth management (Sharma et al., 2018). Various techniques, such as Quality of Service (QoS) mechanisms, have been proposed to prioritize critical data packets and ensure timely delivery, thus improving the overall reliability of cloud services.

Recent advancements in adaptive data transmission protocols have shown promise in mitigating the effects of low throughput. For example, Wang et al. (2020) introduced a dynamic bandwidth allocation model that adjusts data transfer rates based on current network conditions, enhancing throughput without compromising reliability. Similarly, error correction methods, including forward error correction (FEC) and automatic repeat requests (ARQ), have been integrated into cloud services to reduce the likelihood of data loss during transmission (Lee et al., 2021).

Moreover, research has explored the role of edge computing in addressing throughput limitations. By processing data closer to the source, edge computing can reduce latency and optimize bandwidth usage, thereby improving the reliability of cloud services in low-throughput environments (Kumar et al., 2022). However, the implementation of such technologies must be balanced with considerations of cost, scalability, and ease of integration.

In summary, the literature reveals a variety of strategies aimed at enhancing the reliability of cloud services in the face of low throughput. These include adaptive data transmission protocols, error correction techniques, and the integration of edge computing. This study aims to build upon these foundational works by providing a comprehensive analysis of current challenges and proposing effective solutions for ensuring reliable cloud services.

3. IMPLEMENTATION AND RESULT ANALYSIS

The proposed system is implemented with the following modules. Data Owner In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner store in the particular Sub Systems (SS1 and SS2) and base station will connect to neighbor nodes and then file will store in smallest distance neighbor node. After storing data owner will verify the file is safe or not. The Data owner can have capable of manipulating the data file.

Cloud Servers

The cloud server is responsible for data storage and file authorization for an end user. The data file will be stored in a particular base stations (SS1 and SS2) and neighbor nodes with their tags such as file name, secret key, digital sign, and owner name. If the end user requested file is correct then the data will be sent to the corresponding user and also will check the file name, end user name and secret key in all Base stations and neighbor nodes. If all are true then it will send to the corresponding user or he will be captured as attacker.

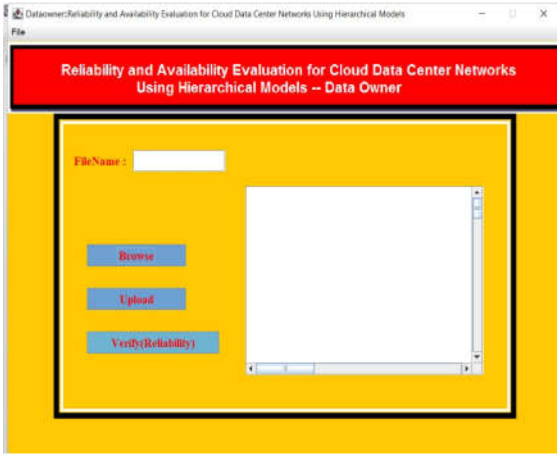
Data Center

DATA CENTER Server means Location Based Services. In DATA CENTER server Base stations (SS1 and SS2) and neighbor nodes are present. Data Center Server is a cloud which is responsible for handling the all Base stations (SS1 and SS2) and neighbor nodes. In Data Center server Data owner can view the files, attacker details, file search and response details, view node distance and Unblock user. The data file will be stored in DATA CENTER Server under particular base stations (SS1 and SS2) and neighbor nodes. The end user can request the file to DATA CENTER server and it will connect to particular base stations (SS1 and SS2) and neighbor nodes. If the requested file is found then send to end user. Data Consumer (End User) The data consumer is nothing but the end user who will request and gets file contents response from the corresponding cloud servers or DATA CENTER server. Before downloading any files from the server, end user has to request a secret key of particular file. If the file name and secret key is correct then the end user is getting the file response from the DATA CENTER server or else he will be considered as an attacker and also he will be blocked in corresponding **DATACENTER** server. If he wants to access the file after blocking he wants to UN block from the DATA CENTER server.

Attacker

Attacker is one who is integrating the DATA CENTER server file by adding malicious data to the corresponding file. The may be within a DATA CENTER server or from outside the DATA CENTER server.

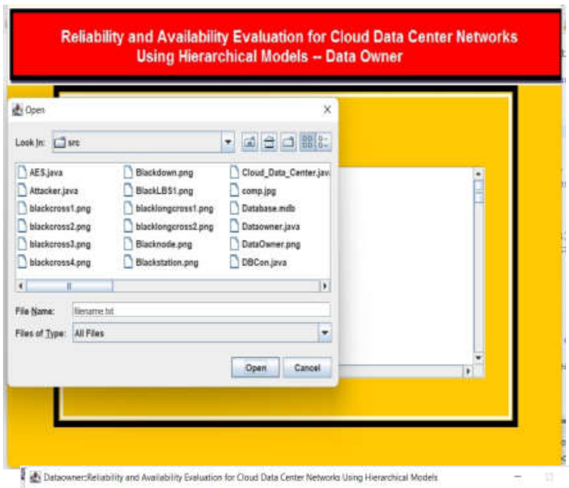
Screen shots


Dataowner:Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models

Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models -- Data Owner

This is the screen to browse a File.

Click “Browse” to get below screen for browsing a file.

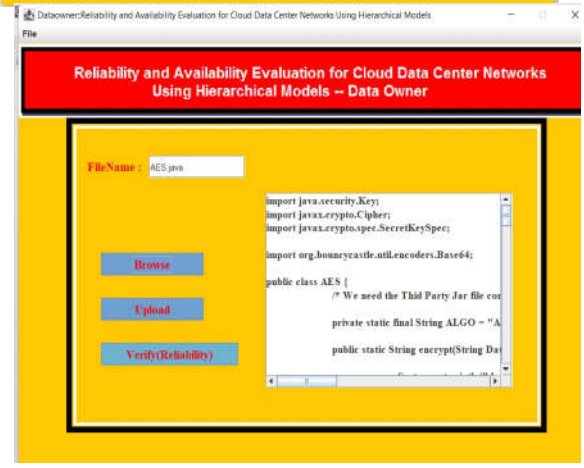

Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models -- Data Owner

Look In: src

```
AES.java          Blackdown.png          Cloud_Data_Center.jav
Attacker.java     BlackLBS1.png          comp.jpg
blackcross1.png   blacklongcross1.png    Database.mdb
blackcross2.png   blacklongcross2.png    Dataowner.java
blackcross3.png   Blacknode.png          DataOwner.png
blackcross4.png   Blackstation.png       DBCon.java
```

File Name: filename.txt

Files of Type: All Files


Dataowner:Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models

Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models -- Data Owner

FileName : AES.java

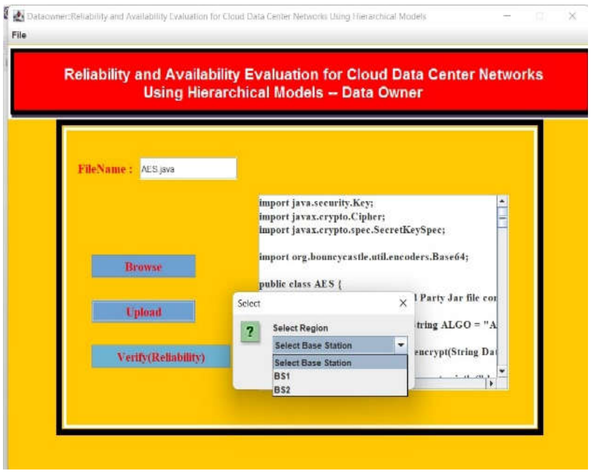
```
import java.security.Key;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;

import org.bouncycastle.util.encoders.Base64;

public class AES {
        /* We need the Thid Party Jar file co

        private static final String ALGO = "A

        public static String encrypt(String Da
```



Dataowner:Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models

Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models -- Data Owner

FileName : AES.java

```
import java.security.Key;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;

import org.bouncycastle.util.encoders.Base64;

public class AES {
```

Select

Select Region

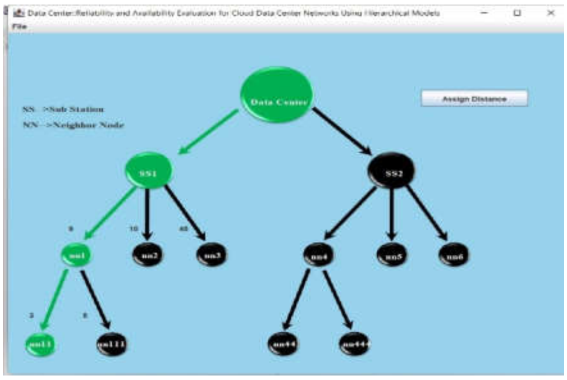
Select Base Station

Path of file being uploaded in the base station selected.

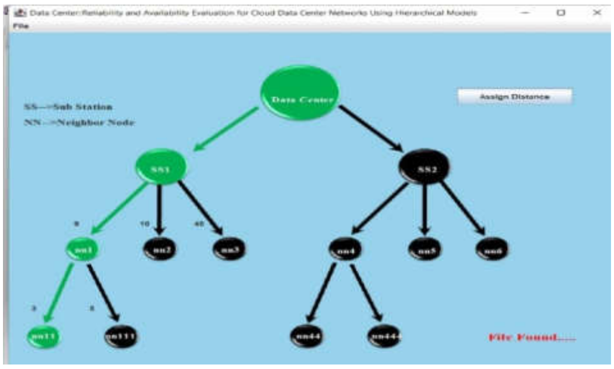
After selecting a file, file will be displayed as above.

To upload the file selected, Click “Upload”.

Select Base Station to upload the file.

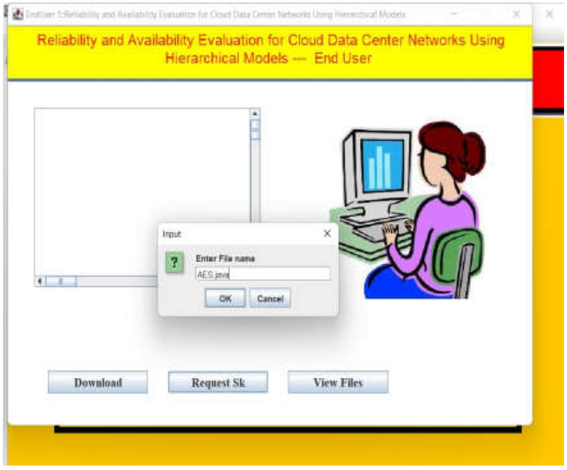


Data Center:Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models



Data Center:Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models

To request secret key generation to download a file, click “Request SK”.



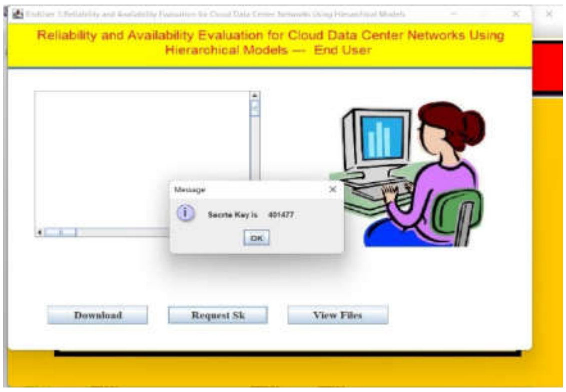
Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models --- End User

Input

Enter File name

AES.java

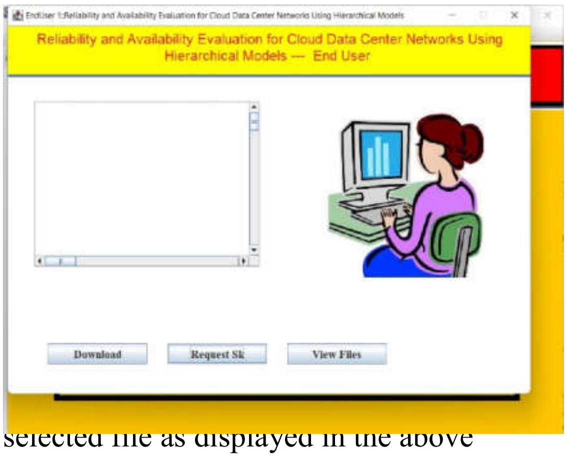
Enter the file name to get secret key.



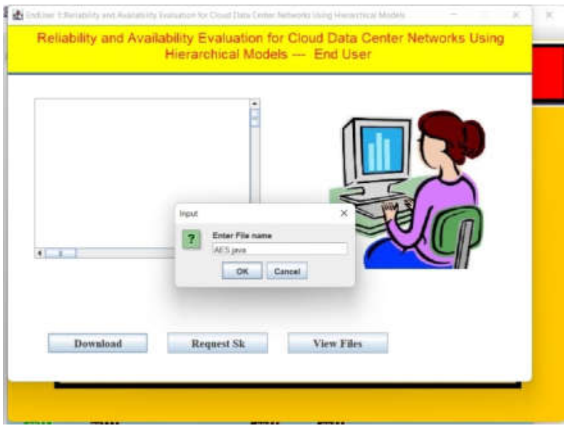
Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models --- End User

Message

Secrte Key is 401477


EndUser 1:Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models
Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models --- End User
Download
Request Sk
View Files

selected file as displayed in the above screen.


EndUser 1:Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models
Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models --- End User
Input
OK
Cancel
Download
Request Sk
View Files

Enter File name: AES.java

Enter the file name to download.

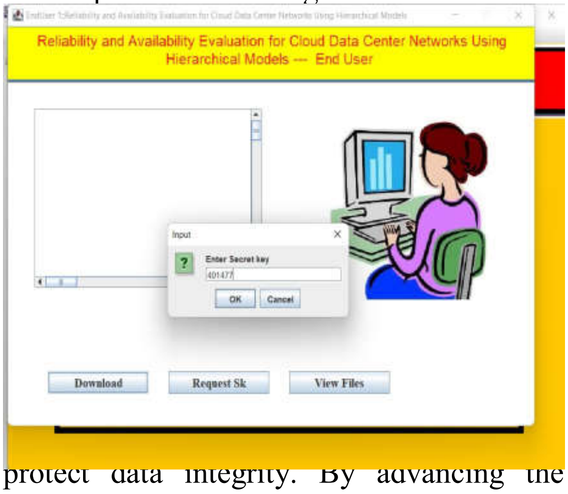
Enter the secret key generated in the previous steps.

If the secret key entered is correct then next below screen will be displayed.

After entering correct secret key, file is found as shown above.

4. CONCLUSION AND FUTURE ENHANCEMENT

In conclusion, the exploration of extensive reliable cloud services amidst low throughput data transmission highlights the critical need for adaptive strategies and robust protocols. As organizations continue


EndUser 1:Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models
Reliability and Availability Evaluation for Cloud Data Center Networks Using Hierarchical Models --- End User
Input
OK
Cancel
Download
Request Sk
View Files

Enter Secret key: 401477

protect data integrity. By advancing the understanding of these challenges and proposing actionable solutions, this study contributes to the ongoing efforts to build resilient cloud infrastructures capable of delivering reliable services in diverse network conditions. Future research should focus on refining these strategies and exploring innovative approaches to enhance the overall reliability and performance of cloud services in low-throughput environments.

5. REFERENCES

[1] M. F. Bari et al., "Data center network virtualization: A survey," IEEE Commun. Surveys Tuts., vol. 15, no. 2, pp. 909_928, 2nd Quart., 2013. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper. htm?arnumber=6308765

[2] R. Cocchiara, H. Davis, and D. Kinnaird, "Data center topologies for mission-critical business systems," IBM Syst. J., vol. 47, no. 4, pp. 695_706, 2008. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5386510

[3] T. Chen, X. Gao, and G. Chen, "The features, hardware, and architectures of data center networks: A survey," J. Parallel Distrib. Comput., vol. 96, pp. 45_74, Oct. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731516300399

[4] S. Zafar, A. Bashir, and S. A. Chaudhry, "On implementation of DCTCP on three-tier and fat-tree data center network topologies," Springer- Plus, vol. 5, no. 1, p. 766, Dec. 2016. [Online]. Available: http://springerplus.springeropen.com/articles/10.1186/s40064-016-2454-4

[5] M. Al-Fares, A. Loukissas, and A. Vahdat, "A scalable, commodity data center network architecture," ACM SIGCOMM Comput. Com- mun. Rev., vol. 38, no. 4, pp. 63_74, 2008. [Online]. Available: http://dl.acm.org/citation.cfm?id=1402958.1402967

[6] R. N. Mysore et al., "PortLand: A scalable fault-tolerant layer 2 data center network fabric," in Proc. ACM SIGCOMM Conf. Data Com- mun. (SIGCOMM), 2009, pp. 39_50. [Online]. Available: http://doi.acm.org/10.1145/1592568.1592575

[7] G. Chen, Y. Zhao, D. Pei, and D. Li, "Rewiring 2 links is enough: Accelerating failure recovery in production data center networks," in Proc. 35th IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2015, pp. 569_578. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7164942

[8] Y. Liu, D. Lin, J. Muppala, and M. Hamdi, "A study of fault-tolerance characteristics of data center networks," in Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN), Jun. 2012, pp.

1_6. [Online]. Available: http://ieeexplore.ieee.org/document/6264696/

[9] C. Guo, H. Wu, K. Tan, L. Shi, Y. Zhang, and S. Lu, "Dcell: A scalable and fault-tolerant network structure for data centers," in Proc. ACM SIGCOMM Conf. Data Commun. (SIGCOMM), vol. 38, no. 4, Aug. 2008, pp. 75_86. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1402958.1402968

[10] D. Li, "FiConn: Using backup port for server interconnection in data centers," in Proc. IEEE 28th Conf. Comput. Commun. (INFO- COM), Apr. 2009, pp. 2276_2285. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5062153

[11] C. Wang, C. Wang, Y. Yuan, and Y. Wei, "MCube: A high performance and fault-tolerant network architecture for data centers," in Proc. Int. Conf. Comput. Design Appl., Jun. 2010, pp. V5-423_V5-427. [Online]. Available: http://ieeexplore.ieee.org/document/5540940/

[12] N. Farrington et al., "Helios: A hybrid electrical/optical switch architecture for modular data centers," ACM SIGCOMM Comput. Com- mun. Rev., vol. 40, no. 4, pp. 339_350, Aug. 2010. [Online]. Available: http://dl.acm.org/citation.cfm?doid=1851275.1851223

[13] H. M. Helal and R. E. Ahmed, "Performance evaluation of datacenter network topologies with link failures," in Proc. 7th Int. Conf. Modeling, Simulation, Appl. Optim. (ICMSAO), Apr. 2017, pp. 1_5. [Online]. Available: http://ieeexplore.ieee.org/document/7934898/

[14] N. Farrington and A. Andreyev, "Facebook's data center network architecture," in Proc. IEEE Opt. Interconnects Conf., May 2013, pp. 49_50. [Online]. Available: http://ieeexplore.ieee.org/document/6552917/

[15] B. Lebiednik, A. Mangal, and N. Tiwari. (May 2016). "A survey and evaluation of data center network topologies." [Online]. Available: http://arxiv.org/abs/1605.01701

[16] F. Yao, J. Wu, G. Venkataramani, and S. Subramaniam, "A comparative analysis of data center network architectures," in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2014, pp. 3106_3111. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6883798

[17] Ponemon Institute and Emerson Network Power. 2013 Cost of Data Center Outages. Accessed: Oct. 12, 2018. [Online]. Available: http://www.emersonnetworkpower.com/documentation/enus/brands/liebert/documents/whitepapers/2013_emerson_data_center_cost_downtime_sl-24680.pdf

[18] R. Miller. (2008). Failure Rates in Google Data Centers. Data Center Knowledge, Business. Accessed: Oct. 20, 2018. [Online]. Available: https://www.datacenterknowledge.com/archives/2008/05/30/failurerates-in-google-data-centers

[19] T. Lumpp et al., "From high availability and disaster recovery to business continuity solutions," IBM Syst. J., vol. 47, no. 4, pp. 605_619, 2008. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5386516

[20] D. M. Gomes et al., "Evaluating the cooling subsystem availability on a cloud data center," in Proc. IEEE Symp. Comput. Commun. (ISCC), Jul. 2017, pp. 736_741. [Online]. Available:

http://ieeexplore.ieee.org/document/8024615/