IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

MULTI-CLOUD AND FOG COMPUTING TO CREATE A SECURE BACKUP SYSTEM

R.Hamsaveni. B.ArulMozhi,S.Shanthi,R,Shobana,T.Sandhiya

Assistant Professor, Department of computer science, DKM colleges for Women, Vellore.

Head /Assistant Professor, Department of computer science, DKM colleges for Women, Vellore.

Assistant Professor, Department of computer science and Appli, DKM colleges for Women, Vellore.

Assistant Professor, Department of computer science, DKM colleges for Women, Vellore.

PG Student, Department of computer science, DKM colleges for Women, Vellore

Abstract- For disaster recovery, data backup is critical. Cloud-based solutions already provide a secure infrastructure. However, data privacy cannot be guaranteed when it is stored in a single cloud. Multi-cloud technologies are another option. Although employing several clouds to save smaller chunks of data can improve data privacy, it also requires the edge device to maintain many accounts and manage connection with multiple clouds. Because of these flaws, this technology is rarely used. Using state-of-the-art Multi-Cloud and encryption techniques, we present DropStore as an easy-to-use, highly secure, and reliable backup system. Using a locally hosted device, DropStore creates an abstraction layer for the end-user to hide all system intricacies."The Droplet," which is completely controlled by the user. As a result, the user does not have to rely on any untrustworthy third parties. Fog Computing was used to do this. The combination of Multi-Cloud and Fog Computing principles gives DropStore its distinctiveness. The system is open-source and accessible via the internet. The suggested solution improves data protection in terms of reliability, security, and privacy preservation while keeping a simple and straightforward interface with edge devices, according to performance results.

Key Words:, Cloud Infrastructure, Attribute Based Encryption, Cloud Service Provider, Ciper Text policy, Cloud Backup

I. INTRODUCTION

Many people can now readily share their data with others via online external storage thanks to recent advancements in network and computing technology. People can share their lives with friends by uploading private photos or messages to online social networks like Facebook and Myspace; or they can upload highly sensitive personal health records to online data servers like Microsoft Health Vault and Google Health for easy sharing with their primary doctors or to save money. People's concerns about data security and access control grow as they benefit from these new technology and services. Unauthorized access by outside users or improper data use by the storage server could be dangers to their data. People want to make their own decisions[9].People want their sensitive or private data to be available exclusively to those who have the credentials they specify. Cloud storage offers substantial benefits in terms of data sharing and cost reduction. As a result, an increasing number of businesses and people are outsourcing their data to the cloud to take advantage of this service. However, this new data storage paradigm offers significant issues in terms of data confidentiality. The data owner cannot trust the cloud server to execute secure data access control because the cloud service separates the data from the cloud service client (individuals or businesses), denying them direct control over the data[4]. As a result, secure access control has become a difficult problem in public cloud storage.

CP-ABE (ciphertext-policy attribute-based encryption) is a cryptographic approach for controlling data access in cloud storage. All of these CP-ABE-based approaches allow data owners to implement fine-grained and flexible data access control. CP-ABE, on the other hand, evaluates users' access privileges only based on their intrinsic traits, disregarding any other crucial criteria such as time. In actuality, when dealing with time-sensitive material (for example, publishing the latest electronic magazine or exposing a company's future business plan), the time factor frequently plays a crucial role.Both the mechanism of access privilege timed release and fine-grained access control should be considered in these instances. Consider the following example of enterprise data exposure: A corporation typically prepares some key files for several intended users, who can receive access privileges at different times. For example, this company's future plan could include trade secrets.

Cloud storage offers substantial benefits in terms of data sharing and cost reduction. As a result, an increasing number of businesses and people are outsourcing their data to the cloud to take advantage of this service. However, this new data storage paradigm offers significant issues in terms of data confidentiality. The data owner cannot trust the cloud server to execute secure data access control because the cloud service separates the data from the cloud service client (individuals or businesses), denying them direct control over the data. As a result, secure access control has become a difficult problem in public cloud storage.CP-ABE (ciphertext-policy attribute-based encryption) is a cryptographic approach for controlling data access in cloud storage. All of these CP-ABE-based approaches allow data owners to implement fine-grained and flexible data access control[3]. CP-ABE, on the other hand, evaluates users' access privileges only based on their intrinsic traits, disregarding any other crucial criteria such as time. In actuality, when dealing with time-sensitive data (e.g., to publish the most recent electronic version), the time element frequently plays a crucial role.

II. RELATED WORK

Rongxing Lu et.al[1] The mobile healthcare (m-Healthcare) system has been envisioned as a significant computing application for improving health care quality and saving lives. In an m-Healthcare emergency, an opportunistic computing paradigm can be used to overcome the challenging dependability issue in the PHI process. To solve this problem, we present SPOC, a novel secure and privacy-preserving opportunistic computing paradigm. Marlena

Ning Cao et.al [2] Cloud computing is the long-awaited realisation of computing as a utility, in which cloud customers can store their data remotely in the cloud and access high-quality apps and services on demand from a shared pool of programmable computer resources. Individuals and businesses are both motivated to outsource their local complicated data management system to the cloud because of its excellent flexibility and cost savings. Sensitive data must be protected in the cloud and beyond to prevent unauthorised access.

Jing Chen et.al[3] Wireless mesh networks are used in a variety of applications, including industrial control, environmental monitoring, and military operations. Network coding is a potential technology that can help wireless mesh networks run better. Because the fixed backbone of wireless mesh networks is usually unlimited energy, network coding is appropriate. It effectively addresses the flow coding collision problem by introducing the information process, which effectively lowers the decoding failure rate.

Ruiying Du et.al[4]This problem is addressed by integrating broadcast encryption techniques with ABE schemes in a user-revocable ABE system. To enable direct user revocation, the data owner should accept complete responsibility for maintaining the entire membership list for each attribute group in this scheme. This strategy is not relevant to the data sharing system since after saving their data on an external storage server, the data owners will no longer have direct control over their data. User revocation in the ABE-based data sharing system was also recently addressed by Yu et al. The data server performs user revocation using proxy encryption in this scheme.However, in order to revoke users, the KGC should generate all secret keys on behalf of the data server, including the proxy key. To prevent revoked users from decrypting the ciphertext, the server would reencrypt it using the proxy key received from the KGC.

ZhengxiaZou et.al [5] Many realistic ABE-based systems have recently recognised the need of immediate user revocation. Ostrovky et al. recommended employing ABE, which enables negative clauses, for user revocation. To accomplish so, simply combine the AND of negation of revoked user identities together. One disadvantage of this technique is that the size of the private key grows by a factor of login, where n is the maximum number of attributes. For no monotonic ABE, Lewko et al. presented more efficient instantiations of the Ostrovky et al. architecture, where public parameters are only O(1) group elements and private keys for access structures including t leaf attributes are of size O. (t). However, these user-revocable schemes have a constraint in terms of the number of users.

III. PREVIOUS IMPLEMENTATIONS

Researchers have been concerned about the concept of big data. Using big data to gather useful information has become a popular trend in recent years. Big data research's main purpose is to process massive amounts of data in order to extract useful information. Furthermore, in the long run, a proper approach to large data processing is crucial. However, dealing with large amounts of data requires more than a single computer or server. As a result, in the building of big data, the distributed structure is extremely crucial.Cloud computing originated from distributed computing, which may provide a variety of big data-related services such as distributed processing, virtualization, and distributed databases.

- It is impossible to cope with huge data on a single computer or server.
- A great number of security issues can occur when all data must be uploaded to the cloud.
- They encrypt real data with a symmetric key encryption process and utilize a deniably encrypted plan-ahead symmetric data encryption key[4].
- Most decryption error concerns exist in deniable encryption methods. The designed decryption mechanisms are at blame for these problems.
- Decryption is performed using the subset decision process. According to the subset decision result, the receiver selects the decrypted message.
- An error occurs if the sender selects an element from the universal set while the element is found in the specialized subset.
- All transparent set-based systems have the same issue[7].

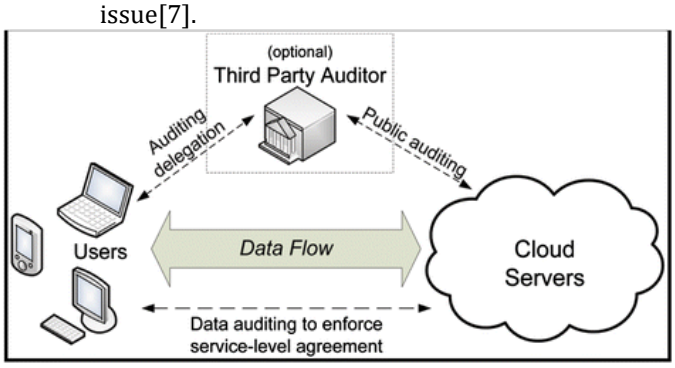


Fig: Architecture of the cloud storage environment

Wang et al. consider dynamic data storage in a distributed environment in [11]. They proposed a protocol for determining data accuracy as well as locating potential flaws. However, the authors, like [9], only examine partial support for dynamic data operations. As a result, they presented a system based on a combination of BLS-based homomorphic authenticator and MHT in their future work [12]. This combination would allow fully dynamic data to be audited by the public. A novel proof of irretrievability (PoR) scheme is suggested in [13]. To secure both possession and irretrievability of data files on the cloud storage system, this approach employs both spot-checking and error-correcting codes.However, as with [9], the maximum number of queries a client can make is predetermined, and the use of precompiled sentinels hinders the development of dynamic data updates. [14] Proposes a better PoR technique based on publically verifiable homomorphic authenticators constructed from BLS signatures. The security model defined in [13] has full proofs of security. The proofs can be combined into a small authenticator value, resulting in public irreversibility. Despite the fact that the enhancement accomplishes the goal, the authors only examine static data files. The authors present the concept of TPA in [15] to reduce online strain while maintaining data integrity and privacy. Using the concept of TPA, an enhanced method of certifying data integrity on the cloud has been developed.

- **Cloud server (CS):** an entity with a lot of storage and processing power. A cloud service provider (CSP) manages the cloud server and provides data storage services to anyone who wants to store data in the cloud.
- **A cloud user (CU)** is someone who has a large number of data files to store on a cloud server.
- **Third-party auditor (TPA):** a person with experience and capabilities that users may lack, and who is trusted to analyses and reveal risk associated with cloud storage services on their behalf.

A user stores data in the cloud through a CSP into a set of cloud servers that are working in a parallel, cooperative, and dispersed manner. For cloud data storage and upkeep, the user relies on the CS. After that, the user can dynamically interact with the CS via CSP to access and retrieve/update the stored data for various application reasons. Because the user no longer has local access to his or her data, it is vital that the user ensures that his or her data is properly kept and preserved, which means the user should be provided with the necessary tools [8].Even without the presence of local copies, he can make ongoing correctness assurance (to enforce cloud storage service-level agreements) of his stored data. Auditing should be done to ensure the accuracy and integrity of data kept on cloud servers. The user can delegate data auditing chores to an optional trusted TPA of their choice to ensure the outsourced data's storage security while still keeping his data private from the TPA.

V. IMPLEMENTATION OF CLOUD

1. Setup phase:

The organization admin initializes the public and secret parameters settings of the system using the KEYGEN algorithm, and preprocesses the data using SigGen to generate verification metadata (connection details, user accounts). The administrator then uploads the data to the cloud server, deletes the local copy, and sends the verification information to TPA for auditing. The user can edit the data file during pre-processing by enlarging it or adding new metadata to be saved on the server.

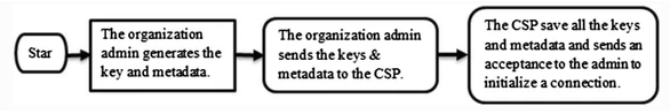


Fig: Setup Phase

Data Accessing Phase

The organization's administrator turns to a TPA with experience in data auditing. To audit the outsourced data on the CS, activate the TPA account and deliver the secret key and metadata (details about the data files but not the data files themselves) to the TPA. The TPA sends an audit message to the cloud server to ensure that the data file was properly stored on the cloud server at the time of the audit. By executing GenProof [19], the cloud server will derive a response message from a function of the stored data file F. The TPA checks the response using verify proof [19] using the verification metadata. The TPA sends the auditing report to the client.

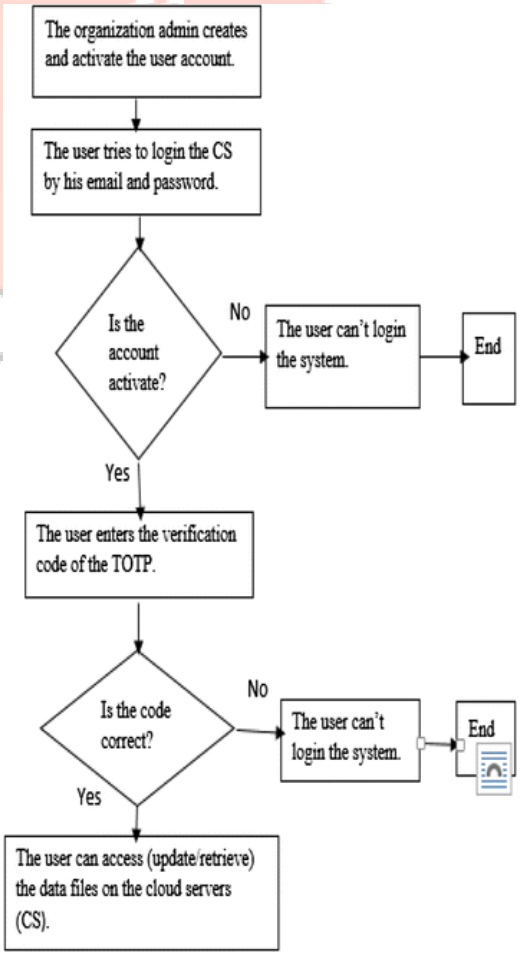


Fig: Data Access Phase

3. Data Auditing Phase

Any organization (for example, trading businesses, banks, and commercial firms) can use the suggested system to store their data on cloud storage provided by the providers. The organization can hire a TPA for the auditing process to avoid the TPA and CSP contract being used to hide data losses. The auditing process can take place at any moment, depending on the needs of the organization. Furthermore, the proposed method can help the organization authenticate users so that they can access their system several times after registering [5].

1. The organization admin sets up the setup scheme by generating keys and information with the KEYGEN [11, 12] algorithm and sending them to the CSP.

2 The CSP responds to the admin's request by accepting the set up scheme using the SINGEN [11, 12] algorithm. As a result, a link between the admin and the CSP is established. Data is encrypted using a sophisticated encryption technology called advanced encryption system before being sent to the CS (AES).

3 According to the CIA trinity for information security, the user must have an account (emails and password) to access stored data in order to achieve information confidentiality, integrity, and availability. The admin can place extra limits on these this system has accounts. Activated accounts, where the only person who may activate or deactivate the accounts is the administrator.

4 The accounts of enabled users can be accessed using a two-stage authentication method: username and password, as well as the TOTP, which is valid for one session between the user and the cloud server.

5 If the organization's administrator wishes to audit the outsourced data on the cloud server, he turns to a TPA who specializes in data auditing. The TPA, on the other hand, must have a system account. The organization's administrator must additionally activate this account. The secret key and metadata would be sent to the TPA to audit the outsourced data if the TPA account was activated by the organization admin.6TPA with the secret key and metadata sends the auditing request to the CSP to initialize the auditing process.

7Using the APB, the CSP sends a query about the auditing process to the organization admin, who must authorize the query and TPA metadata.

8 If the APB is true, the admin transmits the approval along with the metadata to the cloud service provider; otherwise, the TPA is unable to access the system.

9 A report on data auditing is available from the TPA.

10 The TPA provides the auditing report together with the metadata to the organization's admin, who subsequently deactivates the TPA account to avoid any arrangement between the CSP and the TPA to hide data losses from the admin.

4. Input Design

The link between the information system and the user is the input design. It entails creating data preparation specifications and procedures, as well as the steps required to convert transaction data into a usable format for processing. This can be accomplished by inspecting the computer to read data from a written or printed document, or by having people key data directly into the system. Limiting the amount of input required, controlling errors, avoiding delays, avoiding superfluous stages, and making the process simple are all goals of input design. The input has been created in such a way that it gives security and convenience while maintaining privacy. The following factors were considered by Input Design:

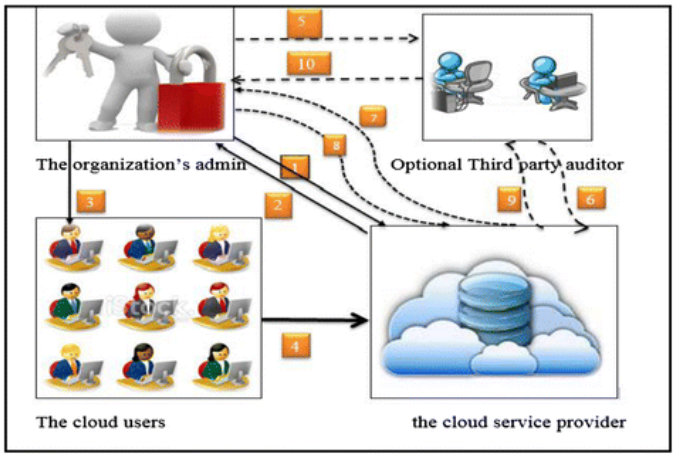


Fig 1.3 Process Diagram

1. Organization admin: an entity, who has huge amount of data to be stored in the cloud, can be either enterprise or individual customers. The admin has all the privileges over the users and the third party auditors.

2. Cloud user (CU): a user who has permission to access (edit or retrieve) data in the cloud under the supervision of the organization's administrator.

3. Third-party auditor (TPA): someone who can be hired to audit data kept in the cloud if the administrator requests it.

4. Cloud service provider (CSP): a company that manages cloud servers with plenty of storage capacity for any company that needs to store data.Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.According to RFC 6238 [18], the TOTP is based on HOTP with time stamp replacing the incrementing counter. The reference implementation of the HOTP algorithm is as follows:

Algorithm Implementation

1K is a secret key.

2C is a counter.

3HMAC (K, C) = SHA1 (K ⊕ 0x5c5c ... ||SHA1 (K ⊕ 0x3636 ... ||C)) is a HMAC calculated with SHA cryptographic technique.

4HOTP (K, C) = Truncate (HMAC (K, C)) & 0x7FFFFFFF.

The current time stamp has turned into an integer time-counter (TC) that depends on two parameters; the start of an epoch (T0) and the time step (TS). TC calculated as:

$$TC = (\text{time now} - \text{time (T0)})/TS. \quad (1)$$

The TOTP is computed as follows:

$$TOTP = HOTP(\text{secret key (K)}, TC)\ TOTP\ \text{value} = TOTP \bmod 10^d \quad (2)$$

Where, d is the desired number of digits of the one-time password, according to RFC6238 [18] reference implementation.

VI. EVALUATION RESULT:

The proposed system is built with a Java enterprise edition web application and a Tomcat server. Every organization in the proposed system has an administrator who ensures data confidentiality, integrity, and availability. The administrator creates the keys and metadata, connects to the CS, and then saves the data to

the cloud server. However, data is encrypted before being sent to the CS using a powerful encryption technique (AES). The admin enables the users' accounts on the CS to gain access to the data, as shown in Fig. 6. The TOTP then authenticates the users with the cloud service provider's approval.The admin delegated the auditing process to the TPA and used the ABP to authorize the activated TPA to audit the outsourced data, as shown in Fig. 8 and Fig. 9. If the APB allows it, the admin transmits the metadata together with the secret key to the TPA for auditing. The TPA submits the auditing report to the admin, who subsequently deactivates the TPA account to prevent the TPA from logging into the system again. These constraints on TPA add to the.

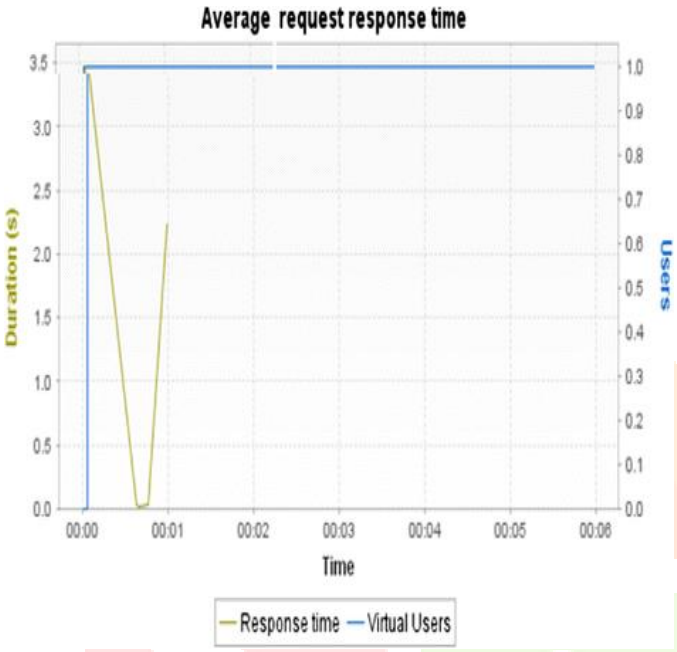
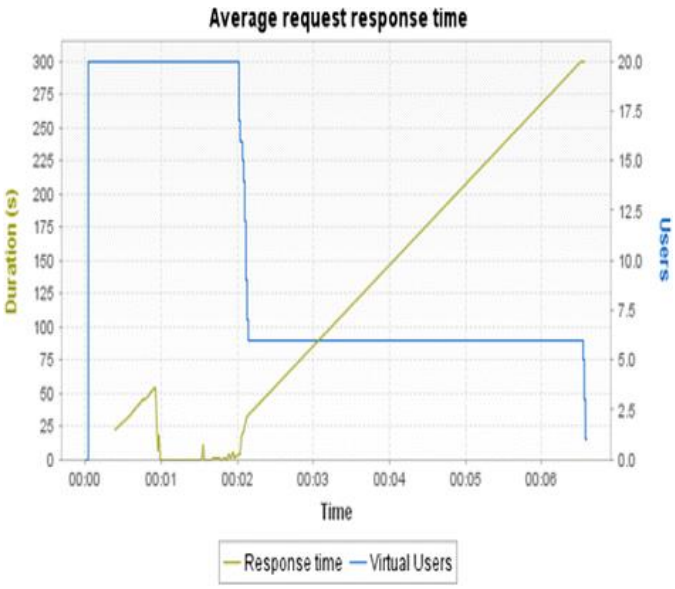


Fig: Average request time for 10 users

The proposed system's throughput (number of gigabytes of data per second) is tested when different numbers of users (i.e., 10 users, 20 users, 50 users) login the system, taking into account the users request time. The system throughput of returned data in megabytes by 10, 20, and 50 users is shown in Figures 13, 14, and 15.

With each rise in the number of queries, the average response time increases. Furthermore, the suggested system's throughput (the amount of megabits of data per second returned by the server) improves as the number of users grows.



CONCLUSION

Propose a brand new symbol-based trie-traverse searching scheme, where a multi-way tree structure is built up using symbols transformed from the resulted expressive keyword sets. Through rigorous security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of expressive keyword search. Extensive experimental results demonstrate the efficiency of the proposed solution.solvedthe issue of public audits while maintaining privacy. A novel secure cloud storage method is presented to protect companies' data from both the cloud provider and third-party auditor, as well as from some users who use outdated accounts to access data stored in the cloud. The suggested system uses two authentication techniques: time-based one-time password (TOTP) and automatic blocker protocol to boost authentication security (ABP).In the proposed system, the data owner has complete control over all privileges, ensuring that only authorized individuals have access to the outsourced data on cloud storage servers. User authentication is verified using two-factor authentication to boost security: the first is performed with a username and password, while the second is triggered by the usage of TOTP. The experimental results show that the suggested approach is effective and efficient at auditing shared data integrity.

REFERENCES:

[1] S. Bell, C. L. Zitnick, K. Bala, and R. Girshick. Insideoutside net: Detecting objects in context with skip pooling and recurrent neural networks. arXiv preprint arXiv:1512.04143, 2015. 6

[2] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. FeiFei. Imagenet: A large-scale hierarchical image database. In Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on, pages 248–255. IEEE, 2009. 1

[3] M. Everingham, L. Van Gool, C. K. Williams, J. Winn, and A. Zisserman. The pascal visual object classes (voc) challenge. International journal of computer vision, 88(2):303– 338, 2010. 1

[4] P. F. Felzenszwalb, R. B. Girshick, and D. McAllester. Discriminatively trained deformable part models, release 4. http://people.cs.uchicago.edu/ pff/latent-release4/. 8

[5] R. B. Girshick. Fast R-CNN. CoRR, abs/1504.08083, 2015. 5, 6

[6] K. He, X. Zhang, S. Ren, and J. Sun. Deep residual learningforimagerecognition.
ArXivpreprintarXiv:1512.03385, 2015. 2, 5, 6
[7] S. Ioffe and C. Szegedy. Batch normalization: Accelerating deep network training by reducing internal covariate shift. arXiv preprint arXiv:1502.03167, 2015. 2, 5
[8] A. Krizhevsky, I. Sutskever, and G. E. Hinton. Imagenet classification with deep convolutional neural networks. In Advances in neural information processing systems, pages 1097–1105, 2012. 2
[9] M. Lin, Q. Chen, and S. Yan. Network in network. arXiv preprint arXiv:1312.4400, 2013. 4
[10] T.-Y. Lin, M. Maire, S. Belongie, J. Hays, P. Perona, D. Ramanan, P. Doll´ar, and C. L. Zitnick. Microsoft coco: Common objects in context. In European Conference on Computer Vision, pages 740–755. Springer, 2014. 1, 6
[11] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, and S. E. Reed. SSD: single shot multibox detector. CoRR, abs/1512.02325, 2015. 5, 6
[12] G. A. Miller, R. Beckwith, C. Fellbaum, D. Gross, and K. J. Miller. Introductiontowordnet: Anon-linelexicaldatabase. International journal of lexicography, 3(4):235–244, 1990. 6
[13] J. Redmon. Darknet: Open source neural networks in c. http://pjreddie.com/darknet/, 2013–2016. 5
[14] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi. You only look once: Unified, real-time object detection. arXiv preprint arXiv:1506.02640, 2015. 5, 6
[15] S. Ren, K. He, R. Girshick, and J. Sun. Faster r-cnn: Towards real-time object detection with region proposal networks. arXiv preprint arXiv:1506.01497, 2015. 2, 3, 5, 6

AUTHORS PROFILE

Dr.R.Hamsaveni received B.Sc Computer Science from Madras University and M.Sc Computer Science Degree from Bharathidasan University, Trichy and M.Phil in Mother Tersa Women's ,Kodaikanal. She completed her Ph.D degree in Computer Science at SCSVMC University. She has 20 years of teaching experience. She is working as Assistant Professor of Computer Science Department in DKM College for Women,(Autonomous),Vellore. She has guided more than 25 M.Phil Research students are completed in various universities. She has published more than 15 research articles in national and international reputed journals. She has presented a paper in International level seminar at various universities and colleges. And her research interests include Network Security and Cloud Computing.