SAFEGUARDING THE DIGITAL WORLD DATA SHARING WITH PROXY RE-ENCRYPTION USING BLOCKCHAIN

Gade Vaishnavi(20641A6726), Btech Student Student, CSD, Vaagdevi College of Engineering

Munjala Vasavi(20641A6747), Btech Student, CSD, Vaagdevi College of Engineering

Jagarlapudi Ram Laxman(20641A6732), Btech Student, CSD, Vaagdevi College of Engineering

Ch. Rajkumar(20641A6757), Btech Student, CSD, Vaagdevi College of Engineering

Mr. Sayyed Hasanoddin, Assistant Professor, CSE (Data Science),Vaagdevi College of Engineering

ABSTRACT

The evolution of the Internet of Things has seen data sharing as one of its most useful applications in cloud computing. As eye-catching as this technology has been, data security remains one of the obstacles it faces since the wrongful use of data leads to several damages. In this article, we propose a proxy re-encryption approach to secure data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while proxy re-encryption construction will grant legitimate users access to the data. With the Internet of Things devices being resource-constrained, an edge device acts as a proxy server to handle intensive computations. Also, we make use of the features of information-centric networking to deliver cached content in the proxy effectively, thus improving the quality of service and making good use of the network bandwidth. Further, our system model is based on blockchain, a disruptive technology that enables decentralization in data sharing. It mitigates the bottlenecks in centralized systems and achieves fine-grained access control to data. The security analysis and evaluation of our scheme show the promise of our approach in ensuring data confidentiality, integrity, and security

1. INTRODUCTION

THE Internet of Things (IoT) has emerged as a technology that has great significance to the world nowadays and its utilization has given rise to an expanded growth in network traffic volumes over the years. It is expected that a lot of devices will get connected in the years ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposes in applications such as healthcare, vehicular networks, smart cities, industries, and manufacturing, among others [1]. The sensors measure a host of parameters that are very useful for stakeholders involved. Consequently, as enticing as IoT seems to be, its advancement has introduced new challenges to security and privacy.

IoT needs to be secured against attacks that hinder it from providing the required services, in addition to those that pose threats to the confidentiality, integrity, and privacy of data.

A viable solution is to encrypt the data before outsourcing to the cloud servers. Attackers can only see the data in its encrypted form when traditional security measures fail. In data sharing, any information must be encrypted from the source and only decrypted by authorized users in order to preserve its protection. Conventional encryption techniques can be used, where the decryption key is shared among all the data users designated by the data owner. The use of symmetric encryption implies that the same key is shared between the data owner and users, or at least the participants agree on a key. This solution is very inefficient. Furthermore, the data owners do not know in advance who the intended data users are, and, therefore, the encrypted data needs to be decrypted and subsequently encrypted with a key known to both the data owner and the users. This decrypt-and-encrypt solution means the data owner has to be online all the time, which is practically not feasible. The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users.

Although simple, the traditional encryption schemes involve complex key management protocols and, hence, are not apt for data sharing. Proxy re-encryption (PRE), a notion first proposed by Blaze et al. [2], allows a proxy to transform a file computed under a delegator's public key into an encryption intended for a delegatee. Let the data owner be the delegator and the data user be the delegate. In such a scheme, the data owner can send encrypted messages to the user temporarily without revealing his secret key. The data owner or a trusted third party generates the re-encryption key. A proxy runs the re-encryption algorithm with the key and revamps the ciphertext before sending the new ciphertext to the user. An intrinsic trait of a PRE scheme is that the proxy is not fully trusted (it has no idea of the data owner's secret key). This is seen as a prime candidate for delegating access to encrypted data in a secured manner, which is a crucial component in any data-sharing scenario. In addition, PRE allows for encrypted data in the cloud to be shared to authorized users while maintaining its confidentiality from illegitimate parties Data disclosures can be minimized through the use of encryption since only users delegated by the data owner can effectively access the outsourced data.

Motivated by this scenario, this article proposes an improvement in IoT data sharing by combining PRE with identity-based encryption (IBE), information-centric networking (ICN), and blockchain technology. Shamir [3] first presented the notion of IBE, in which a sender encrypts a message to a recipient using the identity (email) as the public key. It is a very powerful primitive

used to combat numerous key distribution problems and has consented to the development of several cryptographic protocols, including public-key searchable encryption [4], [5], secret handshakes, and chosen ciphertext attack (CCA) secure public-key encryption [3]. IBE is preferred over attribute-based encryption (ABE) because ABE involves heavy computations on data encryption, decryption, and key management, and these processes are not convenient for the resource-constrained IoT devices. The strength of this article is increased by borrowing the idea of ICN to cater for the growth in information sharing.

The appeal for low-latency applications introduced the notion of ICN [1], where data owners can distribute and assign unique names to their data which can be replicated and saved in network caches [2], [3]. This ensures that there is an efficient data delivery and utilization of network bandwidth, which is a prerequisite for the IoT ecosystem regardless of the enormous growth in network volumes. On issues of trust, a decentralized, distributed system that can smoothen secure and trusted data sharing was introduced by Nakamoto [4]. This is the blockchain technology, and it has gained much attention due to its ability to preserve data privacy. Although there exist optimization issues when storing vast sizes of data, emerging system applications have used the blockchain for access control in database management. Data confidentiality and user revocation can also be achieved using blockchain.

PRE, together with IBE and the features of ICN and blockchain, will enhance security and privacy in data-sharing systems. PRE and IBE will ensure fine-grained data access control, while the concept of ICN promises a sufficient quality of service in data delivery because the in-network caching provides efficient distribution of data. The blockchain is optimized to prevent storage and data-sharing overheads and also to ensure a trusted system among entities on the network. In our article, the data owner propagates an access control list which is stored on the blockchain. Only the authorized users are able to access the data. The contributions of this article are summarized as follows

1) We propose a secure access control framework to realize data confidentiality, and fine-grained access to data are achieved. This will also guarantee data owners' complete control over their data.

2) We give a detailed description of our PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.

3) To improve data delivery and effectively utilize the network bandwidth, edge devices serve as proxy nodes and perform re-encryption on the cached data. The edge devices are assumed to have enough computation capabilities than the IoT devices and as such provide high performance networking.

2. LITERATURE SURVEY

Internet of Things: A survey on enabling technologies, protocols, and applications.

This paper provides an overview of the Internet of Things (IoT) with emphasis on enabling technologies, protocols, and application issues. The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic premise is to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. This paper starts by providing a horizontal overview of the IoT. Then, we give an overview of some technical details that pertain to the IoT enabling technologies, protocols, and applications. Compared to other survey papers in the field, our objective is to provide a more thorough summary of the most relevant protocols and application issues to enable researchers and application developers to get up to speed quickly on how the different protocols fit together to deliver desired functionalities without having to go through RFCs and the standards specifications. We also provide an overview of some of the key IoT challenges presented in the recent literature and provide a summary of related research work. Moreover, we explore the relation between the IoT and other emerging technologies including big data analytics and cloud and fog computing. We also present the need for better horizontal integration among IoT services. Finally, we present detailed service use-cases to illustrate how the different protocols presented in the paper fit together to deliver desired IoT services.

Divertible protocols and atomic proxy cryptography.

First, we introduce the notion of divertibility as a proto- col property as opposed to the existing notion as a language property (see Okamoto, Ohta (OO90)). We give a definition of protocol divertibil- ity that applies to arbitrary 2-party protocols and is compatible with Okamoto and Ohta's definition in the case of interactive zero-knowledge proofs. Other important examples falling under the newdefinition are blind signature protocols. We propose a sufficiency criterion for divertibil- ity that is satisfied by many existing protocols and which, surprisingly, generalizes to cover several protocols not normally associated with di-vertibility[2],[5] (e.g., Diffie-Hellman key exchange). Next, we introduce atomic proxy cryptography, in which an atomic proxy function, in conjunction with a public proxy key, converts ciphertexts (messages or signatures) for one key into ciphertexts for another. Proxy keys, once generated, may be made public and proxy functions applied in untrusted

environments. We present atomic proxy functions for discrete-log-based encryption, identification, and signature schemes. It is not clear whether atomic proxy functions exist in general for all public-key cryptosystems. Finally, we discuss the relationship between divertibility and proxy cryptography.

3. PROBLEM STATEMENT

combined key-policy ABE (KP-ABE) and PRE to propose a system for data sharing in the cloud. The data was encrypted using KP-ABE which meant that only an appropriate collection of the attribute secret keys can make decryption possible. Besides the encrypted data, the cloud also managed all attribute secret keys except one special secret key in order to handle revocation of users. When users are revoked, new keys were distributed to the remaining users by the data owner and the encrypted data had to be re-encrypted.

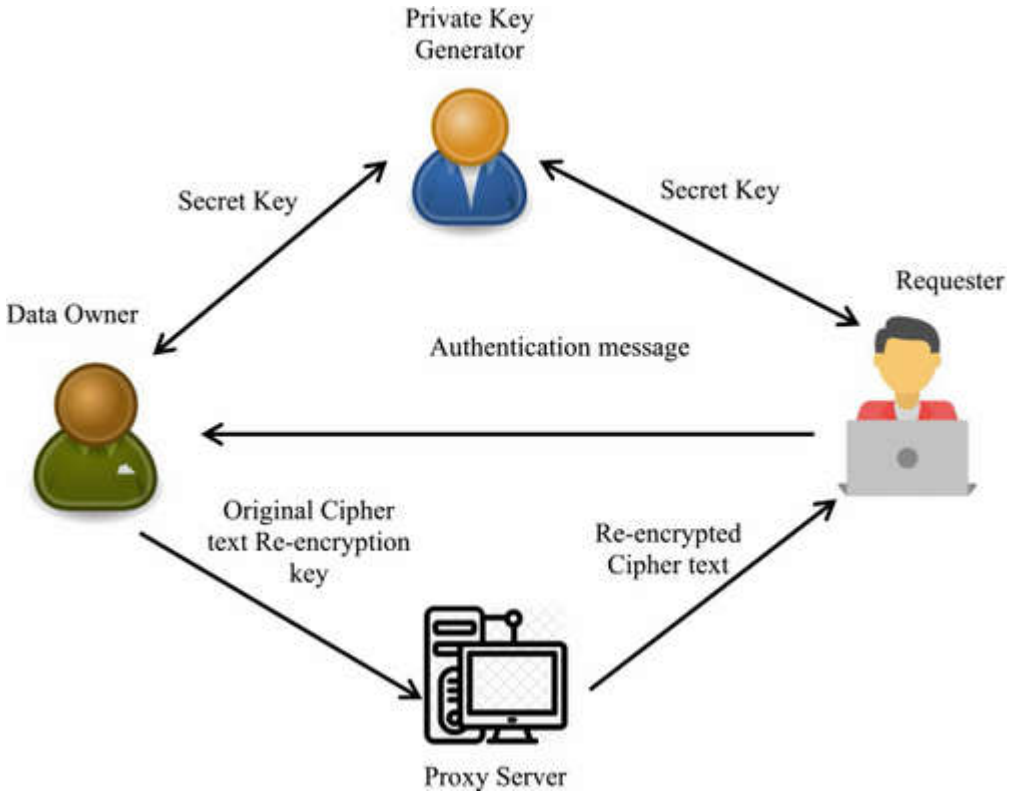
3.1 LIMITATION OF SYSTEM

The re-encryption was performed in a lazy way, and, therefore, the security of the scheme was weakened. provided a modification to the scheme in, where collusion between the service provider and revoked users is avoided

4. PROPOSED SYSTEM

Our system model introduces a blockchain-based PRE approach to data sharing. The additional entities to the data-sharing model as discussed in Fig. 1 are the edge devices and the blockchain. The edge devices serve as proxy nodes and provide re-encryption services to the authorized user(s). When the data is cached at the edge of the network, the edge devices provide services to users with high availability and performance. They receive the re-encryption key from the data owner, fetch the ciphertext from the CSP[5], and transform the ciphertext in the identity of the data user. It is an honest-but-curious entity.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

6.1.DATA OWNER

Data owner should register with the application then login into application after successful login he can perform some operations such as encrypt and upload files into cloud, view all uploads and view request and send re-encrypt request to proxy server with user identity and logout.

6.2.DATA USER

Data user should register with the application then login into application after successful login he can perform some operations such as can search a file and send request to block chain and view response and decrypt file and download files and logout.

6.3.TRUSTED AUTHORITY(BLOCK CHAIN)

Here trusted authority can directly login with the username and password then perform some operations such as view users and owners generate membership key and view all submitted data by proxy server and logout.

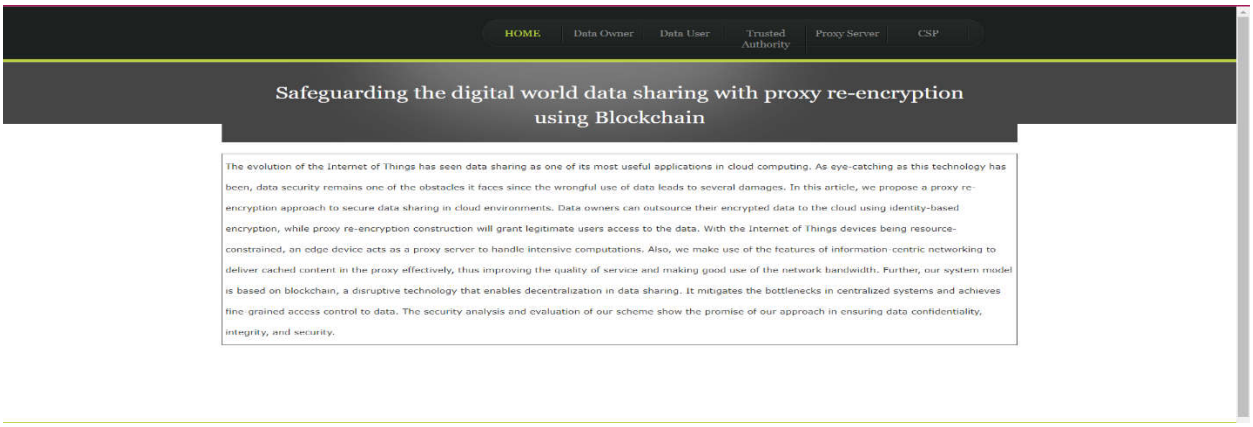
6.4.PROXY SERVER

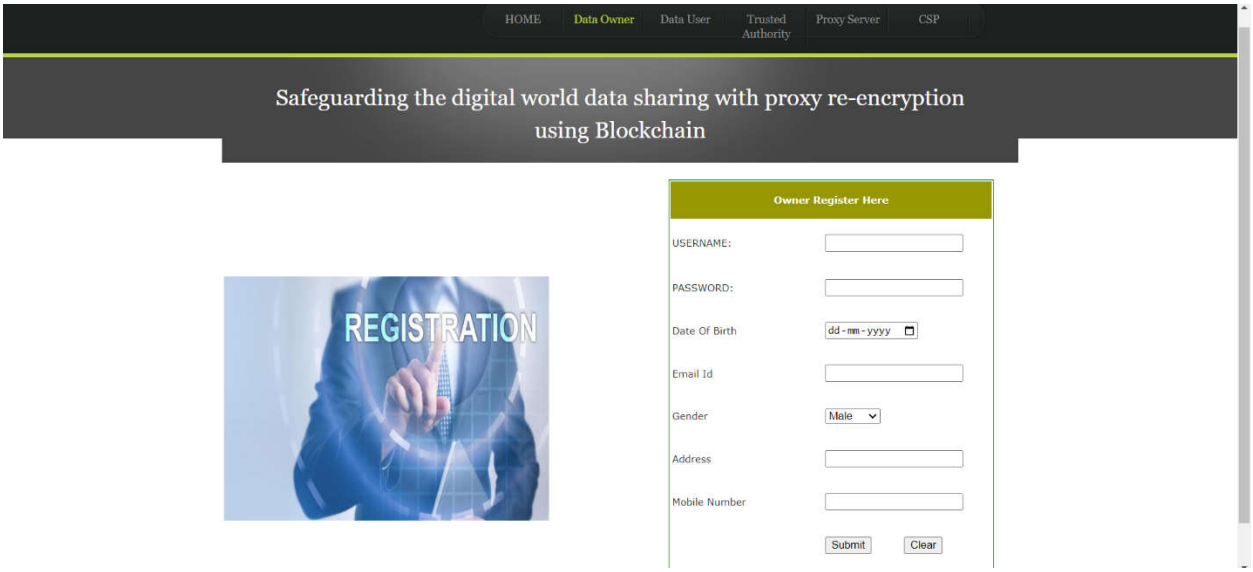
Here proxy server can directly login with the username and password then perform some operations such as view re-encrypt request and get response from cloud like url and upload to block chain,user and logout.

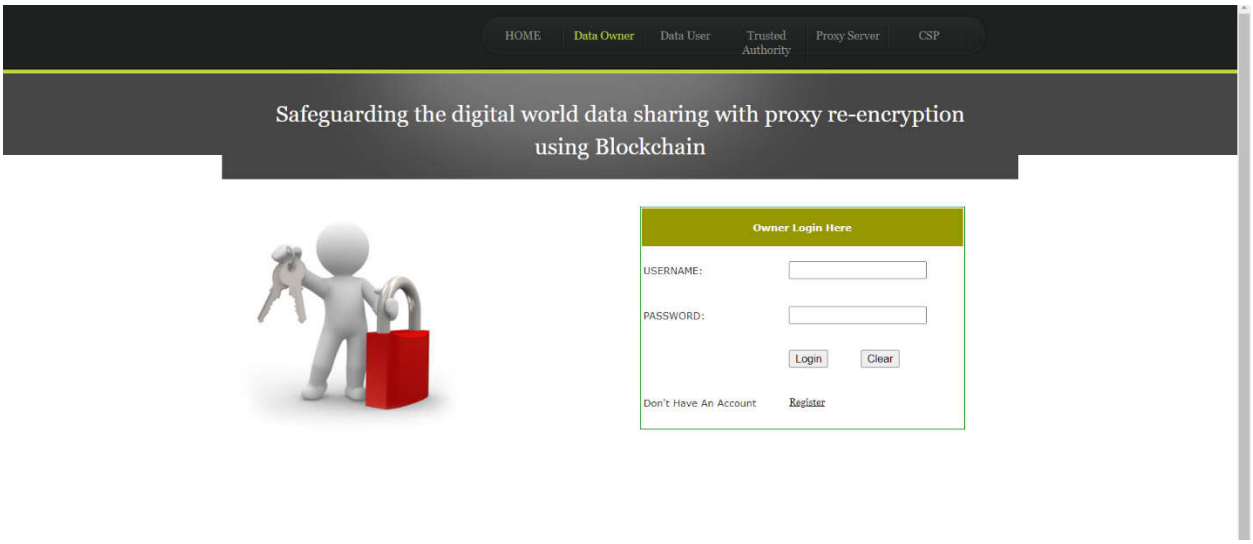
6.5.CSP

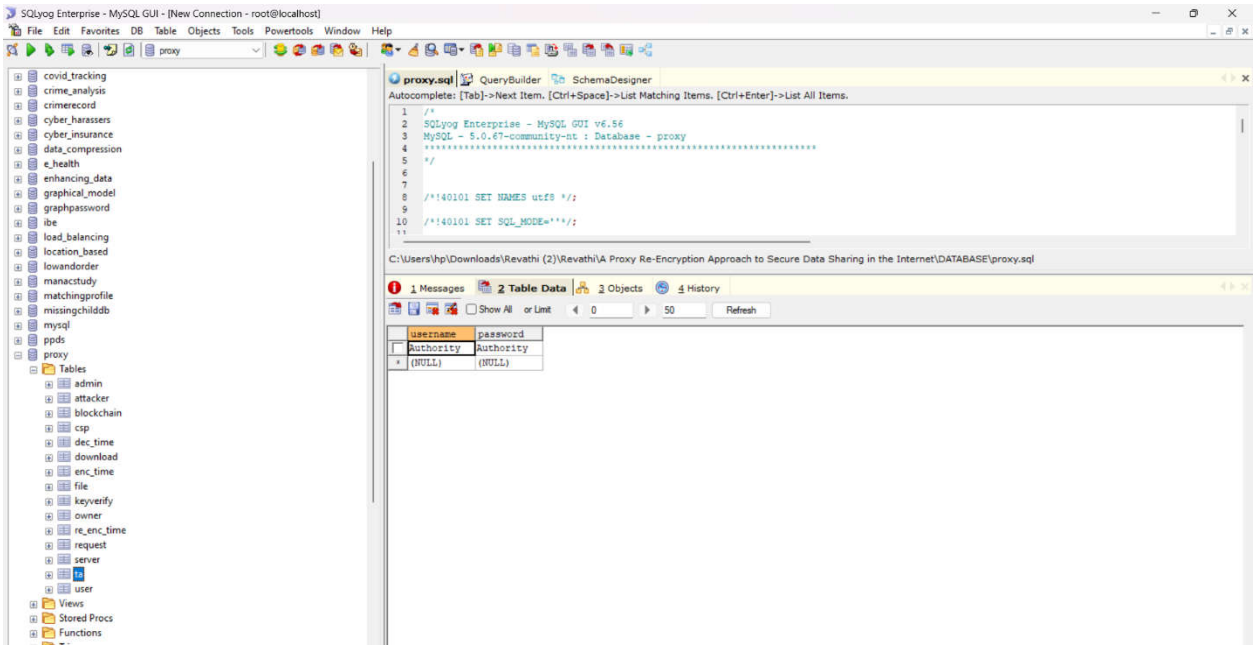
Here CSP can directly login with the username and password then perform some operations such as view all files and view all request and response and encryption time graph and re-encryption time graph and decryption time graph and all download graph and attacked file graph and logout.

7. OUTPUT EXPERIMENTS









8. CONCLUSION

The emergence of the IoT has made data sharing one of its most prominent applications. To guarantee data confidentiality, integrity, and privacy, we propose a secure identity-based PRE data-sharing scheme in a cloud computing environment. Secure data sharing is realized with IBPRE technique, which allows the data owners to store their encrypted data in the cloud and share them with legitimate users efficiently. Due to resource constraints, an edge device serves as the proxy to handle the intensive computations. The scheme also incorporates the features of ICN to proficiently deliver cached content, thereby improving the quality of service and making great use of the network bandwidth. Then, we present a blockchain-based system model that allows for flexible authorization

on encrypted data. Finegrained access control is achieved, and it can help data owners achieve privacy preservation in an adequate way. The analysis and results of the proposed model show how efficient our scheme is, compared to existing schemes.

Future Scope

The blockchain-based system model further enhances the security and privacy of data sharing by enabling flexible authorization on encrypted data. Fine-grained access control ensures that data owners have granular control over who can access their data, thus preserving privacy in a robust manner. In conclusion, the analysis and results of the proposed model demonstrate its efficiency and effectiveness compared to existing schemes. However, there are still avenues for future exploration and enhancement:

1. Scalability: Investigate methods to scale the proposed scheme to accommodate larger IoT deployments and increasing data volumes.
2. Interoperability: Explore ways to ensure seamless integration with diverse IoT devices, platforms, and protocols to enhance interoperability.
3. Security Enhancements: Continuously improve security measures to mitigate emerging threats and vulnerabilities, ensuring the long-term resilience of the system.
4. Optimization: Further optimize the system's performance, particularly in terms of computational overhead and response times, to provide a seamless user experience.

5. Standardization: Advocate for standardization efforts to promote adoption and interoperability across different IoT ecosystems.

9. REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347–2376, Oct./Dec. 2015.

[2] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 1998, pp. 127–144.

[3] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984, pp. 47–53.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 2004, pp. 506–522.

[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in NDSS, vol. 4. Citeseer, Feb. 2004, pp. 5–6.

[6].CHARY, D. C. N., BABU, M. R., & MORE SADANANDAM, S. K. (2023). Leveraging Deep Learning Techniques for the Stability Principles of Current Artificial Neural Networks Are Emerging Into Their Activation Functions.

[7].CH, D. (2021). NARASIMHA CHARY,”. COMPREHENSIVE STUDY ON MULTI-OPERATOR BASE STATIONS CELL BINARY AND MULTI-CLASS MODELS USING AZURE MACHINE LEARNING”," A JOURNAL OF COMPOSITION THEORY, 14(6).