ISSN: 2366-1313

SERVER SECURITY IN CLOUD COMPUTING USING BLOCKCHAIN

[1]Mrs.Nvn.Sowjanya,[2]K.Krishna Charit Vyas,[3]K.Bindu Priya,[4]M.Jyosna,[5]M.Meghana

[1]Assistant Professor, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

sowjanya.nvn@gmail.com

[2, 3, 4, 5, BTech] Student, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

Krishancharitvyas.kurra@gmail.com,Kashapakabindu@gmail.com,mukkerajyosna14@gmail.com,methukumeghana70@gmail.com

ABSTRACT:

In modern times, sharing data is the one of the very few things which is done by anyone and everyone. Much of this sharing is done digitally, i.e., over the internet, which makes it the most recurrent way of doing the sharing globally. Enablement of the sharing is aided using copious Cloud Service Providers, allowing the end user, not only the ability of sharing the data but also, storing it. But with the amenities, comes the risk of intentional and unintentional manipulation of the tons of data that is stored and shared in every minute. Breaches like Data Piracy, Hack Attacks etc. are the most common threats that tempers with security of the cloud in these times. It is the need of the hour to make the sensitive data stored by the user safe from intentional/unintentional misuse/manipulation. Thereby, it is necessary to make this system more secure to ensure and maintain the confidentiality of the user data. In this paper, we have ventured the introduction of a system that anchorage Block chain for securing the data over the cloud. To ensure safety of the user's data, block chain enables a prominent Controlled Access Mechanism. This mechanism accredits the user to share personalized hyperlinks deliberated to a single user. This approach logs details of all the actions and operations that are being done on or with the data and are at owner's disposal at all points. Actual Proprietary and privacy are few of the many benefits which are provided by this solution ensuring a more secure cloud space for the data.

Keywords: Block chain, Cloud Computing.

ISSN: 2366-1313

I INTRODUCTION

We need to stay updated because as the technology is advancing so are the hackers, crackers and people with a destructive mindset. Procedures and technologies securing cloud environment enablers resistant to both implicit and explicit security related threats are necessitated under Cloud Security. No matter how secure the system is, it always is vulnerable in some way or the other. Like for instance, Cloud flare a renowned cloud security service provider publicized that back in 2016, a censorious bug in one of its software caused a data leak and that affected at least 2 million websites, which including many internet companies such as uber and 1password. . Hence, block chain technology came into the picture. Initial introductory of the Block chain technology was made through the introduction of Bit coin. As Block chain is a known to be a crystalline mechanism which provides secured and innominate transactions, many crypto currencies and many others utilize it. Every transaction or process that takes place is recorded as a "block". Those are then connected with the ones before and after. Processes or Transactions are locked together in the form of an irreversible chain, hence, creating a block chain, improvising on the security of the data, including, and not limited to privacy and integrity of the data

II. LITERATURE SURVEY

"Using Blockchain in Cloud Computing to Enhance Relational Database Security"

Cloud computing has now become a very standardized concept in our society. However, many modern applications need a better level of security that includes saving data from internal breaches. Thus, cloud databases need effective security mechanisms to keep track of data modifications. This paper will introduce the enhanced structure of cloud relational database (RDB) based on blockchain technology (BC) named BC over cloud-RDB. Through a self-verification mechanism, it enables the client to detect and prevent erroneous RDB manipulation. We proposed two systems to improve cloud-RDB namely, agile BC-based RDB and secure BC-based RDB. Both are distributed among several cloud service providers based on the Byzantine Fault Tolerance consensus. Additionally, both rely on linking records to each other using the SHA-256. At the same time, secure BC-based RDB uses a proof-of-work consensus to make data offensive operation impossible. On the basis of

ISSN: 2366-1313

performance of both systems' and security analysis, the agile BC-based RDB is highly suggested for the high throughput database. On the other hand, the secure BC-based RDB is recommended for RDB that contains sensitive data and low throughput performance. The improved RDB is flexible and can be operated according to the data owner's specifications

"A survey on blockchain for information systems management and security"

Blockchain technologies have grown in prominence in recent years, with many experts citing the potential applications of the technology in regard to different aspects of any industry, market, agency, or governmental organizations. In the brief history of blockchain, an incredible number of achievements have been made regarding how blockchain can be utilized and the impacts it might have on several industries. The sheer number and complexity of these aspects can make it difficult to address blockchain potentials and complexities, especially when trying to address its purpose and fitness for a specific task. In this survey, we provide a comprehensive review of applying blockchain as a service for applications within today's information systems. The survey gives the reader a deeper perspective on how blockchain helps to secure and manage today information systems. The survey contains a comprehensive reporting on different instances of blockchain studies and applications proposed by the research community and their respective impacts on blockchain and its use across other applications or scenarios.

"Establishing Trust despite attacks in cloud computing: a survey"

Cloud computing has become an integral part of our lives as it provides ondemand, rapid provisioning of services with ease of implementation, accessibility and flexibility. The pay-as-you-use aspect is very attractive for customers who usually pay fixed price for resources whose usage does not tally with the cost of purchase. In this paper, we present a survey on security in cloud computing despite various attacks. It presents the various security aspects in the services provided by the cloud such as IaaS, PaaS and SaaS. Since virtualization is used vastly in cloud, we take a look at the various attacks virtual machines are subjected to. Trusted computing was introduced for the customers to be assured that the resources they use over cloud is reliable. Further, we also observe how remote attestation plays a role to assure trustworthiness and how the Trusted Platform Module is used in the

ISSN: 2366-1313

attestation mechanism. The paper thus provides an overall view of existing techniques to secure and trust cloud and its components.

III SYSTEM ANALYSIS

EXISTING SYSTEM

The existing system for the project titled "Server Security in Cloud Computing Using Blockchain" addresses the prevalent challenges associated with data sharing and storage in the digital landscape. In the current scenario, where the majority of data sharing occurs digitally over the internet, Cloud Service Providers play a crucial role in facilitating this process. However, this convenience is accompanied by significant risks, including intentional and unintentional manipulation of vast amounts of data, leading to common threats such as Data Piracy and Hack Attacks. Recognizing the urgency to bolster the security of cloud systems and protect sensitive user data from potential misuse, the existing system proposes the integration of Blockchain technology. By anchoring Blockchain for securing data over the cloud, the system introduces a Controlled Access Mechanism. This mechanism empowers users with personalized hyperlinks, tailored to individual data access, while logging all actions and operations for transparency and accountability. The use of Blockchain ensures data integrity, tamper resistance, and a decentralized ledger, providing users with a more secure cloud space and addressing the imperative need for maintaining the confidentiality of user data in the digital age.

Limitations of Existing System

Scalability Challenges:

Blockchain systems, especially those based on public decentralized networks, may face scalability challenges as the number of users and transactions increases. This can potentially impact the performance of the system, leading to delays and higher resource requirements

Integration Complexity:

Integrating Blockchain technology into existing cloud computing infrastructure can be a complex task. Ensuring seamless interoperability with diverse cloud service providers and applications may pose challenges and require significant development efforts.

Energy Consumption:

The consensus mechanisms employed in many Blockchain networks, such as Proof of

ISSN: 2366-1313

Work (PoW), can be energy-intensive. This poses environmental concerns and may be a limitation for cloud-based systems aiming for sustainability and reduced energy consumption.

PROPOSED SYSTEM

The proposed system titled "Server Security in Cloud Computing Using Blockchain" aims to revolutionize the security paradigm of cloud-based data storage and sharing. Building upon therecognition of vulnerabilities in the existing system, the proposed framework introduces a robust security architecture by leveraging Blockchain technology. The core innovation lies in the implementation of a Controlled Access Mechanism, facilitated by Blockchain, which grants users personalized hyperlinks for data access while ensuring the integrity and confidentiality of the stored information. Smart contracts play a pivotal role in automating and enforcing access control rules within the Blockchain network. The system not only addressesthe pressing concerns of intentional and unintentional data manipulation but also enhancestransparency and accountability by maintaining a detailed and immutable log of all user actions. Through the integration of Blockchain, the proposed system offers heightened security features, such as tamper resistance and decentralized consensus, thereby establishing a more trustworthy and resilient cloud space for sensitive user data. The envisaged benefits encompass enhanced security, user privacy, and a streamlined approach to data management in the cloud.

Proposed system Advantages:

Enhanced Security Through Blockchain:

The incorporation of Blockchain technology fortifies the security of the cloud system by providing a tamper-resistant and decentralized ledger.

Controlled Access Mechanism:

The proposed Controlled Access Mechanism, enabled by Blockchain, introduces a personalized and user-centric approach to data access. Users are granted unique hyperlinks, offering a fine-grained control over who can access their data, thereby reducing the risk of unauthorized sharing.

Transparent and Immutable Log:

The system maintains a detailed and immutable log of all actions and operations performed onthe data. This transparency enhances accountability, allowing users to track and verify every interaction with their stored information, thereby mitigating the

ISSN: 2366-1313

risk of data breaches and ensuring data integrity.

Privacy Assurance:

Through the use of Block chain's cryptographic techniques and controlled access mechanisms, the proposed system ensures a higher level of privacy for user data. Users have greater control over who can access their data, reducing the likelihood of unintentional exposure or unauthorized sharing.

IV IMPLEMENTATION

Architecture:

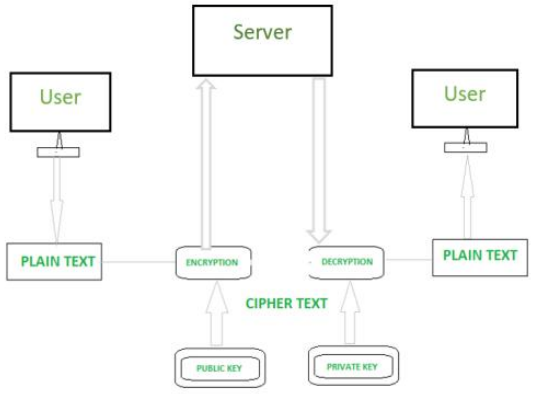


Fig-1. Architectures of the system model

When the user want to upload the data which may be in the form of plain text or image or videoetc. After uploading the data it encryptes the data by using public key and it stores into the server when the user wants to retrive the data by using the Decryption with the help of the private key he can access the data which is in encrypted format.

MODULES

Blockchain Integration Module:

This module focuses on integrating Blockchain technology into the existing cloud infrastructure. It includes the deployment of smart contracts, consensus mechanisms, and cryptographic techniques to establish a tamper-resistant and decentralized ledger for secure data transactions.

Controlled Access Mechanism Module:

The Controlled Access Mechanism module is designed to implement personalized and fine-grained access controls for user data. It involves the generation of unique hyperlinks for data access, smart contract development to enforce access rules, and mechanisms for user friendly management of access permissions.

Smart Contracts and Automation Module:

Smart contracts play a crucial role in automating and enforcing the access control policies defined within the system. This module involves the development and

ISSN: 2366-1313

deployment of smart contracts to facilitate automated, trustless, and transparent execution of predefined rules for data access and sharing.

User Interface Module:

The User Interface module focuses on creating a user-friendly front-end for seamless interaction with the Blockchain-based security system. It includes features for generating personalized access links, monitoring data access logs, and managing user-specific security settings. A well-designed interface enhances user experience and facilitates effective utilization of the system.

Logging and Monitoring Module:

This module is dedicated to capturing and storing detailed logs of all user actions and operations performed on or with the data. It includes mechanisms for time stamping, logging, and storing these activities in a secure manner. Blockchain Integration Module: Controlled Access Mechanism Module: Smart Contracts and Automation Module: User Interface Module: Logging and Monitoring Module:

Procedure

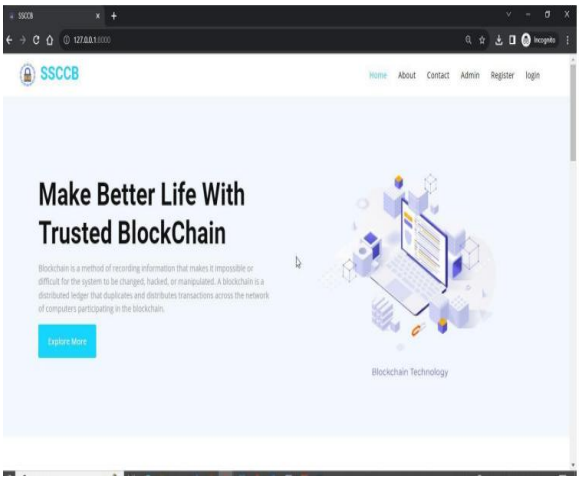
- Frist we need to install Python 3.10.7 and install the Python server by using pip install python -server
- After that we need to install the MYSQL database and set the passwordas the “root”. And the Username as the root
- Then install Django Server by using pip install python-django
- After installing the Django we need to install the date and time in the command prompt by using the pip install -dateandtime.
- After that we have to run rs before the server run by using the pip install -rs which means before the main server we should have to run rs
- Then we have to run run the Server and it gives the http urlhttp://127.0.0.1:8000/login_page
- By using the given link it opens the HTML then we can login and register as well as admin also
- If the user wants to login then Admin have to accept the request of the client then only the user can have the access to login he can upload the data and download the data whenever he want. The data may be in the form of Picture or text or video or song etc.

ISSN: 2366-1313

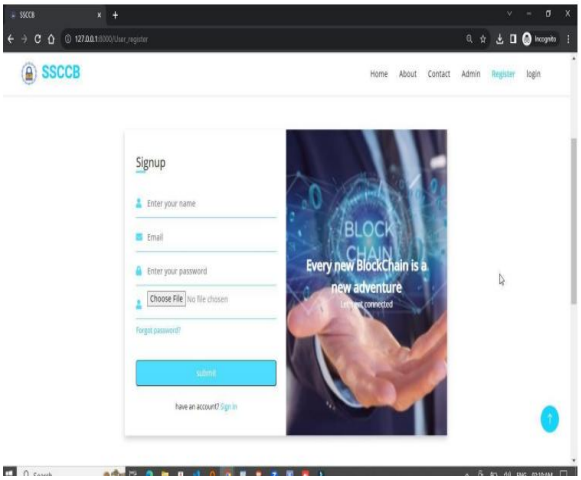
• When we upload the it will send a private key to our email by using that private key we can have download the data from cloud to into our file

V RESULT AND DISCUSSION

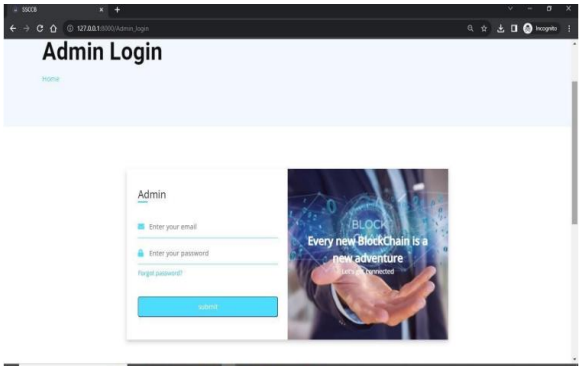
Home page:



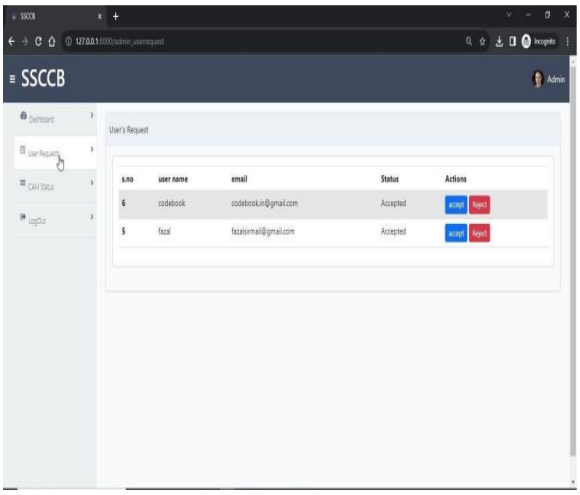
Registration Page:



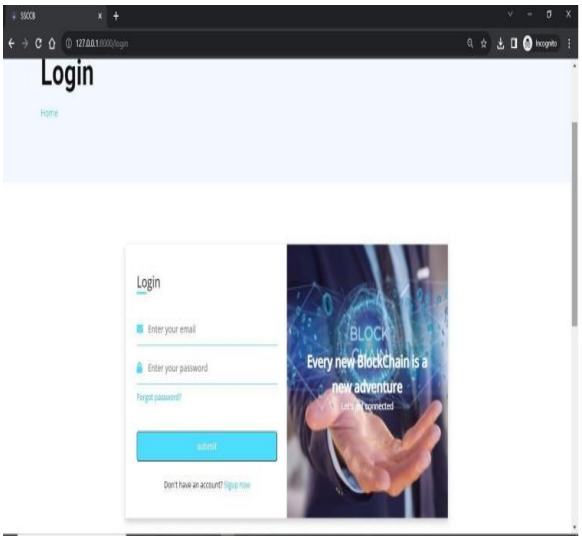
Admin Login Page:



User Request:

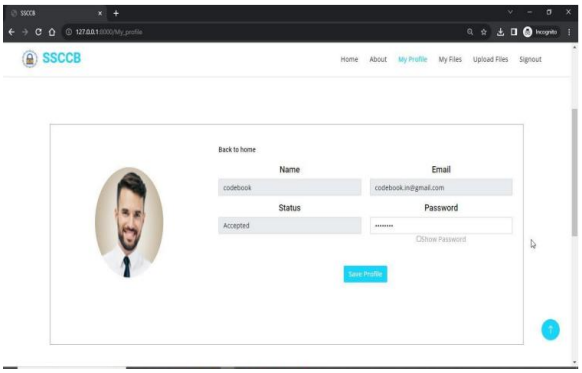


User login page:

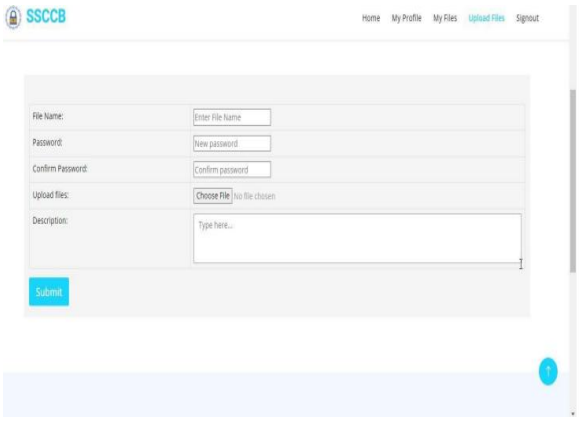


User Details:

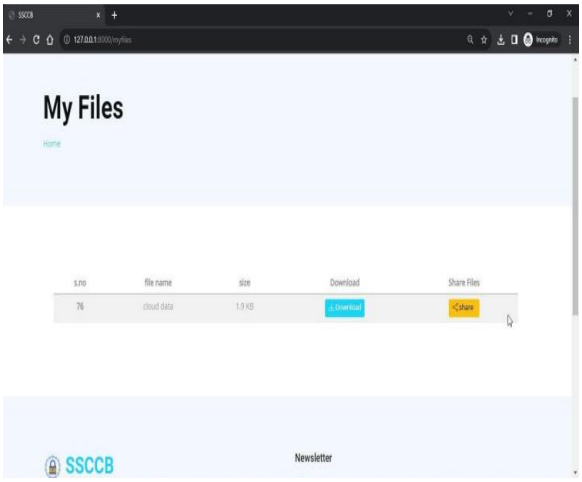
ISSN: 2366-1313



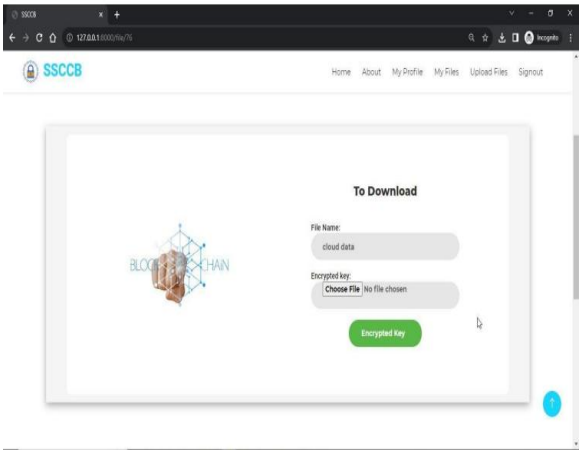
Uploading files:



Files Status



Download From Cloud:



VI CONCLUSION

In this paper, we have proposed for integration of cloud computing development with block chain development for giving predominant security in the cloud environment. This paper confirms the integration of cloud advancement with block chain advancement by showing up exploratory results done by the computer program utilizing java programming language. Block chain integration with cloud security makes a distinction in getting the result more secure and specific for the users as well as the clients in various ways like RSA Algorithm is used for encryption as well as decryption on the text file mentioned above. Storing the encrypted file in the cloud. Agreeing to a large wide variety of papers which have been investigated, most clients and analysts of the block chain pay extra consideration to the utility of block chains and innovation itself, however much

ISSN: 2366-1313

less attention and research to security. We think block chain secrecy research and higher level security, particularly application layer security calls for persistent consideration and research. I'm hoping that the paintings of this paper can alarm the professionals.

FUTURE ENHANCEMENT

There are several promising areas for future enhancements in server security for cloud computing using blockchain:

- Scalability Solutions: Researchers are actively developing new consensus mechanisms and sharing techniques to improve the scalability of blockchain for cloud environments. These advancements aim to enable faster transaction processing and handling of larger data volumes.
- Integration with SDN (Software-Defined Networking): Merging blockchain with SDN offers exciting possibilities. SDN provides dynamic control over network traffic, and blockchain can secure communication and enforce access policies. This combination could lead to a more secure and programmable cloud infrastructure.
- Hybrid and Permissioned Block chains: Public blockchains, while secure, might not be ideal for all cloud security needs. Permissioned blockchains, where access is restricted, and hybrid models combining public and private elements are being explored to provide a balance between security, scalability, and control for cloud providers and users.
- Privacy-Enhancing Techniques: Data privacy is a major concern in cloud computing. Future advancements in blockchain could include integrating privacy preserving techniques like holomorphic encryption, allowing computations on encrypted data without decryption. This would enable secure data processing and analysis in the cloud while maintaining user privacy.
- Self-Sovereign Identity (SSI): SSI empowers users to control their identities in the cloud. Blockchain can be used to create a secure and tamper-proof record of user identities and access rights. This would enhance security and streamline access management in cloud environments

VII REFERENCES

[1] Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, Reji Thomas, Tai-Hoon Kim, "ProofOf-Work Consensus Approach In Blockchain Technology For Cloud And Fog

Computing Using Maximization-Factorization Statistics", IEEE Vol-6 Issue-4, 2019

[2] M.Banerjee, J.Lee, KKR Choo, "A blockchain future to Internet of Things security: A position paper, Digital Communications and Networks", 2017

[3] Yutao Jiao, Ping Wang, DusitNiyato, KongrathSuankaewmanee, "Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks", IEEE vol-30 issue-9, 2019

[4] Prasadu Peddi (2023). AI-Driven Multi-Factor Authentication and Dynamic Trust Management for Securing Massive Machine Type Communication in 6G Networks. International Journal of Intelligent Systems and Applications in Engineering, 12(1s), 361–374.

[5] Ruizhe Yang, F. Richard Yu, Pengbo Si, Zhaoxin Yang, Yanhua Zhang, "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges", IEEE vol-21 issue 2, 2019

[6] RubaAwadallah and AzmanSamsudin, "Using Blockchain in Cloud Computing to Enhance Relational Database Security", IEEE, vol-9, 2021

[7] Wenjuan Li, Jiyi Wu, Jian Cao, Nan Chen, Qifei Zhang and RajkumarBuyya, "Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions", Springer, 2021 [8] M.Chandni, N. P. Sowmiya, S. Mohana, M. K. Sandhya, "Establishing Trust despite attacks in cloud computing: a survey", IEEE, 2017

[9] Enas F. Rawashdeh, Inas I. Abuqaddom, Amjad A. Hudaib, "Trust models for services in cloud environment: a survey", IEEE, 2018

[10] Prasadu Peddi (2015) "A review of the academic achievement of students utilisinglarge-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.

AUTHORS

Mrs. Nvn.Sowjanya,Assistant Professor Dept. of CSE, Teegala Krishna Reddy Engineering College Meerpet, Hyderabad.

Email: sowjanya.nvn@gmail.com

Mr. K.Krishna Charit Vyas, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: Krishancharitvyas.kurra@gmail.com

Miss. K.Bindu Priya, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: Kashapakabindu@gmail.com

Miss. M.Jyosna, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: mukkerajyosna14@gmail.com

ISSN: 2366-1313

Miss. M.Meghana, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.

Email: methukumeghana70@gmail.com