Decentralized Identity and Access Management platform using blockchain

L D Mukil,Kevansh Reddy ,Pranav Krishnan M, Madhav Manoj,Shinu M Rajagopal*,Niharika Panda*
Dept. of Computer Science and Engineering.
Amrita School of Computing,Bengaluru, Amrita Vishwa Vidyapeetam,
India
BL.EN.U4CSE21109@bl.students.amrita.edu,BL.EN.U4CSE21199@bl.students.amrita.edu,
BL.EN.U4CSE2113@bl.students.amrita.edu,BL.EN.U4CSE2116@bl.students.amrita.edu
mr_shinu@blr.amrita.edu ,p_niharika@blr.amrita.edu

***Abstract*—Implementing a decentralized Identity and Access Management (IAM) platform using blockchain technology involved meticulous steps. Understanding platform needs and selecting a suitable blockchain were crucial aspects. A robust data model was designed, and smart contracts were deployed for automation. Integration with cloud services and implementing strong identity verification were essential components. User-friendly interfaces were developed, and rigorous testing ensured platform integrity. Community engagement facilitated adoption, resulting in a revolutionary IAM platform for cloud services.**

***Index Terms*—Decentralized Identity,Blockchain Technology,Access Control Policies,Smart Contracts,Security Posture**

I. Introduction

In today's digital landscape, organizations of all stripes place importance on securing and providing efficient access to their resources and services. However, traditional access control systems have some weaknesses: they are single points of failure and are not very transparent, and while doing so, they become vulnerable to unauthorized entry. So, decentralized identity and access management on a blockchain is the answer.

This decentralized platform for IAM using blockchain entails getting acquainted with the platform requirements, picking a proper blockchain platform, designing a solid data model, developing smart contracts, integration with cloud service, improvement of security measures, development of user interfaces, testing and auditing, and the involvement of the community.[7] This comprehensive program holds the promise for the revolution of IAM for cloud services, contributing enormously to the security assurance strategies in today's digital environment.

Vulnerabilities of Centralized Systems: Single points of failure are their points of vulnerability to an unauthorized breach and access attempt. Lack of Transparency: Systems of a traditional nature are opaque and, thus, provide inefficient visibility into access activities, presenting an obscure way of tracking and monitoring user interactions. Wasteful Authorization Processes: Manual authorization processes are time-wasting, and at times, errors involved may delay operations.

II. Societal impact / how is your project beneficial to the society

The implementation of an IAM system for cloud resources using Amazon Managed Blockchain (AMB) and AWS services provides huge benefits to society.

High Security and Privacy Enhanced: The use of blockchain technology for identity management and access control policies ensures further security and privacy for both the user and the organization. Invariable records of identity verification and access permissions save against probable data breaches and unauthorized access, further protecting sensitive information and potentially reducing harm to individuals and organizations.

Transparency and Accountability: The use of blockchain ensures the transparency and accountability of the IAM system. Each transaction and change in access permissions is recorded on the blockchain and thereby provides an audit source transparent to parties with access authorization. This, in turn, builds stakeholders' trust, and accountability means fraud risk is less likely to happen.

Protection against Identity Theft and Fraud: This project, through the effective process of determining identity and access control policies, highly reduces identity theft and fraud. Users can also gain a greater level of confidence regarding the security of their identities and digital property, thus creating a safer online environment and minimizing financial loss from fraud.

Enabling Regulatory Compliance: The project supports and ensures that organizations act in compliance with necessary laws and regulations that advance, protect, and guard against data breaches and invasion of privacy. This is made possible by ensuring the IAM system incorporates rigid security measures, encryption, and auditing that comply with GDPR and HIPAA.

Empowers Individuals: A secure and user-centric way to manage the digital identity of individuals ensures that the user is in total control of their digital identity profile and personal data. Privacy and consent rights can be respected by the users, typically promoting autonomy and self-determination in digital environments.

Supporting Economic Growth and Innovation: The success of the IAM system solidifies security infrastructure, resulting

in the adaptation of cloud computing technologies that lead to innovation and the overall growth of the economy. Business enterprises can access innovative and scalable cloud resources that are highly secure for fostering innovative products and services, which can lead to job creation and, in the process, prosperity in society.

Inclusivity and Accessibility: The IAM system ensures inclusivity and accessibility through secure access to digital services, consequently allowing different types of people from all walks of life to utilize them. This project, for that reason, avoids barriers and results in an essential bridge to the digital divide and promotes social inclusivity.

In summary, the implementation of an IAM system using blockchain technology and AWS services increases security and privacy, fosters transparency and accountability, ensures regulatory compliance, empowers individuals, supports economic growth and innovation, and promotes inclusivity and accessibility. Place these social benefits on record to understand the positive impact of the project on creating a more risk-controlled, safe, and fair digital environment for all stakeholders.

RELATED WORKS

The objective of the paper is to propose a novel decentralized and dynamic Single Sign-On (SSO) identity access management system tailored for multi-application outsourcing in cloud environments, addressing challenges while leveraging emerging technologies for enhanced security and scalability. This paper presents a novel solution for decentralized and dynamic Single Sign-On (SSO) identity access management in cloud outsourcing, improving security and scalability while taking into consideration the dynamism of evolving cloud environments. Its novel approach leverages emerging technologies to decrease risks and make the control of access smoother across multiple applications. The existing literature lacks comprehensive solutions that effectively address both the decentralization and dynamic nature of Single Sign-On (SSO) identity access management systems for multi-application outsourcing in cloud environments.[1]

The goal of the paper is to investigate and propose blockchain-based decentralized solutions to make data transfer more secure, efficient, and reliable in cloud environments. A novel contribution that takes advantage of blockchain technology in decentralizing cloud solutions to enhance security, reliability, and efficiency of data transfer, meanwhile reducing the associated risks with centralized systems. A research gap of not having such a full study of blockchain-based decentralized solutions for optimizing data transfer within cloud domains indicates the scope for further research and development in this area. [2]

The goal of the paper is to propose and investigate the effectiveness of BIA as a blockchain-based identity authorization mechanism for further enhancement ofsecurity and efficiency in digital identity management systems. A novel contribution that will introduce BIA for blockchain-based identity authorization to enhance security, transparency, and resiliency against unauthorized access to address the vital concerns in the area of digital identity management. A research gap of not having such a complete individual study in the past related to blockchainbased identity.[3]

The purpose of the paper is to introduce and assess a blockchain-based authentication and security mechanism developed to optimize the security and integrity of IoT systems, covering vulnerabilities and ensuring trust in data exchange. This paper provides an innovative blockchain-based authentication and security mechanism for IoT that provides higher data integrity, prevention from tampering, and a better decentralized trust mean to decrease risks and increase reliability in IoT ecosystems. The research gap is that very little detailed research is available that focuses exclusively on blockchain-based authentication and security mechanisms made to meet the special requirements and limitations of IoT settings. Thus, exploration and development must occur to assist in solving the emerging issues of IoT security.[4]

The objective of the paper is to propose and evaluate a blockchain-based authentication and authorization framework designed to enhance the security, privacy, and trustworthiness of smart city applications, addressing vulnerabilities and ensuring secure access control in a decentralized manner.The paper introduces a blockchain-based authentication and authorization framework for smart city applications, offering enhanced security, transparency, and decentralization, thereby mitigating risks associated with centralized authentication systems and ensuring the secure access control in the dynamic urban environment.The gap is the fact that blockchain-based authentication and authorization mechanisms for smart city applications are infrequently exposed in accordance with their complex and diversified requirements, therefore calling for further research to resolve the new security and scalability challenges of the urban environment.[5]

The objective of the paper is to propose, implement, and evaluate BCTrust, a decentralized authentication mechanism based on blockchain technology, aiming to enhance security, transparency, and resilience in identity management and access control systems. The paper introduces BCTrust, a decentralized authentication mechanism based on blockchain technology, enhancing the security, transparency, and trust of identity management systems while reducing risks associated with centralized authentication methods. The research gap here is related to the little discussion of the decentralized authentication mechanisms specifically designed for a blockchain environment; thus, the need for further research to tackle the emerging challenges of identity management and access control within decentralized systems.[6]

Identity management [7] involves managing user roles and access rights, traditionally being centralized and governed by an authority, which raises concerns about privacy and is vulnerable to attacks. This paper proposes a DIMS leveraging blockchain technology. It provides users with control over their data using the concepts of self-sovereign identity, decentralized identifiers, and verifiable credentials. A wide range of identity providers are also given to the user to

choose from. It does not need a central authority, and the verification time is short. Also, it is possible to share data in a permissioned manner and verify its origin during the sharing process. This research aims to deal with the problem of blockchain adoption and specifically the application of decentralized identity (DID) management using blockchain in global organizations. The challenges that have been a barrier to blockchain use beyond cryptocurrencies and, more specifically, within organizations include identity management. DID is an emerging use case that uses blockchain to improve data protection and access control over traditional methods.Via Using a qualitative secondary case-based study methodology, the authors examine the present challenges and potential benefits of Identity management or Personal identification in severe aChallengeillance. design cube conceptual framework for ana-lyzing DID platforms is suggested, which adds to theoretical knowledge, as well as practical implementation in secure identity management.

Identity and Access Management System (IDMS) [8] plays a crucial role in identifying the authenticity and authorization of users in organizational systems. Traditional systems, relying on centralized authorities, are vulnerable to single points of failure. BC is a highly decentralized and distributed technology that can revolutionize IDMS through Self-Sovereign Identity (SSI), perfect for giving the user complete control over his/her digital identity. BC-based IDMS design in implementing proper SSI, however, is still at its premature stage of development. A review of academic and commercial literature related to the BC-based SSI solutions addresses blockchain technology's fundamentals along with the prospects for a roadmap designed for IDMS solutions. This has resulted in the identification of five key elements to offer potent BC-based IDMS implementation: authentication, integrity, privacy, trust, and simplicity. A security analysis also resolved the potential adversarial threats. It has gets focused on the problems and challenges faced during a study of the existing BC-based IDMS solutions implemented. This also helped in identifying research gaps that guide prospective research steps

Identity management (IdM) [9] is important for establishing user identities, but its centralized nature poses concerns, especially concerning the increasing value of personal data and the General Data Protection Regulation (GDPR). Current identity management systems, dominated by identity providers (IdP) and single-point services, entrust personal data control to third parties, posing security and privacy risks. The challenge exists on how the data can be managed securely while trusting responsible entities. Blockchain do eval flag, model evaluation is started and the technology introduces self-sovereign identities, yet inherent flaws persist. DNS-IdM aims to shift that paradigm by offering the design of a smart contract-based identity management system that allows.

Identity management solutions [11] play a crucial role in managing digital identities and authentication operations, extensively utilized in practical applications. Recent efforts have focused on introducing blockchain-based identity management solutions, allowing users to exert control over their own identities, known as self-sovereign identity. The paper considers the research and patents that have been published on blockchainbased identity management between May 2017 and January 2020, in an attempt to ascertain potential research gaps and opportunities available for guiding future investigations.

IAM systems are very important in all information systems, and more so in healthcare with the high sensitivity of data. HIoT applications are good targets for attackers making IAM systems that are designed up to very high standards necessary. BC is being employed significantly for decentralized IAM. However, its integration with HIoT requires due consideration because it is still evolving. In [12], Alamri et al. conducted a systematic literature review comprising BC- based IAM studies in HIoT applications with concern on security. Twenty-four of the studies that met the criteria of inclusion were subjected to quality as- sessment. The procedure entailed BC- based solutions in HIoT that were analyzed regarding IAM system architecture, security needs, and threats. Major components, layered architectures, and technologies were summarized. Some of the research gaps in this literature include the fact that they only considered the investigations of the security features of the solutions to the exclusion of the functional performance of the solutions, and excluded other Distributed ledger technologies such as IOTA with regards to IAM systems.

Fugkeaw et al. [13] puts forth D2-IAM, a blockchainbased IAM scheme that strives for enhanced security in Single Sign-On (SSO) access control personal cloud resources. D2-IAM leverages smart contracts and blockchain for core parts of the access control, creating accountability by the keeping of access transactions. Access to SSO is provided by high-level-of-assurance authentication and by hashedbased token management. Less communication overhead with typical identity providers. Fine-grained access is made possible by an access policy that is designed over a document database for each user. Their schemes are validated on Google Cloud with results showing nearly four times faster processing time than that achieved from existing studies. This scheme still leaves a gap by needing to develop an auditing protocol to certify the integrity of the access policies that are residing on the cloud. Furthermore, the integrity of the policy should mandatorily be asserted, even if they are rendered partially in enciphered form.

This study by Kiruba et al. (2021) highlights the transformative impact of blockchain technology in agriculture, enhancing supply chain security and efficiency[14]. Nilaiswariya et al. (2021) demonstrate the synergy between blockchain and Recurrent Neural Networks, improving scalability and security in medical datasets[15]. Enayati et al. (2024) analyze the potential of blockchain in empowering rural fishermen for livelihood sustainability[16]. Hemalatha (2021) underscores the importance of blockchain and IoT in monitoring and securing healthcare data [17]. Nair et al. (2021) explore blockchainenabled smart communities with electric vehicles, enhancing energy transactions [18]. Shibu et al. (2024) propose an integrated approach using IoT, blockchain, and smart con-

tracts for optimizing microgrid resilience during power outages [19].

METHODOLOGY

A. Truffle - Smart Contract Development and Deployment

Truffle is a large development framework for Ethereum, oriented to ease the process of smart contract building, testing, and deployment. It provides a set of tools making the development of smart contracts easier and less prone to errors. This includes tools associated with development environment, testing framework, asset pipeline, and network management. This paper makes use of Truffle to make smart contracts.

B. Ganache - Local Blockchain for Development

Ganache is a personal blockchain for Ethereum development, designed for deploying contracts, developing applications, and running tests. It gives you the ability to have a local, personal, safe, and fast blockchain right in your toolkit. Key features for Ganache include local blockchain, tied to Truffle, rich API. The Ganache we used is shown in fig.1. The image also says how many wallets are connected and how many ETH is available in that wallet.

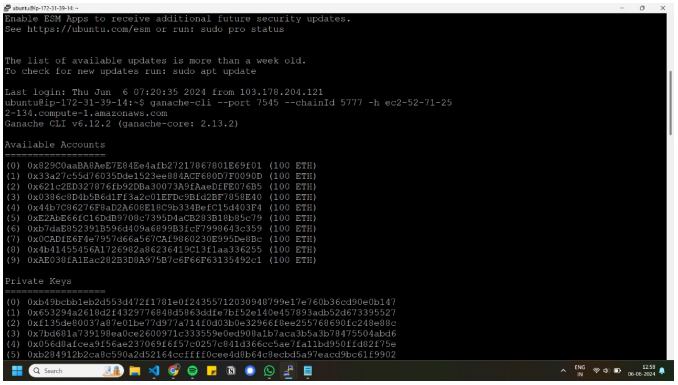

Fig. 1. putty window for ganache

C. MetaMask - Software Cryptocurrency Wallet

MetaMask is software that enables software wallet management of cryptocurrencies interfacing with the Ethereum blockchain. MetaMask is cryptocurrency wallet management software, and an interface to manage accounts on Ethereum and access advanced features of the future information superhighway, including browser integration, account management, transaction handling, security, and interacting with smart contracts.

In setting up the project, it's essential to have Node.js, Truffle Suite, and Ganache installed for blockchain development, The study focuses on the development of Ethereum smart contracts in Solidity, enabling functionalities such as identity management creation, updates, and revocation. In addition, digital signatures and role-based access control are embedded to advance the mechanisms. Ganache is set to connect with Truffle, and the whole blockchain environment can be simulated locally. Contracts are then deployed for full testing purposes to Ganache. The frontend is then developed in React.js for communication between users and the blockchain.

This study creates a IAM contract interface which contains functions which help in assigning roles , revoking roles and checking roles.For this study the roles available are admin , manager and employee. The roles are made in such a way that admin is in the top of the control hierarchy then manager and in the end employee. The admin has the power to assign or revoke the roles of manager and employee. The manager can assign or revoke the role of employee. This event of assigning or revoking roles are done in a decentralised manner.The study utilises the Aamazon Web Services. A EC2 instance is created for the testnet purpose.

Connectivity with smart contracts is established through Web3.js, implementing secure authentica- tion mechanisms for user interactions. Off-chain identity verification processes, such as biometrics or government-issued ID checks, shall be included, associating the data integrity of the verifications with the blockchain. Extensive testing is carried out using the Truffle framework, which simulates different scenarios. Finally, the preparation is made for contract deployment on a public testnet.

RESULTS AND DISCUSSION

The project is successfully developed and deployed with the implementation of an IAM system that harnesses blockchain technology. The system's deployment is done with an EC2 instance of Amazon Web Services as seen in Fig.3, hosting the testnet environment, making it scalable and secure. Smart contracts, developed in Solidity and heavily tested using the Truffle framework, provide role assignment, revocation, and checking functionalities according to role-based access control, where the admin, manager, and employee represent a hierarchy of roles. The frontend is built using React.js and is connected to the blockchain using Web3.js, which allows the user to interact seamlessly with the smart contracts.This can be seen in Fig.2. MetaMask has been used for wallet management and handling the transactions securely. The released IAM interface includes role assignment, role revocation, role checking, and role transfer features for a complete identity management system. Extensive testing with Truffle simulates various scenarios to verify the robustness and reliability of the smart contracts before deployment on a public testnet. The security of the IAM system is enhanced with off-chain identity verification mechanisms, such as biometrics or government-issued ID checks. The result is a solution that operates properly and securely in a decentralized system, using blockchain for IAM systems—one that is able to defend its efficiency and practicability. The project presents a new approach of blockchain integration on security solutions for IAM, with a modern solution of security, scalability, and user-friendly interaction.

This page helps in assigning roles to various users. Contracts such as access control give various permisssions to different type of users. For instance, ADMIN role, has access to admin

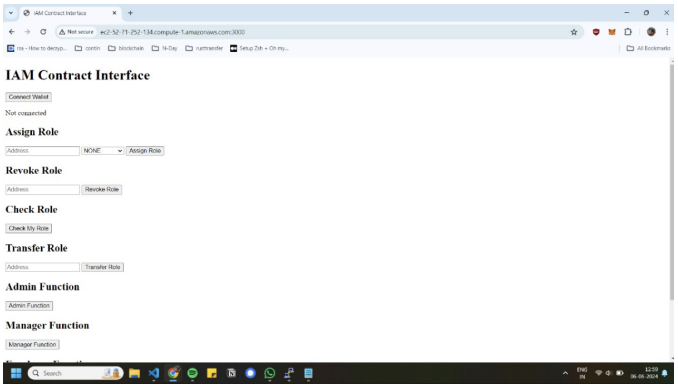

Fig. 2. IAM interface

functions and lower. MANAGER role has access to manager roles and lower and so on.

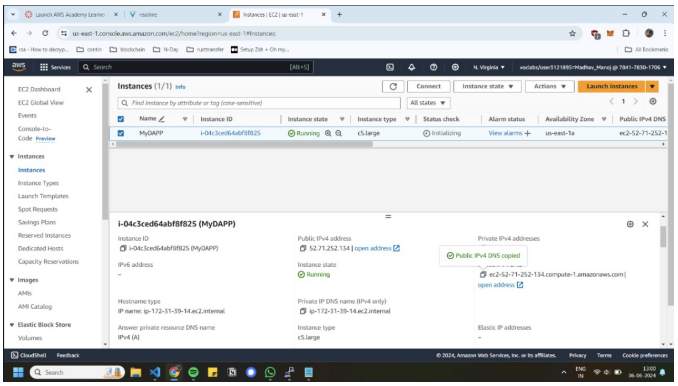

Fig. 3. AWS Dashboard

This is the EC2 instance where the IAM webpage is launched as a dAPP. It has access to a local blockchain through which the entire structure is built.

As the project is run on the local blockchain using Ganache and not the mainnet due to cost concerns, this figure shows the locally mined ETH alongside their private and public key which is then used for various purposed such as transaction and contract costs.

Conclusion and Future Enhancement

In conclusion, a decentralized IAM implementation with the usage of blockchain technology means a whole new solution to problems associated with conventional and central-type systems. Finally, by inherently providing the security, transparency, and efficiency associated with blockchain technology, decentralized IAM with blockchain at the helm will transform access management for organizations across multiple verticals and ensure standards in security. The very nature of blockchain being immutable allows for transparent audit trails that not only ensure accountability but also compliance. Access control processes will become much smoother and easier for an end-user to operate, making everything very efficient. With the increased maturity of blockchain technology, there is a lot of potential to have decentralized IAM solutions full of advantages in terms of security, privacy, and innovation. Using blockchain for IAM shapes the critical move to a secure and efficient digital future for organizations will mitigate risks and explore new opportunities for growth and innovation.

References

[1] Liguori, P., Al-Hossami, E., Cotroneo, D., Natella, R., Cukic, B., & Shaikh, S. (2021). Can we generate shellcodes via natural language? An empirical study. Automated Software Engineering, 29.

[2] G. Yang, X. Chen, Y. Zhou and C. Yu, "DualSC: Automatic Generation and Summarization of Shellcode via Transformer and Dual Learning," 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Honolulu, HI, USA, 2022, pp. 361-372, doi: 10.1109/SANER53432.2022.00052.

[3] Patel, Dhrumil, Aditya Basu, and Anish Mathuria. "Automatic generation of compact printable shellcodes for x86." 14th USENIX Workshop on Offensive Technologies (WOOT 20). 2020.

[4]]Basu, Aditya Mathuria, Anish Chowdary, Nagendra. (2014). Automatic Generation of Compact Alphanumeric Shellcodes for x86. 399-410. 10.1007/978-3-319-13841-1_22.

[5] Kumar, Pratik & Chowdary, Nagendra & Mathuria, Anish. (2013). Alphanumeric Shellcode Generator for ARM Architecture. 10.1007/978-3-642-41224-0_3.

[6] Guang Yang, Yu Zhou, Xiang Chen, Xiangyu Zhang, Tingting Han, and Taolue Chen. 2023. ExploitGen: Template-augmented exploit code generation based on CodeBERT. J. Syst. Softw. 197, C (Mar 2023).

[7] T. Bao, R. Wang, Y. Shoshitaishvili and D. Brumley, "Your Exploit is Mine: Automatic Shellcode Transplant for Remote Exploits," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2017, pp. 824-839, doi: 10.1109/SP.2017.67.

[8] Li, H., Wang, Y. P., Yin, J., & Tan, G. (2019). SmartShell: Automated Shell Scripts Synthesis from Natural Language. International Journal of Software Engineering and Knowledge Engineering, 29(2), 197-220.

[9] Liguori, P., Al-Hossami, E., Orbinato, V., Natella, R., Shaikh, S., Cotroneo, D., & Cukic, B. (2021). EVIL: Exploiting Software via Natural Language. 2021 IEEE 32nd International Symposium on Software Reliability Engineering (ISSRE), 321-332.

[10] Huang, Dong, et al. "Bias assessment and mitigation in llm-based code generation." arXiv preprint arXiv:2309.14345 (2023).

[11] Touvron, H., Martin, L., Stone, K., Albert, P., Almahairi, A., Babaei, Y., Bashlykov, N., Batra, S., Bhargava, P., Bhosale, S. and Bikel, D., 2023. Llama 2: Open foundation and fine-tuned chat models. arXiv preprint arXiv:2307.09288.

[12] Pietro Liguori, Cristina Improta, Simona De Vivo, Roberto Natella, Bojan Cukic, and Domenico Cotroneo. 2023. Can NMT understand me? towards perturbation-based evaluation of NMT models for code generation. In Proceedings of the 1st International Workshop on Natural Language-based Software Engineering (NLBSE '22). Association for Computing Machinery, New York, NY, USA, 59–66.

[13] Jiang, A.Q., Sablayrolles, A., Mensch, A., Bamford, C., Chaplot, D.S., Casas, D.D.L., Bressand, F., Lengyel, G., Lample, G., Saulnier, L. and Lavaud, L.R., 2023. Mistral 7B. arXiv preprint arXiv:2310.06825.

[14] Venugopalan, M. and Gupta, D., 2015, August. Exploring sentiment analysis on twitter data. In 2015 eighth international conference on contemporary computing (IC3) (pp. 241-247). IEEE.

[15] Subhash, P.M., Gupta, D., Palaniswamy, S. and Venugopalan, M., 2023, July. Fake News Detection Using Deep Learning and Transformer-Based Model. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[16] Vasudevan, S.K., Abhishek, S.N., Kumar, V., Aswin, T.S. and Nair, P.R., 2019. An innovative application for code generation of mathematical equations and problem solving. Journal of Intelligent & Fuzzy Systems, 36(3), pp.2107-2116.

[17] Amritha, G., Kh, V., VC, J.S. and Nair, M.G., 2022, November. Autoencoder Based FDI Attack Detection Scheme For Smart Grid Stability. In 2022 IEEE 19th India Council International Conference (INDICON) (pp. 1-5). IEEE.

[18] Srivastava, S., Paul, B. and Gupta, D., 2023. Study of word embeddings for enhanced cyber security named entity recognition. Procedia Computer Science, 218, pp.449-460.

[19] Murugesan, N., Velu, A.N., Palaniappan, B.S., Sukumar, B. and Hossain, M.J., 2024. Mitigating Missing Rate and Early Cyberattack Discrimination Using Optimal Statistical Approach with Machine Learning Techniques in a Smart Grid. Energies, 17(8), p.1965.