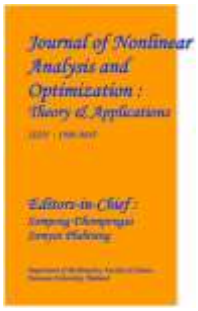
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**



DESIGN DECENTRALIZED E-GOVERNMENT FRAMEWORK USING BLOCKCHAIN

HIMAM BASHA SHAIK[1], **B.VISHNU KUMAR**[2]

[1]Assistant Professor, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

[2]PG Scholar, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

ABSTRACT— Electronic Government (e-Government) systems constantly provide greater services to people, businesses, organisations, and societies by offering more information, opportunities, and platforms with the support of advances in information and communications technologies. This usually results in increased system complexity and sensitivity, necessitating stricter security and privacy-protection measures. The majority of the existing e-Government systems are centralised, making them vulnerable to privacy and security threats, in addition to suffering from a single point of failure. This study proposes a decentralised e-Government framework with integrated threat detection features to address the aforementioned challenges. In particular, the privacy and security of the proposed e-Government system are realised by the encryption, validation, and immutable mechanisms provided by Blockchain. The insider and external threats associated with blockchain transactions are minimised by the employment of an artificial immune system, which effectively protects the integrity of the Blockchain. The proposed e-Government system was validated and evaluated by using the framework of Ethereum Visualisations of Interactive, Blockchain, Extended Simulations (i.e. eVIBES simulator) with two publicly available datasets.

Index Terms— Blockchain, e-governance, digital transformation

I. INTRODUCTION

E-Government uses digital technologies to deliver public services to individuals,

agencies, businesses, and other affiliates in order to improve efficiency, participation, accountability, transparency, and shared responsibilities with various stakeholders. This significantly improves the inclusiveness of government services by ensuring full access to services without the need for physical visits, among other advantages. In general, e-Government is one of the most complex information systems, requiring efficiency, security, and privacy protection. However, various privacy and security breaches are frequently reported around the world as a result of, amongst others, the disclosure of sensitive information, inappropriate sharing and mishandling of private information, and sophisticated attacks on e-Government systems. Most existing commonly used e-Government systems, such as websites and electronic identity management systems (eIDs), are centralised, with all data processed and computed through central servers. Centralised services frequently have a single point of failure, making the systems vulnerable to cyber attacks such as malware, worms, denial of service (DoS), and distributed denial of service attack (DDoS). Furthermore, insider threat is becoming an increasingly critical challenge in many organisations around the world, including e-Government systems; because it originates from a trusted account, it cannot be detected using external security measures such as firewalls. It enables the development of highly secure and privacy-preserving decentralised applications in which information is not controlled by a centralised host or third parties. Transactions are encrypted and stored in linked blocks (i.e. ledgers), which are distributed across the network in a verifiable and immutable manner using blockchain. This means that once information is added to the chain, it cannot be removed or changed in the future. Because of the immutability nature of blockchain, adding invalid transactions must be avoided.

Unwanted traffic, such as spyware, worms, ransomware, and spam, can be extremely expensive and financially disastrous. As a result, such traffic must be identified and prevented from being added to the e-Government blockchain. As a result, this work proposes an anomaly detection system for identifying and mitigating unwanted traffic in e-Government systems using artificial immune systems (AISs). In a nutshell, an AIS is a computational model created by simulating the behaviour and operation of the biological human immune system. Consequently, DCA is adopted to the proposed e-Government system herein,

but the application of other decentralised intrusion detection approaches and corresponding comparative studies of these approaches, remains as a piece of future work. The proposed framework was validated and evaluated using the Ethereum Visualisations of Interactive, Blockchain, Extended Simulations (i.e. eVIBES simulator). The open source eVIBES simulator offers off-chain (sideDB) data storage, which is crucial for e-Government systems since it allows for the storing of items like contacts, photos, and other data/information that are too large to be saved in the blockchain or that must be destroyed or updated in the future.

II. LITERATURE SURVEY

E-government diffusion is an international phenomenon. This study compares e-government adoption in the U.K. to adoption in the U.S. In particular, this study seeks to determine if the same factors are salient in both countries. Several studies have explored citizen acceptance of e-government services in the U.S. However, few studies have explored this phenomenon in the U.K. To identify the similarities and differences between the U.K. and the U.S. a survey is conducted in the U.K. and the findings are compared to the literature that investigates diffusion in the U.S. This study proposes a model of e-government adoption in the U.K. based on salient factors in the U.S. A survey is administered to 260 citizens in London to assess the importance of relative advantage, trust and the digital divide on intention to use e-government. The results of binary logistic regression indicate that there are cultural differences in e-government adoption in the U.K. and the U.S.

A. Privacy and security aspects of E-government in smart cities

E-government is an indispensable part of a Smart City. Information and communication technologies transform the relationship between citizens, businesses, and government departments, which enables the implementation of e-government, making operational processes efficient and speedy. This chapter investigates the current deployment strategies and the technological solutions of e-government in terms of security and privacy in a Smart City environment; it also identifies the challenges of adoption. In addition, this chapter proposes a decentralized framework based upon blockchain and artificial intelligence to provide a secure and privacy-preserving infrastructure. The proposed framework integrates technologies to provide mutual

trust between individuals, businesses, and governments, leading to a greater transparency of activity and less operational overhead. The reduction in process overhead results in lower running costs (therefore increasing revenue) and improves the speed of cross-boundary transactions.

B. Security and privacy issues in E-government

In developing technology, hackers are actively collecting personal information. To achieve their goals and acquire simple access to information about any individual, they use a range of methods and techniques. A privacy breach occurs when hackers gain access to complete information without the user's permission. Threats and dangers to security can arise for a variety of reasons, including technological flaws and targeted attacks. The government provides digital public facilities to people and the business community. Consumers have the expectation that e-government provides security and protects their data and personal information. Users have expressed concerns about their personal data privacy and safety. The main object of this chapter is to give strategies for IT specialists and e-government services because they need continuous improvement in privacy and security issues. The findings of this chapter may be useful to new researchers and may aid in the avoidance of security breaches and privacy issues.

III. PROPOSED SYSTEM

The overview of our proposed system is shown in the below figure.

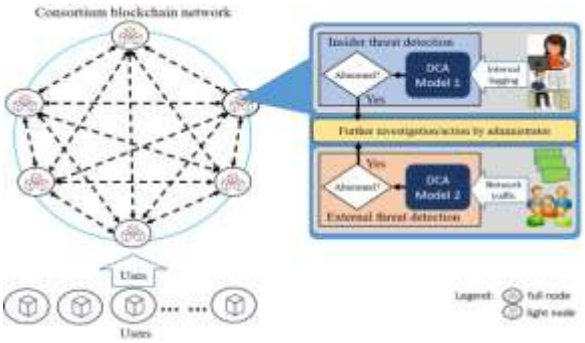


Fig. 1: System Overview

Implementation Modules

Admin

- In this module Admin can login with valid username and password after login successful admin can perform some operations: can view all datasets, view all cyber threat by blockchain, view all cyber threat results, view all gov classify type by blockchain, view all gov classify type results and logout.

User

- In this module user can register and login with valid username and password after

login successful user can perform operations are: user can upload datasets, find cyber threat type results by blockchain, find threat type and logout.

IV. RESULTS

Fig. 2: Home Page

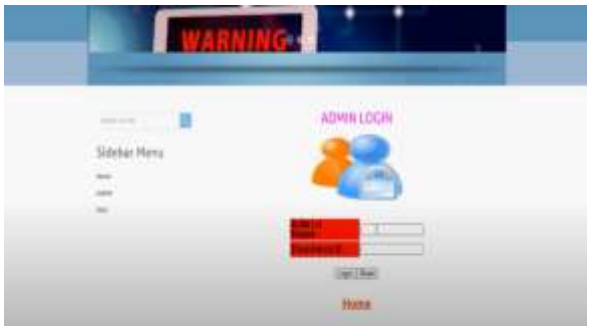


Fig. 3: Admin Login

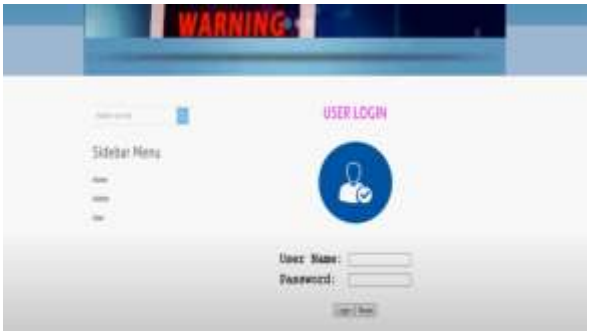


Fig. 4: User Login

Fig. 5: Cyber Threat Results

Fig. 6: Gov Classification Type

V. CONCLUSION

This project presents a decentralised, secure, and privacypreserving e-Government framework using consortium blockchain and artificial immune systems. The decentralised structure and encryption/validation mechanism provided by blockchain technology ensure the security, privacy, and integrity of information, which is further enhanced by the insider and external threats detection functionalities realised through an artificial immune system. The proposed framework was implemented using the eVIBES simulator. The experimental results show that the proposed e-Government

framework can provide e-services to users in an effective and secure manner, with the potential of increasing trust in public sectors. A direct piece of future work following the experimentation will be to investigate the innovative application of advances in artificial intelligence with the goal of speeding up block creation when there is a spike in transactions in the e-Government network so as to make the system more scalable and robust. In addition, it is worthwhile to study the application of other artificial immune systems to provide a security shield to the proposed e-Government system.

REFERENCE

[1] L. Carter and V. Weerakkody, ‘‘E-government adoption: A cultural comparison,’’ Inf. Syst. Frontiers, vol. 10, no. 4, pp. 473–482, Sep. 2008.

[2] L. Yang, N. Elisa, and N. Eliot, ‘‘Privacy and security aspects of E-government in smart cities,’’ in Smart Cities Cybersecurity and Privacy. Amsterdam, The Netherlands: Elsevier, 2019, pp. 89–102.

[3] M. A. Shaik, A. Rahim, V. Subhalakshmi, D. R. Ravi Kumar, R. Pasunuri and D. Verma, "Exploring Time Series Techniques in Production Function Modeling: ARIMA and VECM Applications," 2025 International Conference on Intelligent Computing and Control Systems (ICICCS), Erode, India, 2025, pp. 160-165, doi: 10.1109/ICICCS65191.2025.10985700.

[4] N. Elisa, L. Yang, F. Chao, and Y. Cao, ‘‘A framework of blockchain-based secure and privacy-preserving E-government system,’’ Wireless Netw., vol. 24, pp. 1–11, Dec. 2018.

[5] M. A. Shaik, G. Rakshitha, K. Saipriya, T. Thrisha, M. Varshini and J. G. Sai, "Machine Learning for Detecting the Phishing Threats," 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Goathgaun, Nepal, 2025, pp. 1221-1226, doi: 10.1109/ICMCSI64620.2025.10883227.

[6] (2019). Verizon Insider Threat Report. Accessed: Mar. 22, 2020. [Online]. Available: https://www.verizon.com/about/news/verizon-refocuses-cyberinvestigations-spotlight-world-insider-threats/

[7] M. A. Shaik, V. S. Rani, A. Fatima, M. Parveen, J. Juwairiyyah and N. Fatima, "Secure Data Exchange in Cloud Computing: Enhancing Confidentiality, Integrity, and Availability Through Data Partitioning and Encryption," 2024 International Conference

on Smart Technologies for Sustainable Development Goals (ICSTSDG), Chennai - 600077, Tamil Nadu, India, 2024, pp. 1-6, doi: 10.1109/ICSTSDG61998.2024.11026651.

[8] N. E. Nnko, A Decentralised Secure and Privacy-Preserving E-Government System. Tyne, U.K.: University of Northumbria at Newcastle, 2020.

AUTHORS Profile

Mr. Himambasha Shaik is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Anna University, Chennai. With a strong research background, He has authored and co-authored research papers published in reputed peer-reviewed journals. His research interests include Machine Learning, Artificial Intelligence, Cloud Computing, and Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Mr. B.Vishnu Kumar has revived has received her Bca (Computers)And Degree From ANU 2023 Pursuing MCA Qis College Of Engineering And Technology Affiliated to JNTUK 2023-2025