IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Securing E-Government With Blockchain And Artificial Immunity For Privacy

T. Lakshmi Parvathi[1], Mrs. E. Sindhu[2]

[1]PG student Vemu Institute of Technology, P.Kothakota.

[2]Assistant Professor,Vemu Institute of Technology,P.Kothakota.

ABSTRACT

As research introduces a novel decentralized e-Government architecture fortified with threat detection capabilities to tackle security and privacy issues prevalent in centralized systems. By harnessing Blockchain's encryption and validation mechanisms, the proposed framework ensures stringent privacy and security measures. Integrating an artificial immune system further bolsters the system's resilience against potential threats to Blockchain integrity. Validation conducted via the eVIBES simulator using publicly available datasets affirms the framework's efficacy in mitigating both insider and external threats while upholding data privacy standards. This decentralized approach not only addresses vulnerabilities inherent in traditional e-Government systems but also demonstrates marked improvements in security measures and a resilient privacy framework, essential for optimizing service delivery in the digital governance domain. Additionally, to bolster accuracy, we have implemented the XGBOOST algorithm with genetic algorithm features, leveraging its ensemble approach to refine model performance and enhance accuracy.

Keywords: Blockchain, E-Government

INTRODUCTION

E-Government, leveraging digital technologies, aims to enhance public service delivery by fostering efficiency, participation, transparency, and accountability. However, the complexity of e-Government systems demands robust security and privacy measures to combat cyber threats, including insider risks. Traditional centralized systems are vulnerable to various attacks, prompting the need for innovative solutions.

This paper proposes a decentralized e-Government framework harnessing Blockchain technology. Blockchain offers secure, immutable data storage and sharing, ensuring transparency and privacy without centralized control. To address security challenges, an anomaly detection system using Artificial Immune Systems (AIS) is integrated, specifically employing the Dendritic Cell Algorithm (DCA). The framework is validated

using the eVIBES simulator and tested with real-world datasets, affirming its efficacy in enhancing government services' efficiency and security. This research contributes a pioneering decentralized e-Government model, amalgamating consortium blockchain and DCA for robust security and privacy preservation, vital for modern governance.

LITERATURE SURVEY

L. Carter and V. Weerakkody*et al*

Sincethe author conducts a comparative study on e-government adoption between the U.K. and the U.S., aiming to uncover shared and distinct factors influencing adoption. While the U.S. context has been extensively studied, the U.K. remains relatively unexplored. Through a survey in London, the study evaluates factors like relative advantage, trust, and the digital divide's impact on e-government usage intentions. Findings from binary logistic regression highlight cultural disparities, revealing that while relative advantage and trust are universal drivers, barriers like ICT access and skill may vary across cultures. The study proposes a model of e-government adoption in the U.K., extrapolated from salient U.S. factors, with implications for further research and practical applications.

L. Yang, N. Elisa, and N. Eliot*et al*

As author delves into the pivotal role of e-government within Smart City ecosystems, highlighting its transformative impact on citizen-government interactions. This chapter scrutinizes existing e-government deployment strategies, emphasizing security and privacy concerns in Smart City environments. To address these challenges, the author proposes a decentralized framework leveraging blockchain and artificial intelligence. This innovative solution fosters mutual trust among stakeholders while enhancing transparency and reducing operational overhead. By streamlining processes, the framework not only cuts costs, boosting revenue, but also expedites cross-boundary transactions, thus advancing the efficiency and effectiveness of e-government in Smart Cities.

R. Palanisamy and B. Mukerji*et al*

Because author underscores the pivotal role of government in delivering secure online services to citizens and businesses, emphasizing the paramount importance of safeguarding privacy. This chapter outlines the myriad security and privacy challenges confronting e-government, detailing their origins, impact, and mitigation strategies. By elucidating these issues, the chapter aims to furnish state and federal administrators, as well as IT professionals, with invaluable guidance for bolstering e-government security and privacy measures. The ultimate goal is to facilitate continuous enhancement in these domains, ensuring that e-citizens can confidently engage with e-government services while their personal information remains safeguarded.

PROBLEM STATEMENT:

Now-a-days Government is using online technology in almost all fields such as publishing education results online, publishing new welfare schemes, online AADHAR or personal identification registration and many more other services. In existing techniques all services were managing by single centralized server and if this server hack or crash then data will be lost and services will be

disturbed. Existing centralised server can be easily alter or theft by internal working employees and consider as internal attacks. Outsider attackers may send malicious request to centralized server to steal data or crash server.

PROPOSED METHOD:

Due to above disadvantages of centralized server author of this paper employing distributed Blockchain technology in which data will be store at multiple nodes and if one node down then data can be obtained from other working node. Blockchain store data as block or transaction and associate each block with unique hash code and this hash code will get verify before new block storage and if data alter then hash code get mismatch and data alteration will get detected thus Blockchain is tamper proof. Data store in Blockchain can be access by authenticated user so data stealing is impossible.

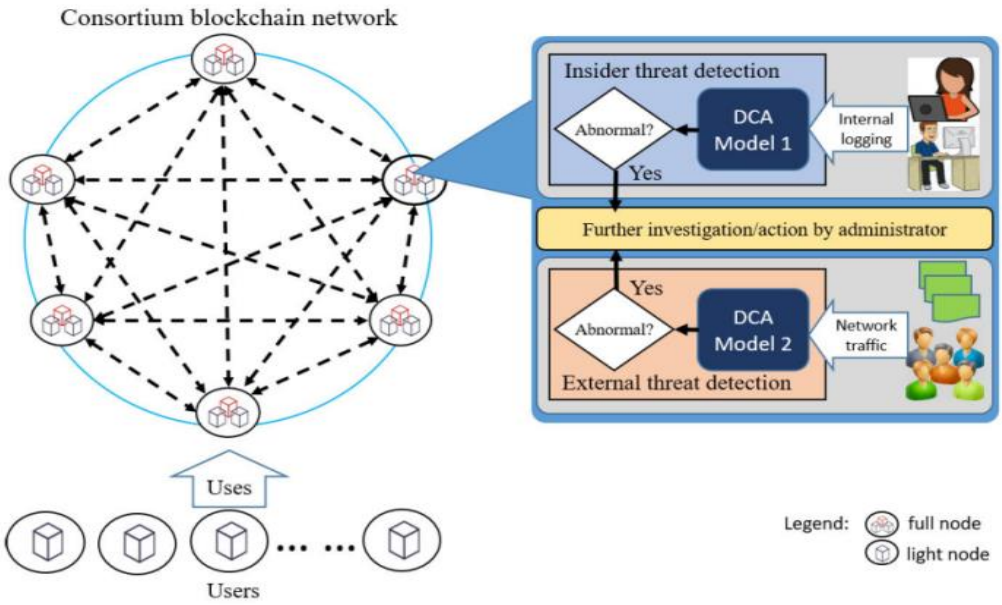
In propose work to tackle attacks author has used Artificial Intelligence algorithms with Genetic Features Selection algorithm to select relevant features from network data to accurately identify request as genuine or attack. Propose Genetic algorithm performance has evaluated with various algorithm such as SVM, Random Forest, Naïve Bayes, ANN and Decision Tree. Each algorithm performance is evaluated in terms of accuracy, precision, recall and FSCORE. Among all algorithms propose Genetic Features computation algorithm is giving best accuracy.

In propose work author introduced Identity Based Verification algorithm with Expander signatures which allow user to generate signature prior and can perform verification using any device like laptop, computer or tablet.

Propose work consists of Secret Key Generation and then generate Public Key based on Secret Key and then signed message using secret key and then can perform verification using public key.

All key verification and generation can be perform using Blockchain Smart Contract which contains function to UPLOAD and VERIFY signatures and this contract can be designed using solidity programming.

ARCHITECTURE



METHODOLOGY:

1. Data Preprocessing:

Data Cleaning: The dataset undergoes thorough cleaning to handle missing values appropriately, ensuring the integrity of the data for further analysis and modeling.

Label Encoding: Categorical features such as 'proto', 'service', 'state', and 'attack cat' are encoded into numerical values to make them compatible with machine learning algorithms, facilitating effective model training.

Normalization: To ensure that all features have the same scale and contribute equally to the modeling process, the dataset is normalized using techniques such as Min-Max scaling or Standard scaling.

2. Model Training:

Feature Selection: Utilizing Genetic Selection CV, the most relevant features are selected from the dataset, optimizing the model's performance and reducing computational complexity.

Model Selection: A variety of machine learning algorithms, including Decision Tree, Naive Bayes, Support Vector Machine (SVM), Random Forest, Artificial Neural Network (ANN), and XGBoost, are explored for classification tasks, allowing for comprehensive comparison and selection of the most suitable model.

Evaluation: The performance of the trained models is evaluated using cross-validation techniques, assessing metrics such as accuracy, precision, recall, and F1-score to gauge their effectiveness in classifying instances accurately.

3. Blockchain Integration:

Data Storage: Leveraging smart contracts, details of users and their activities are securely stored on the blockchain, ensuring immutability, transparency, and tamper-proof records.

Verification: Blockchain technology is employed to verify users' identities and activities, enhancing data integrity and security by providing a decentralized and trustless environment for authentication.

4. Web Application Development:

User Interface: A user-friendly web application is developed using the Django framework, offering intuitive access to the anti-tamper system's

functionalities for both government officials and citizens.

Authentication: Robust authentication mechanisms are implemented, creating separate login portals for government officials and citizens to ensure secure access to relevant functionalities based on user roles and permissions.

Functionalities: The web application encompasses various functionalities, including adding citizens, viewing citizen details, and accessing anti-tamper system results, enhancing user experience and system usability.

5. Testing and Deployment:

Test Data: Test data is utilized to validate the effectiveness of the trained machine learning models in real-world scenarios, ensuring their robustness and reliability in practical applications.

Performance Analysis: The performance of each machine learning algorithm is comprehensively analyzed based on metrics such as accuracy, precision, recall, and F1-score, with graphical representations provided for easy interpretation and comparison.

Deployment: The entire system, comprising the web application and machine learning models, is deployed on a suitable server infrastructure, making it accessible to the public while ensuring scalability, reliability, and security.

6. Security Measures:

Data Encryption: Sensitive information, including user details and blockchain transactions, undergo encryption to safeguard against unauthorized access and maintain confidentiality.

Authentication: Strict authentication protocols are implemented to verify the identity of users before granting access to the system, mitigating the risk of unauthorized entry and data breaches.

Error Handling: Robust error handling mechanisms are put in place to gracefully handle exceptions and errors, enhancing system resilience and preventing potential security vulnerabilities that could compromise system integrity.

Precision:

$$\text{Formula: Precision} = \frac{\text{True Positives}}{\text{True Positives+False Positives}}$$

Code: precision = precision_score(testY, predict, average='macro') * 100

Recall (Sensitivity):

$$\text{Formula: Recall} = \frac{\text{True Positives}}{\text{True Positives+False Negatives}}$$

Code: recall = recall_score(testY, predict, average='macro') * 100

F1 Score:

$$\text{Formula: } F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}}$$

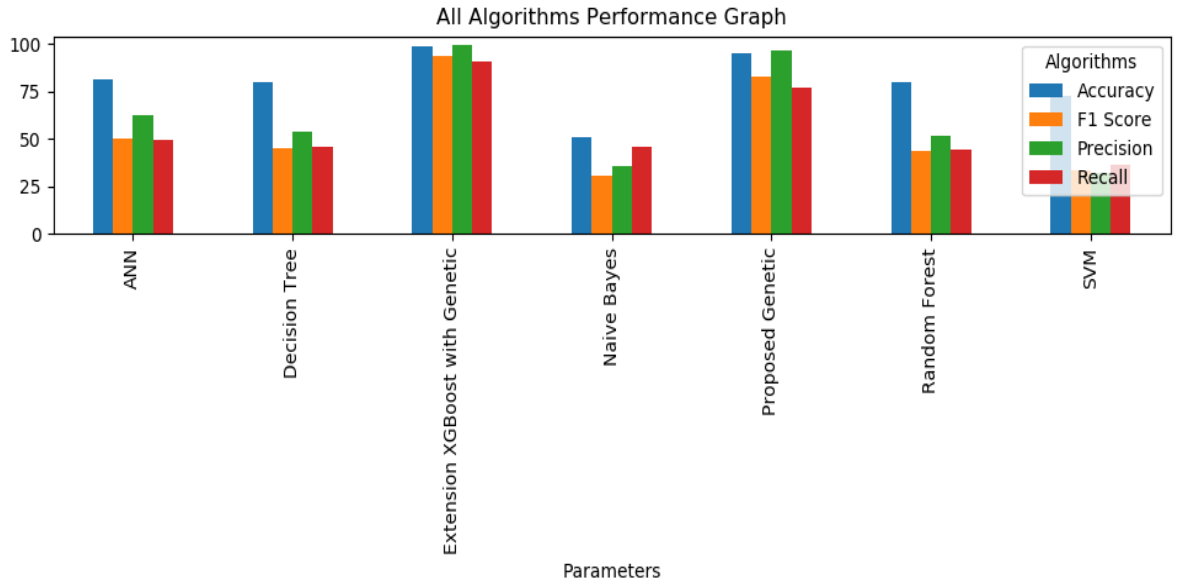
Code: f1 = f1_score(testY, predict, average='macro') * 100

Accuracy:

$$\text{Formula: Accuracy} = \frac{\text{Correct Predictions}}{\text{Total Predictions}}$$

Code: accuracy = accuracy_score(testY, predict) * 100

RESULTS:



Training of all AI algorithms, in above graph x-axis represents algorithm names and y-axis represents accuracy, precision, recall and FSCORE in different colour bars and in all algorithms Extension and Propose algorithm got high accuracy

Algorithm Name	Accuracy	Precision	FSCORE	Recall
Decision Tree	80.16666666666666	54.15240170142132	45.401660414932095	45.75826612275493
Naive Bayes	50.66666666666667	35.994083982100086	30.7157428210618	46.07536779950572
SVM	73.0	31.86015091762218	33.1704255907939	36.179753342487764
Random Forest	79.66666666666666	51.84810201953851	43.58507367570629	44.151112717355915
ANN	81.5	62.80633225609541	50.12835637071268	49.10275951110797
Proposed Algorithm with Genetic Features	94.83333333333334	96.74942263594747	82.84429259919457	76.82780182780182
Extension XGBoost with Genetic Features	98.5	99.21001519588603	93.8733224202578	90.58722142055476

All algorithm performance in tabular format

Test Data	Predicted Attack
[8.80000000e+01 1.00000000e-05 4.00000000e+00 0.00000000e+00 2.00000000e+00 2.00000000e+00 0.00000000e+00 1.44800000e+03 0.00000000e+00 1.00000003e+05 2.54000000e+02 0.00000000e+00 5.79200000e+08 0.00000000e+00 0.00000000e+00 0.00000000e+00 1.00000000e-02 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 7.24000000e+02 0.00000000e+00 0.00000000e+00 0.00000000e+00 4.30000000e+01 2.00000000e+00 5.00000000e+00 5.00000000e+00 1.00000000e+00 4.00000000e+01 0.00000000e+00 0.00000000e+00 0.00000000e+00 5.00000000e+00 3.90000000e+01 0.00000000e+00]	Normal
[5.76970000e+04 3.00000000e-06 2.00000000e+00 0.00000000e+00 2.00000000e+00 2.00000000e+00 0.00000000e+00 2.00000000e+02 0.00000000e+00 3.33333322e+05 2.54000000e+02 0.00000000e+00 2.66666656e+08 0.00000000e+00 0.00000000e+00 0.00000000e+00 3.00000000e-03 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 1.00000000e+02 0.00000000e+00 0.00000000e+00 0.00000000e+00 4.00000000e+00 2.00000000e+00 1.00000000e+00 1.00000000e+00 1.00000000e+00 4.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 2.00000000e+00 4.00000000e+00 0.00000000e+00]	Exploits
[5.76980000e+04 3.00000000e-06 1.00000000e+00 0.00000000e+00 2.00000000e+00 2.00000000e+00 0.00000000e+00 2.00000000e+02 0.00000000e+00 3.33333322e+05 2.54000000e+02 0.00000000e+00 2.66666656e+08 0.00000000e+00 0.00000000e+00 0.00000000e+00 3.00000000e-03 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 1.00000000e+02 0.00000000e+00 0.00000000e+00 0.00000000e+00 5.00000000e+00 2.00000000e+00 2.00000000e+00 2.00000000e+00 2.00000000e+00 5.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00 2.00000000e+00 5.00000000e+00 0.00000000e+00]	Exploits

In above screen in first column we can see the TEST data and in second column showing predicted attack.

Citizen Personal Identity	Citizen Name	Gender	Contact No	Address	Photo Filename	Record Create Date	Photo	SHA code
5001	kumar	Male	9876543210	hyd	download.jpg	2023-08-29		adb019dcde61d092941e0fec4e89b405130df238877e2611c330ae95a7266487

Citizen view his details with SHA code

CONCLUSION

The implementation of a secure and privacy-preserving e-government framework using blockchain and artificial immunity marks a significant advancement in safeguarding government services against internal and external threats. By adopting distributed blockchain technology, the project ensures data integrity and availability, mitigating the risks associated with centralized servers. The integration of smart contracts facilitates user authentication and data verification, enhancing transparency and trust in government operations. Furthermore, the utilization of artificial intelligence algorithms, coupled with genetic feature selection, demonstrates the efficacy of advanced techniques in accurately identifying and mitigating potential attacks. Through extensive evaluation and testing, the project underscores the feasibility and effectiveness of leveraging innovative technologies to fortify e-government systems against emerging threats.

REFERENCES:

[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] R. Palanisamy and B. Mukerji, ‘‘Security and privacy issues in E-government,’’ in Cyber Behavior: Concepts, Methodologies, Tools, and Applications. Pennsylvania, PA, USA: IGI Global, pp. 880–892, 2014.

[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] J. Glasser and B. Lindauer, ‘‘Bridging the gap: A pragmatic approach to generating insider threat data,’’ in Proc. IEEE Secur. Privacy Workshops, May 2013, pp. 98–104.

[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] N. Elisa, L. Yang, H. Li, F. Chao, and N. Naik, ‘‘Consortium blockchain for security and privacy-preserving in E-government systems,’’ 2020, arXiv:2006.14234.

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

[9] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, ‘‘Consortium blockchain for secure energy trading in industrial Internet of Things,’’ IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3690–3700, Aug. 2017.

[10] S. Underwood, ‘‘Blockchain beyond bitcoin,’’ Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.

[11] N. Elisa, L. Yang, H. Li, F. Chao, and N. Naik, ‘‘Consortium blockchain for security and privacy-preserving in E-government systems,’’ in Proc. ICEB, 2019, pp. 99–107.

[12] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, ‘‘Consortium blockchains: Overview, applications and challenges,’’ Int. J. Adv. Telecommun., vol. 11, nos. 1–2, pp. 1–14, 2018.

[13] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Decentralized Bus. Rev., Manubot, Tech. Rep. 21260, 2008.

[14] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Sebastopol, CA, USA: O’Reilly Media, 2014.

[15] J. Greensmith, U. Aickelin, and S. Cayzer, ‘‘Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection,’’ in Proc. Int. Conf. Artif. Immune Syst. Springer, 2005, pp. 153–167.

[16] Z. Chelly and Z. Elouedi, ‘‘A survey of the dendritic cell algorithm,’’ Knowl. Inf. Syst., vol. 48, no. 3, pp. 505–535, Sep. 2016.

[17] N. Elisa, L. Yang, X. Fu, and N. Naik, ‘‘Dendritic cell algorithm enhancement using fuzzy inference system for network intrusion detection,’’ in Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE), Jun. 2019, pp. 1–6.

[18] A. Deshpande, P. Nasirifard, and H.-A. Jacobsen, ‘‘EVIBES: Configurable and interactive Ethereum blockchain simulation framework,’’ in Proc. 19th Int. Middleware Conf. (Posters), Dec. 2018, pp. 11–12.

[19] N. Moustafa and J. Slay, ‘‘UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),’’ in Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), Nov. 2015, pp. 1–6.

[20] J. R. Gil-Garcia, S. S. Dawes, and T. A. Pardo, ‘‘Digital government and public management research: Finding the crossroads,’’ Public Manage. Rev., vol. 20, no. 5, pp. 633–646, May 2018