**J**ournal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1 : 2024
ISSN : **1906-9685**


# E-GOVERNMENT SERVICE'S MACHINE LEARNING - BASED CYBERSECURITY THREAT DETECTION

**#1 Mrs.S.LAVANYA, #2 G.PAVANA SRAVANTHI, #3 K.VANDANA KRISHNA, #4 M.UDAY KIRAN, #5 M.VASUNDARA DEVI**
#1Assistant professor in Department of IT, DVR &Dr.HS MIC College of Technology,Kanchikacherla
#2#3#4#5 B.Tech with Specialization of Information Technology , DVR &Dr.HS MIC College of Technology,Kanchikacherla-521180

**ABSTRACT_**One of the most important technologies of the Fourth Industrial Revolution (Industry 4.0) is artificial intelligence (AI), which guards computer network systems from damage, phishing, malware, cyberattacks, and unauthorised access. Through e-Government, artificial intelligence (AI) has the potential to improve the cyber capabilities and security of states, municipalities, and non-state actors. Research currently available shows a mixed link between cybersecurity, e-Government, and AI; however, it is thought that this relationship depends on the situation. Different stakeholders with varying levels of knowledge and experience in their respective fields have an impact on and influence AI, e-Governance, and cybersecurity. This study explores the direct relationship between cybersecurity, e-Government, and AI in order to close this context-specific gap.
Additionally, the moderating influence of stakeholder involvement on the relationship between AI, e-Governance, and cybersecurity is examined, as is the mediating role of e-Governance in this relationship. PLS-SEM route modelling analysis results showed that e-Governance has a somewhat mediating effect between cybersecurity and AI. Similarly, it was shown that stakeholder involvement had a moderating effect on the relationship between cybersecurity and e-Government as well as AI and e-Government. Because all stakeholders have an interest in a thriving, transparent, and safe cyberspace when using e-services, it is implied that stakeholder involvement in AI and e-Governance is crucial. This study offers smart city governments useful recommendations for bolstering their cybersecurity defences.

## 1.INTRODUCTION

Network safety has turned into a basic and essential subject that requires safeguarding the PC network from possible dangers in the present current world [1], [2]. A digital assault is a purposeful assault focusing on PC organizations, pertinent information, programs, and electronic data, bringing about sub-public substances prompting viciousness towards noncombatant rivals. As innovation grows, so do digital dangers, requiring the advancement of new counteraction techniques [3], [4]. It has been affirmed that digital assaults have become more common in the modern area, bringing about serious framework harm and huge money related misfortune. The ascent of digital assaults among associations is basically because of the developing dependence on web-based advances that empower the capacity of individual and financial information [5].Consequently, it is recognized as maybe the most basic issue in the cutting edge setting since it makes monetary misfortune and uncovers classified data. Cyberattacks incorporate phishing, refusal of administration, malware, and ransomware pervasions, which can hurt anyone in the public eye [6]. Digital goes after likewise mentally affect people, delivering misery, strain, and stress among individuals [7].

Computerized reasoning (simulated intelligence) applications can emphatically impact the digital abilities and public safety of the sovereign country, provincial government elements, and non-state associations [8], [9].

Computer based intelligence is a solid strategy for moderating digital assault impacts [10]. Computer based intelligence is machine knowledge that executes exercises associated with insight [11]. Human experts' aptitude is coordinated for key preparation and decision-production [12], including making clinical conclusions and getting experiences from skill in closing. As far as online protection, Zarina et al., [ 10] have delineated that man-made intelligence makes both gainful and unsafe impacts, with the destructive impact of working with the impelling period of cyberattacks, coming about in speedier and additional staggering assaults. Looking forward, simulated intelligence can possibly significantly further develop network protection by expanding security safeguards and advancing security in the internet. Besides, computer based intelligence helps security specialists in distinguishing digital risk side effects and has improved the AI applications for malware arrangement and organized interruption recognition [13]. Finally, the advanced peculiarity in computer based intelligence has changed creative arrangements and further developed city outer assaults against serious security dangers [14].

A savvy city gives numerous inventive answers for a few difficulties that city organization faces. Be that as it may, data and correspondence innovation (ICT) has turned into an indispensable part of e-Government. Executing ICT into a city's framework presents risks and checks [15]. Individuals habitually utilize shaky Wi-Fi organizations to browse their email messages, e-banking, and other advanced administrations, uncovering themselves to cybercrimes including hacking, disavowals of administration, and breaking. Network safety applying advancements to safeguard e-Taxpayer supported organizations is among the main particular highlights that can be used to sort safe urban areas around the world [16].Somewhere in this propensity, the 'comprehensive shrewd city' structure has set areas of strength for off in light of the fact that it accentuates the significance of relational and social capital in metropolitan drives that attention on partners' consideration in the Computerized Domain and including occupants in help improvement to carry out suitable taxpayer supported organizations that match residents' necessities [17], [18]. Late investigations on e-administrations and innovations likewise have stressed the significance of carrying out a residents focused system for savvy urban communities since expected to serious areas of strength for foster ecologies rely unequivocally upon web innovation. Thus, web advances and administrations can altogether affect partner associations [19]

## 2.LITERATURE SURVEY

The literature survey encompasses a comprehensive review of scholarly works and research findings related to artificial intelligence (AI), cybersecurity, e-government, and smart cities. The surveyed literature sheds light on the intersection of these domains, highlighting emerging trends, challenges, and opportunities.

In the realm of AI in cybersecurity, researchers such as Alhayani et al. (2021) and Komar et al. (2017) emphasize the growing importance of AI in bolstering cybersecurity defenses. Various AI techniques, such as machine learning and natural language processing, are explored for their efficacy in enhancing security measures. Additionally, studies delve into the potential impact of AI on cybersecurity practices and the evolving threat landscape (Alhayani et al., 2021; Komar et al., 2017).

Cloud computing emerges as a critical component in modern cybersecurity strategies, as discussed by scholars such as Cavelty (2007). They highlight the capabilities of cloud-based solutions for rapid risk assessment and mitigation, along with exploring innovative approaches to secure cloud environments and mitigate cyber threats effectively (Cavelty, 2007).

The literature underscores the importance of integrating cybersecurity measures into e-government initiatives. Researchers like Corallo et al. (2022) discuss the role of AI-driven technologies in optimizing government services, enhancing citizen engagement, and improving cybersecurity resilience. Additionally, studies highlight the need for robust cybersecurity frameworks to safeguard sensitive government data and ensure the

integrity of e-government systems (Corallo et al., 2022).

Smart city initiatives are examined in the context of cybersecurity challenges and opportunities. Scholars such as Khatoun and Zeadally (2017) explore how AI technologies can support the development of secure and resilient smart city infrastructure. They emphasize the importance of stakeholder collaboration in addressing cybersecurity threats effectively (Khatoun&Zeadally, 2017).

## 3.PROPOSED SYSTEM

Advanced technologies including artificial intelligence (AI), machine learning (ML), and big data analytics are incorporated into proposed cybersecurity systems to improve threat detection and response capabilities. Large volumes of data may be instantly analysed by AI and ML algorithms to spot irregularities and possible dangers. Furthermore, these systems are more resistant to new attacks because of their ability to continuously learn and adapt to new attack strategies. Furthermore, in order to expedite incident response procedures and shorten reaction times, suggested solutions frequently incorporate automation and orchestration features. The suggested systems combine these cutting-edge technologies in an effort to offer proactive and flexible cybersecurity solutions that can successfully mitigate a broad spectrum of cyberthreats.


Fig 1:Architecture

### 3.1 IMPLEMENTATION

**User Module:**

user will register with application and get user name and password. Owner can see all encrypted files uploaded by all users and send request to respective user and get approval to download data and three keys for RSA are shared to owner email which can be used for owner download.

Use can view data of owner if it is not attacked packet

**Owner Module:**

owner will register into the application by providing all the necessary details and therefore he can login into the application using username and password and user can upload the files to application and share with the other registered users. He can also view the files uploaded by him and can also view the requests for secret key from the other users and we can respond and the key will be sent to user by mail. Using that key, he can download the file and view the information.

When owner sends data to user application will predict and check if the given packet is fraud or not using Machine learning if packet is attack it is detected by machine learning and stops before upload to cloud.

**Attack detection Machine learning stage:**

In this stage cloud network dataset is taken as input and trained using machine learning algorithms and integrated in to cloud module where when user sends data it will check packet and predict if user is attacker or not.

**Data COLLECTION:**

There are three symbolic data types in NSL-KDD data features: protocol type, flag and service. We use one-hot encoder mapping these features into binary vectors. One-Hot Processing: NSL-KDD dataset is processed by one-hot method to transform symbolic features into numerical features. For example, the second feature of the NSL-KDD data sample is protocol type. The protocol type has three values: tcp, udp, and icmp. One-hot method is processed into a binary code that can be recognized by a computer, where tcp is [1, 0, 0], udp is [0, 1, 0], and icmp is [0, 0, 1]

**Pre-processing:**

When the dataset is extracted, part of the data contains some noisy data, duplicate values, missing values, infinity values, etc. due to extraction errors or input errors. Therefore, we first perform data preprocessing. The main work is as follows. (1) Duplicate values: delete the sample’s duplicate value, only keep one

valid data. (2) Outliers: in the sample data, the sample size of missing values(Not a Number, NaN) and Infinite values(Inf) is small, so we delete this. (3) Features delete and transform: In CSE-CIC-IDS2018, we delete features such as ‘‘Timestamp’’, ‘‘Destination Address’’, ‘‘Source Address’’, ‘‘Source Port’’, etc. If features ‘‘InitBwd Win Byts’’ and features ‘‘InitFwd Win Byts’’ have a value of −1, we add two check dimensions. The mark of −1 is 1. Otherwise, it is 0. In NSL-KDD, we use the One Hot encoder to complete this conversion. For example, ‘‘TCP’’, ‘‘UDP’’ and ‘‘ICMP’’ are functions of three protocol types. After OneHot encoding, they become binary vectors (1, 0, 0), (0, 1, 0), (0, 0, 1). The protocol type function can be divided into three categories, including 11 categories for flag function and 70 categories for service function. Therefore, the 41 dimensions initial feature vector becomes 122 dimensions. (4) Numerical standardization: In order to eliminate the dimensional influence between indicators and accelerate the gradient descent and model convergence, the data is standardized, that is, the method of obtaining Z-Score, so that the average value of each feature becomes 0 and the standard deviation becomes 1, converted to a standard normal distribution, which is related to the overall sample distribution, and each sample point can have an impact on standardization. The standardization formula is as follows, u is the mean of each feature, s is the standard deviation of each feature, and x 0 i is the element corresponding to each column’s features.

**Train-Test Split and Model FITTING:**

Now, we divide our dataset into training and testing data. Our objective for doing this split is to assess the performance of our model on unseen data and to determine how well our model has generalized on training data. This is followed by a model fitting which is an essential step in the model building process.

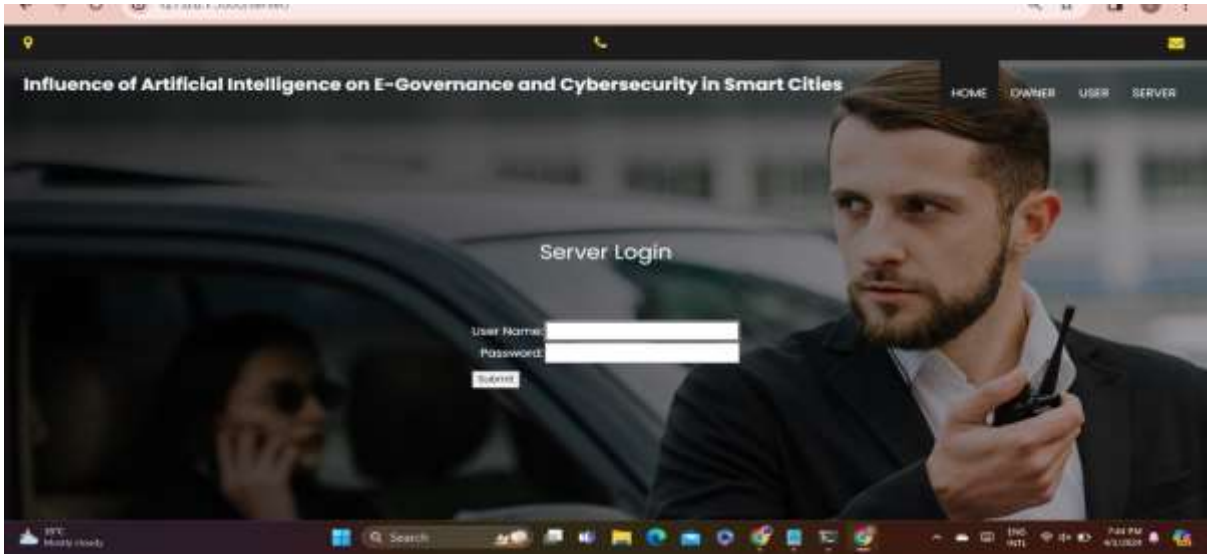
**Model Evaluation and Predictions:**

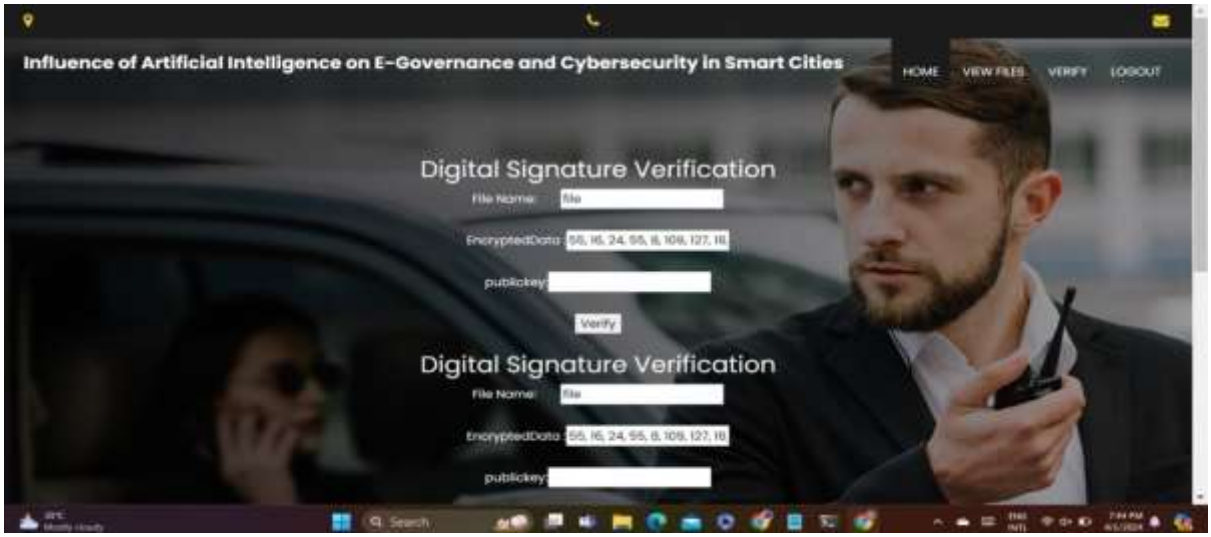
This is the final step, in which we assess how well our model has performed on testing data using certain scoring metrics, I have used 'accuracy score' to evaluate my model. First, we create a model instance, this is followed by fitting the training data on the model using a fit method and then we will use the predict method to make predictions on x_test or the testing data, these predictions will be stored in a variable called y_test_hat. For model evaluation, we will feed the y_test and y_test_hat into the accuracy_score function and store it in a variable called test_accuracy, a variable that will hold the testing accuracy of our model. We followed these steps for a variety of classification algorithm models and obtained corresponding test accuracy scores.

## 4.RESULTS AND DISCUSSION




Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities
HOME
VIEW FILES
VERIFY
LOGOUT
shiva
shiva
shiva


Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities
HOME
OWNER
USER
SERVER
Server Login
User Name:
Password:
Submit


Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities
HOME
VIEW FILES
VERIFY
LOGOUT
Digital Signature Verification
File Name:
file
EncryptedData:
publickey:
Verify
Digital Signature Verification
File Name:
file
EncryptedData:
publickey:

## 5.CONCLUSION

The current examination dives into the reconciliation of man-made reasoning (artificial intelligence) to handle online protection challenges. It highlights the developing meaning of artificial intelligence as a urgent innovation in upgrading data security. As digital dangers advance, conventional methodologies become deficient, requiring imaginative systems. Artificial intelligence offers progressed examination and danger knowledge capacities that engage security experts to alleviate chances and strengthen venture security systems. In addition, the review analyzes the likely effect of computer based intelligence on day to day existence, with different viewpoints on its impact, going from worries about disastrous consequences for mechanical advancement to hopeful perspectives on its positive commitments. With regards to network protection, distributed computing arises as a key empowering influence for quick gamble evaluation and relief. Be that as it may, the heightening complexity of cybercriminal strategies presents considerable difficulties. Computer based intelligence driven arrangements assume an essential part in peril identification, occurrence the board, and precautionary protection against cyberattacks, subsequently reinforcing network safety pose. Regardless of fears, man-made intelligence vows to drive network protection development and work with the reception of vigorous security methodologies by ventures. Moreover, the exploration investigates the advancing scene of e-taxpayer driven organizations and highlights the basic of coordinating network protection techniques into inventive administration systems. Brilliant city drives plan to cultivate comprehensive administration by drawing in partners and utilizing artificial intelligence advancements to improve administration conveyance and network safety. The review underscores the requirement for public administrations to take on man-made intelligence driven e-administration models, cultivating consistent communication among partners and government substances. Notwithstanding, differences in online protection guidelines persevere, requiring purposeful endeavors to overcome any issues and advance mindfulness among partners.

## REFERENCES

[1] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, ‘‘Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry,’’ Mater. Today, Proc., vol. 531, pp. 1–6, 2021, doi: 10.1016/j.matpr.2021.02.531.

[2] M. Komar, V. Kochan, L. Dubchak, A. Sachenko, V. Golovko, S. Bezobrazov, and I. Romanets, ‘‘High performance adaptive system for cyberattacks detection,’’ in Proc. 9th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl. (IDAACS), vol. 2, Sep. 2017, pp. 853–858.

[3] M. D. Cavelty, Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Evanston, IL, USA: Routledge, 2007.

[4] F. Fransen, A. Smulders, and R. Kerkdijk, ‘‘Cyber security information exchange to gain insight into the effects of cyber threats and incidents,’’ ElektrotechnikInformationstechnik, vol. 132, no. 2, pp. 106–112, Mar. 2015.

[5] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, ‘‘Cybersecurity awareness in the context of the industrial Internet of Things: A systematic literature review,’’ Comput. Ind., vol. 137, May 2022, Art.no. 103614.

[6] G. A. Weaver, B. Feddersen, L. Marla, D. Wei, A. Rose, and M. Van Moer, ‘‘Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach,’’ Transp. Res. C, Emerg. Technol., vol. 137, Apr. 2022, Art.no. 103423.

[7] M. Bada and J. R. C. Nurse, ‘‘The social and psychological impact of cyberattacks,’’ in Emerging Cyber Threats and Cognitive Vulnerabilities. Amsterdam, The Netherlands: Elsevier, 2020, pp. 73–92.

[8] G. Allen and T. Chan, Artificial Intelligence and National Security. Cambridge, MA, USA:

Belfer Center for Science and International Affairs, 2017.
[9] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K. R. Choo, ‘‘Artificial intelligence in cyber security: Research advances, challenges, and opportunities,’’ Artif. Intell. Rev., vol. 55, pp. 1029–1053, Feb. 2022.
[10] Z. I. Khisamova, I. R. Begishev, and E. L. Sidorenko, ‘‘Artificial intelligence and problems of ensuring cyber security,’’ Int. J. Cyber Criminol., vol. 13, no. 2, pp. 564–577, 2019.
[11] J.-H. Li, ‘‘Cyber security meets artificial intelligence: A survey,’’ Frontiers Inf. Technol. Electron. Eng., vol. 19, no. 12, pp. 1462–1474, 2018.
[12] S. A. A. Bokhari and S. Myeong, ‘‘Use of artificial intelligence in smart cities for smart decision-making: A social innovation perspective,’’ Sustainability, vol. 14, no. 2, p. 620, Jan. 2022.
[13] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, ‘‘Cyber threat intelligence sharing: Survey and research directions,’’ Comput. Secur., vol. 87, Nov. 2019, Art. no. 101589.

**#5:-M.VASUNDARA DEVI(20H71A1257)**
B.Tech with Specialization of Information Technology in DVR&Dr.HS MICCollegeofTechnology,Kanchikacherla-52118

Author's Profiles
#1:-Mrs.S.LAVANYA working as Assistant Professor in the Department of IT in DVR&Dr,HS MIC College of Technology,Kanchikacherla-521180

#2:-G.PAVANA SRAVANTHI(20H71A1223) B.Tech with Specialization of Information Technology in DVR &Dr.HS MIC College of Technology,Kanchikacherla-521180
#3:K.VANDANA KRISHNA(20H71A1250)B.Tech with Specialization of InformationTechnology in DVR &Dr.HS MIC College of Technology,Kanchikacherla-521180

#4:-M.UDAY KIRAN (20H71A1252)B.Tech with Specialization of Information Technology in DVR &Dr.HS MIC College of Technology,Kanchikacherla-521180