The Influence of Artificial Intelligence On E-Governance and Cybersecurity in Smart Cities A Stakeholder's Perspective

Dr P Veeresh, Mr. J Mohan Kumar, Kuruva Veeranjaneyulu, Golla Ranganna, Botla Eshwar Sai Prasad, Y Pavan Kumar Reddy

Dept. of Computer Science and Engineering, St. Johns College of Engineering and Technology, Yemmiganur 518301, India

Abstract --Cities that use technology to make life better for people also known as cities have online systems to help get things done quickly. As more things are done on computers, there is a bigger chance of bad people getting into the system and causing problems like stealing information or locking it up and asking for money. The old ways of keeping things safe might not work against these kinds of threats.

In this study, a new way of using computers to think and learn, called Artificial Intelligence, is suggested to make the city run better and safer. The new system uses computer programs to find and stop bad people from getting into the system in real time and to look for things that are not normal, while making sure that people can still get the help they need from the city. The Artificial Intelligence system is used to improve the city and keep it safe from cybersecurity threats, such as data breaches and ransomware attacks. The results of the experiment show that the new method is better at finding threats than the existing method. The new solution ensures that digital governance in cities is safe and effective. It also ensures that everything runs smoothly and quickly. The new solution is good for city settings because it helps with digital governance in a secure and stable manner.

Index Terms— Artificial Intelligence, Smart Cities, EGovernance, Cybersecurity, Machine Learning.

I. INTRODUCTION

Cities use computers and the Internet to help people deal with the government. They have websites where people can do things like pay bills get certificates complain about something and look at records. These online services are fast and easy to use. This makes it

easier for people to complete tasks. The government is also more open and honest because of this technology. They do not have to do much paperwork, which saves time and effort. As more and more services are online, cities need to ensure that their computer systems are safe and secure. Smart cities require digital infrastructure to function effectively. Digital technology is very important in cities.

However, the increased use of digital technology poses a threat to cybersecurity. Government systems contain confidential information, such as personal and financial information, which can be vulnerable to cyber threats, such as hacking, phishing, and ransomware attacks. Conventional security systems are not capable of dealing with contemporary threats. Artificial Intelligence can play a significant role in monitoring unusual activities, detecting potential threats, and reacting quickly to security threats. This study proposes an AI-based framework to enhance e-governance and cybersecurity in smart cities.

II. LITERATURE SURVEY

Artificial Intelligence is very good at helping to keep our computers and networks safe from people. It can detect threats such as malware and phishing and prevent them from entering. Some studies have been conducted. They found out that Artificial Intelligence can look at a lot of network traffic data and find things that do not look right. It is better than systems that only follow rules. Artificial Intelligence can detect cyber threats faster and more accurately. Therefore, Artificial Intelligence is an important tool for keeping our digital information safe. Artificial Intelligence is good at securing the Internet and computers.

In the area of e-Governance, Artificial Intelligence is used to make public services easier to use. This means that people can receive assistance from computers. Artificial Intelligence is also used to maintain records and provide chatbot support services for citizens. Using Artificial Intelligence makes things more efficient, reduces mistakes that people make, and makes the government more transparent.

However, as the government uses computers and the Internet, there is a greater risk of cyber threats. This is a problem. Researchers believe that it is very important to have cybersecurity to protect secret government information. The government needs to ensure that its data are safe from cyber threats. Artificial Intelligence and e-governance are important. The government must also consider cybersecurity.

Few studies have been conducted on AI in cybersecurity and AI in governance separately. However, no study has integrated both concepts into a comprehensive framework. Thus, there is a requirement for a comprehensive AI solution that can enhance e-governance services as well as cybersecurity protection for smart cities.

III. SYSTEM DESIGN AND METHODOLOGY

SYSTEM DESIGN:

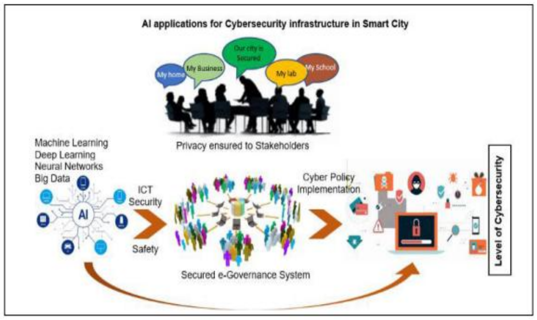
AI applications for Cybersecurity infrastructure in Smart City
My home
My Business
Our city is Secured
My lab
My School
Privacy ensured to Stakeholders
Machine Learning
Deep Learning
Neural Networks
Big Data
AI
ICT Security
Safety
Cyber Policy Implementation
Secured e-Governance System
Level of Cybersecurity

Fig. 1. Integrated AI-Driven Smart City Governance and Cybersecurity Architecture

The new system is meant to bring e-governance services and security that uses Artificial Intelligence in a simple and organized way.

The main idea behind this system is to ensure that people can easily access government services and that these services are safe.

Citizens and officials use a website to request service reports. See what is happening with their requests.

The system has a part that people do not see; it is like the brain of the system. It manages user login handling requests and ensures that all parts of the system communicate smoothly. The system is about making things simple for users, and it is also very powerful in terms of performance.

To keep the system safe from people who try to hack it, we have a special security part that uses artificial intelligence. This security part always watches what the users are doing and checks the system logs to see if anything unusual is happening. The artificial intelligence considers all the information. Problems are identified as soon as they occur. If it sees someone trying to do something, the system informs the people in charge. We keep all the information, such as what we know about the users and how our services work, in a special safe place that is locked so that only the right people can get in. The system is protected so that only authorized personnel can access the information.

METHODOLOGY:

We perform tasks in this system by obtaining information from various sources. We look at what people are doing in the system. We also checked what was happening on the network. We obtain information about the transactions that occur in the system.

We ensure that the information is good and ready for use. We removed any mistakes, copies, and missing parts. Thus, we can examine the information. Understand what the information about the transactions and the system means. After preparing the information, we identified the key pieces of information that would help the system understand what is normal and what is not. This is a very important step because if we fail to prepare the information correctly, it will impact the performance of artificial intelligence. We must ensure that the information is good so that the artificial intelligence models can perform their tasks correctly in the system and with the information.

When the data are ready, people use machine learning algorithms to identify cyber threats and unusual system behavior. The machine learning model is then put into the governance platform, where it keeps an eye on what's happening all the time. If it finds something that does not look right, the system tells the administrator so that they can do what they need to do. Over time as the system gets data the machine learning model gets better at finding new cyber threats and weird system behavior so the cyber threats and the weird system behavior can be stopped. This continuous learning process ensures that the e-governance system remains secure while providing uninterrupted services to its users.

IV. IMPLEMENTATION

The new system was made using Python because it is easy to use and it works well for machine learning and making websites.

The e-Governance system on the web was made using a framework that handles what users ask for checks who they are and gets things done.

The part that users see is safe. It lets people and administrators use the system to do things like register complaints, track services and keep an eye on the e-Governance system and the e-Governance system is very important, for this. A database system is something that we use to keep all the user details and governance data and system logs in a place. This helps us to have everything in order. We use the database system to store things, like user details and governance data and system logs.

For the purpose of ensuring cybersecurity, machine learning algorithms were designed to identify any suspicious behavior and potential cyber threats. The algorithms were trained on labeled data to identify patterns of normal and abnormal behavior. After the system has been implemented, the AI component is responsible for monitoring user behavior in real-time. If any abnormal activities are noticed, the system sends alerts to administrators. This approach ensures that governance services are efficient and highly secured against cyber threats.

V. RESULTS AND DISCUSSION

RESULTS:

The new system for e-Governance that uses Artificial Intelligence and cybersecurity was tested using network traffic data and real data from governance transactions.

The system that uses machine learning was checked to see how well it works by looking at things like how accurate it's how precise it is how well it remembers things and something called the F1-score.

The people in charge looked at the Artificial Intelligence system, for eGovernance and cybersecurity to make sure it is working correctly.

A. Performance of Intrusion Detection System

The people who made the computer program trained it. Then they tried it out to see if it could tell the difference, between normal things that happen on the computer and bad things that people do on purpose. They kept track of how the program worked and they put the results in Table 1.

Table 1: Intrusion Detection Model Performance

Metric	Value
Accuracy	91%
Precision	89%
Recall	90%
F1-Score	89.5%

The table we have here shows that the proposed system can find cyber threats well and it does this with a lot of accuracy. It is also very reliable. It does not give us many false alarms. The proposed system is good, at detecting cyber threats.

B. Comparison with Traditional Security System

The new system that uses Artificial Intelligence was compared to a security system that uses rules. The Artificial Intelligence system was checked to see how it works compared to the security system that uses rules.

Method	Accuracy
Traditional Rule-Based System	76%
Proposed AI-Based System	91%

The new system that uses intelligence is really good at finding threats. It does a better job, than the old systems we used to have. The artificial intelligence system is very accurate when it comes to detecting threats.

C. Performance Analysis of the System

The entire system was looked at to see how well it works. We checked how long it takes to respond if it is stable and if it is easy to use. The systems performance is important so we looked at the response time of the system the stability of the system and the usability of the system.

Parameter	Observed Result
Average Response Time	4–6 seconds
Threat Detection Speed	Real-time
System Stability	High
User Satisfaction	High

The system was able to respond to user requests quickly and detect threats in real time without affecting the governance services.

DISCUSSION

The result clearly shows that the combination of Artificial Intelligence with e-Governance results in a substantial increase in the efficiency of cybersecurity. The artificial intelligence system was able to find the activity correctly. This means we do not need people to watch it all the time.

The new system is better than the security system. It is better in terms of accuracy and speed. The new system is more accurate. It is also faster, than the old security system.

The addition of continuous monitoring and alert systems makes the system more reliable. Moreover, the multi-layer architecture ensures that the services of governance are not hampered even when the security scan is done in the background. The proposed system clearly shows that AI can improve cybersecurity while ensuring efficient digital governance in smart cities.

VI. CONCLUSION

We live in a time where cities are using a lot of technology. These smart cities really need online government services to work. Having these services online makes it faster and easier for people to get what they need from the government. It also means that there is a bigger chance of bad people trying to hack into the system.

The goal of this study was to combine Artificial Intelligence with government services to make them work better and be safer from cyber threats. The system that we developed uses machine learning to keep an eye on what's happening in the system find things that are not right and deal with potential threats right away. This system is about making online government services work better and keeping them safe, from cyber threats by using Artificial Intelligence and machine learning to watch what people are doing in the system and find things that are not normal in the e-Governance systems like the machine learning and Artificial Intelligence we use to make these eGovernance systems more secure.

The findings indicate that the integration of AI technology with governance systems has the potential to improve the accuracy of threat detection rates compared to the traditional security systems in place. On the other hand, the system also enables efficient public service delivery to citizens and administrators without any interruptions. In the future, the system can be improved to use more advanced AI models and improve data privacy policies to create a more secure governance environment.

ACKNOWLEDGMENT

The authors acknowledge with thanks the Department of Computer Science and Engineering, St. John's College of Engineering and Technology, for providing the necessary guidance and infrastructure. They also thank their project guide for his invaluable mentorship and continued support in building this piece of work.

REFERENCES

[1] 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," *Artificial Intelligence Review*, vol. 55, pp. 1029–1053, 2022.

[2] J.-H. Li, "Cyber security meets artificial intelligence: A survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1462–1474, 2018.

[3] R. Khatoun and S. Zeadally, "Cybersecurity and privacy solutions in smart cities," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 51–59, 2017.

[4] J. Ju, L. Liu, and Y. Feng, "Citizen-centered big data analysis-driven governance intelligence framework for smart cities," *Telecommunications Policy*, vol. 42, no. 10, pp. 881–896, 2018.

[5] G. Allen and T. Chan, *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs, 2017.

[6] M. Alam and I. R. Khan, “Application of AI in smart cities,” in *Industrial Transformation*, CRC Press, 2022, pp. 61–86.

[7] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, “Cyber threat intelligence sharing: Survey and research directions,” *Computers & Security*, vol. 87, 2019.

[8] K. Kourtit, M. M. M. Pele, P. Nijkamp, and D. T. Pele, “Safe cities in the new urban world: A comparative cluster dynamics analysis through machine learning,” *Sustainable Cities and Society*, vol. 66, 2021.

[9] S. Myeong, M. J. Ahn, Y. Kim, S. Chu, and W. Suh, “Government data performance: The roles of technology and government capacity,” *Sustainability*, vol. 13, no. 22, 2021.

[10] Z. I. Khisamova, I. R. Begishev, and E. L. Sidorenko, “Artificial intelligence and problems of ensuring cyber security,” *International Journal of Cyber Criminology*, vol. 13, no. 2, pp. 564–577, 2019.