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

T. Saritha

Assistant professor, Mathematics& statistics (ASH), Vignan’s Deemed to be University, Hyderabad

***Abstract*—Artificial intelligence (AI) has been identified as a critical technology of Fourth Industrial Revolution (Industry 4.0) for protecting computer network systems against cyber-attacks, malware, phishing, damage, or illicit access. AI has potential in strengthening the cyber capabilities and safety of nation states, local governments, and non-state entities through e-Governance. Existing research provides a mixed Association between AI, e-Governance, and cyber security; however, this relationship is believed to be context-specific. AI, e-Governance, and cyber security influence and are affected by various stakeholders possessing a variety of knowledge and expertise in respective areas. To fill this context specific gap, this study investigates the direct relationship between AI, e-Governance, and cyber security. Furthermore, this study examines the mediating role of e-Governance between AI and cyber security and moderating effect of stakeholder’s involvement on the relationship between AI, e-Governance, and cyber security. The results of PLS-SEM path modeling analysis revealed a partial mediating impact of e-Governance between AI and cyber security. Likewise, moderating influence of stakeholder’s involvement was discovered on the relationship between AI and e-Governance, as well as between e-Governance and cyber security. It implies that stakeholder’s involvement has vital significance in AI and e-Governance because all stakeholders have interest in vibrant, transparent, and secured cyberspace while using e-services. This study provides practical implications for governmental bodies of smart cities for strengthening their cyber security measures.**

I. INTRODUCTION

Cybersecurity is a critical issue in today's digital world, involving the protection of computer networks from potential threats. Cyber-attacks target networks, data, programs, and electronic information, causing significant damage and monetary loss, especially in the industrial sector. The increasing reliance on online technologies for storing personal and economic data has led to a rise in cyber-attacks, which include phishing, denial of service, malware, and ransomware. These attacks not only cause economic loss and expose confidential information but also have psychological impacts, such as stress and tension.

Artificial intelligence (AI) can significantly enhance cybersecurity and national security. AI's ability to perform tasks related to intelligence makes it a valuable tool for mitigating cyber-attack effects. AI helps detect cyber threats, improve security measures, and enhance machine learning applications for malware classification and intrusion detection. However, AI also has the potential to facilitate the initiation of cyber-attacks, making them quicker and more severe.

Smart cities, which leverage information and communication technology (ICT), face cybersecurity challenges. Insecure Wi-Fi networks and the use of digital services expose users to cybercrimes like hacking and service denials. Cybersecurity measures are crucial for protecting e-Government services in smart cities. The 'inclusive smart city' framework emphasizes the importance of involving stakeholders in digital initiatives to improve government services and meet citizens' needs. Web technologies and services can significantly impact interactions between stakeholders.

While AI's influence on smart mobility, energy management, public services, climate change, and smart security in smart cities is well-documented, its impact on cybersecurity, particularly concerning stakeholders using online government services, is often overlooked. This study aims to address this gap by examining:

II. LITERATURE SURVEY

Cybersecurity has become a paramount concern in the modern world, necessitating robust strategies to protect computer networks from potential threats. The growing reliance on online technologies for storing personal and economic data has increased the prevalence of cyber-attacks, which target networks, data, programs, and electronic information, causing significant damage and monetary loss. These attacks include phishing, denial of service, malware, and ransomware, which can affect anyone in society and have substantial psychological impacts such as stress and tension.

Artificial Intelligence (AI) offers promising solutions to enhance cybersecurity. AI can detect cyber threats, improve security measures, and enhance machine learning applications for malware classification and network intrusion detection. However, AI also has the potential to facilitate the initiation of cyber-attacks, making them quicker and more severe. Despite these risks, AI's overall potential to bolster cybersecurity is significant, as it aids in identifying cyber hazards and enhancing security precautions in cyberspace.

Smart cities, characterized by their integration of ICT, face unique cybersecurity challenges. The implementation of ICT in urban infrastructure introduces vulnerabilities, as people often use insecure Wi-Fi networks for digital services, exposing themselves to cybercrimes. Cybersecurity measures are crucial for protecting e-Government services, which are essential for smart city functionality. The 'inclusive smart city' framework emphasizes the importance of involving stakeholders in digital initiatives to improve government services and meet citizens' needs. Web technologies and services play a significant role in facilitating interactions between stakeholders.

Previous literature has explored the influence of AI on various aspects of smart cities, including smart mobility, energy management, public services, climate change, and smart security. However, the impact of AI on cybersecurity in the context of stakeholders using online government services has been relatively neglected. This gap in research is critical, as the protection of these services is paramount for the successful implementation of smart city initiatives.

Several studies have demonstrated the potential of AI in enhancing cybersecurity. AI can help detect and prevent cyber-attacks, improve response times, and develop innovative solutions to counteract security threats. For example, AI's ability to analyze large datasets can uncover patterns and anomalies indicative of cyber threats, allowing for quicker and more effective responses. Additionally, AI can facilitate the development of more sophisticated and adaptive security measures, capable of evolving in response to new threats.

However, challenges remain in fully integrating AI into cybersecurity frameworks. Issues such as data privacy, ethical considerations, and the potential misuse of AI technologies must be addressed. Furthermore, the development of AI-driven cybersecurity solutions requires significant investment in research and development, as well as collaboration between various stakeholders, including governments, private companies, and academic institutions.

III. SYSTEM ANALYSIS

EXISTING SYSTEM:

Smart cities are characterized by their integration of digital technologies and intelligent gadgets to enhance urban economic efficiency, reduce costs and resource consumption, and improve service delivery, thereby raising citizens' living standards.

Key elements of smart cities include:

- Smart Government: Enhances city governance and citizen life through smart offices, supervision, services, and decision-making, fostering collaboration between the government and citizens.
- Smart Public Services: Offers electronic information and online services to improve public satisfaction and create a service-oriented government.
- Smart Economy: Facilitates resource-driven city development, enhances urban economic efficiency, and generates sustainable employment opportunities.
- Smart Healthcare: Uses e-health records and remote tracking to predict health issues and provide optimal treatment.
- Smart Education: Utilizes data-centric intelligent education to offer personalized learning experiences.
- Smart Buildings: Apply information technologies to meet user needs, ensure

security, flexibility, efficiency, and identify operational defects.

- Smart Transport Systems: Digitally managed systems aid urban development and decision-making, enabling strategic travel scheduling through route projection and real-time monitoring.
- Smart Security: Provides detection, alarms, emergency assistance, and cybersecurity functions to protect individuals and infrastructure.

DISADAVANTAGES:

- The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cybersecurity.
- Data availability: Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.
- Incorrect labeling: The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

PROPOSED SYSTEM:

The primary objective of the proposed system is to investigate the relationship between artificial intelligence and cyber security, performing e-Governance as a mediator and stakeholders' involvement as a moderator. A longitudinal research method is conducted to investigate the hypothesis derived from this study and ascertain the findings. It comprises a study into perceptions of the importance of AI in cyber security in smart cities. The primary data for this study was collected from 478 respondents through a survey questionnaire distributed via emails and online through several social media networks.

Respondents were adequately explained about answers and were encouraged to respond to the questionnaire with utmost honesty, that may minimize issues about potential bias. Lastly, participants might opt out of the survey at any moment.

ADAVANTAGES:

- Artificial intelligence applications in smart cities contribute to e-Governance positively.
- E-Governance execution in smart cities affect cybersecurity positively.
- E-Governance mediates between artificial intelligence and cybersecurity positively.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7 Ultimate.
- Coding Language: Python.
- Front-End: Python.
- Back-End: Django-ORM
- Designing:HTML, CSS, Javascript.
- Database: MySQL (WAMP Server).

SYSTEM STUDY

FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are,

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

ECONOMICAL FEASIBILITY:

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY:

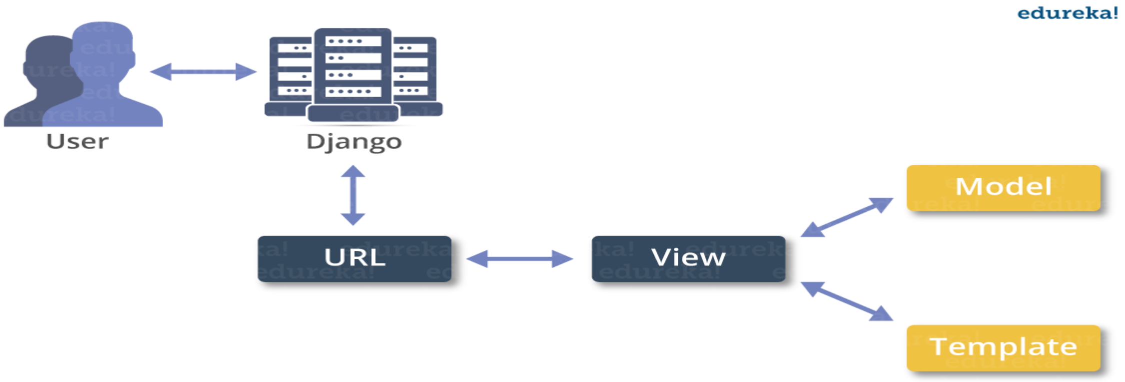
This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY:

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

DJANGO:

Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design. Built by experienced developers, it takes care of much of the hassle of Web development, so you can focus on writing your app without needing to reinvent the wheel. It's free and open source.



Create a Project

Whether you are on Windows or Linux, just get a terminal or a cmd prompt and navigate to the place you want your project to be created, then use this code −

REQUIREMENT ANALYSIS

The project involved analyzing the design of few applications so as to make the application more users friendly. To do so, it was really important to keep the navigations from one screen to the other well ordered and at the same time reducing the amount of typing the user needs to do. In order to make the application more accessible, the browser version had to be chosen so that it is compatible with most of the Browsers.

REQUIREMENT SPECIFICATION

Functional Requirements

- Graphical User interface with the User.

Software Requirements

For developing the application the following are the Software Requirements:

1. Python
2. Django

Operating Systems supported

1. Windows 7
2. Windows XP
3. Windows 8

Technologies and Languages used to Develop

1. Python

Debugger and Emulator

- Any Browser (Particularly Chrome)

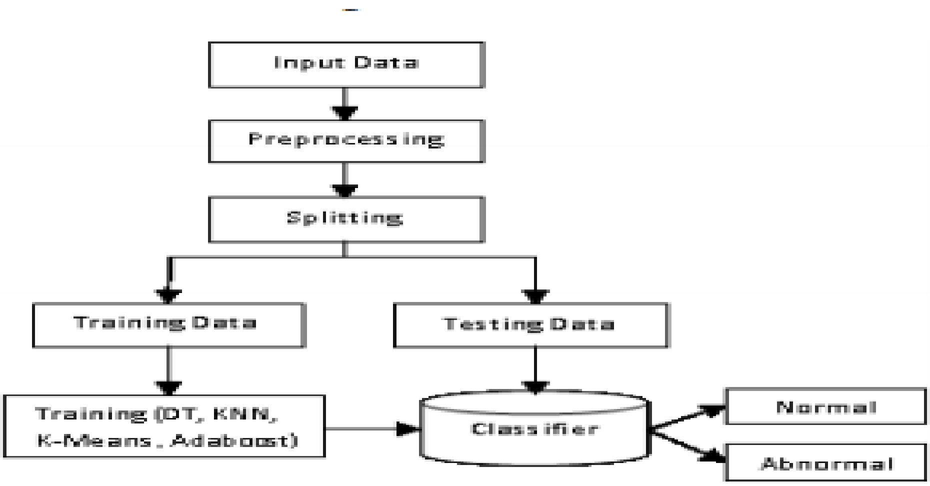
Hardware Requirements

For developing the application, the following are the Hardware Requirements:

- Processor: Pentium IV or higher
- RAM: 256 MB
- Space on Hard Disk: minimum 512MB

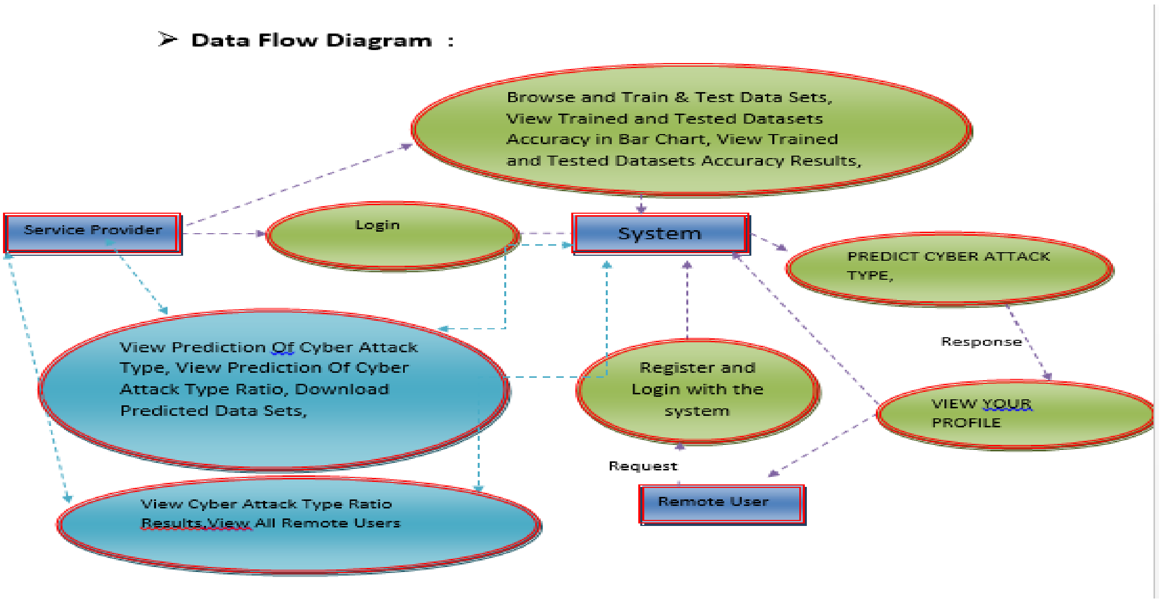
IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE:



DATA FLOW DIAGRAM:

- The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system..The data flow diagram (DFD) is one of the most important modeling tools. It isusedto model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
- DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
- DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail


➢ Data Flow Diagram :
Browse and Train & Test Data Sets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Datasets Accuracy Results,
Service Provider
Login
System
PREDICT CYBER ATTACK TYPE,
Response
View Prediction Of Cyber Attack Type, View Prediction Of Cyber Attack Type Ratio, Download Predicted Data Sets,
Register and Login with the system
VIEW YOUR PROFILE
Request
Remote User
View Cyber Attack Type Ratio Results,View All Remote Users

UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modelling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modelling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modelling of large and complex systems.

The UML is a very important part of developing objects-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

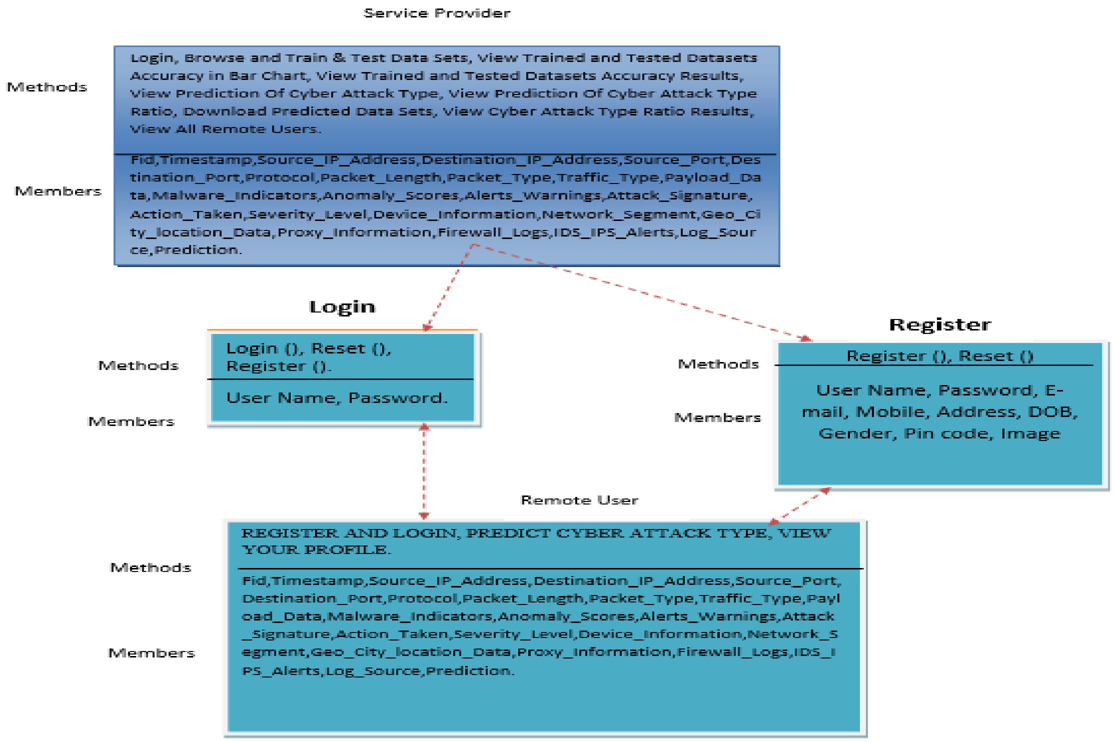
The Primary goals in the design of the UML are as follows:

- Provide users a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
- Provide extendibility and specialization mechanisms to extend the core concepts.
- Be independent of particular programming languages and development process.
- Provide a formal basis for understanding the modelling language.
- Encourage the growth of OO tools market.

USE CASE DIAGRAM:

CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modelling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information


Service Provider
Methods
Login, Browse and Train & Test Data Sets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Datasets Accuracy Results, View Prediction Of Cyber Attack Type, View Prediction Of Cyber Attack Type Ratio, Download Predicted Data Sets, View Cyber Attack Type Ratio Results, View All Remote Users.
Members
Fid,Timestamp,Source_IP_Address,Destination_IP_Address,Source_Port,Destination_Port,Protocol,Packet_Length,Packet_Type,Traffic_Type,Payload_Data,Malware_Indicators,Anomaly_Scores,Alerts_Warnings,Attack_Signature,Action_Taken,Severity_Level,Device_Information,Network_Segment,Geo_City_location_Data,Proxy_Information,Firewall_Logs,IDS_IPS_Alerts,Log_Source,Prediction.
Login
Methods
Login (), Reset (), Register ().
Members
User Name, Password.
Register
Methods
Register (), Reset ()
Members
User Name, Password, E-mail, Mobile, Address, DOB, Gender, Pin code, Image
Remote User
Methods
REGISTER AND LOGIN, PREDICT CYBER ATTACK TYPE, VIEW YOUR PROFILE.
Members
Fid,Timestamp,Source_IP_Address,Destination_IP_Address,Source_Port,Destination_Port,Protocol,Packet_Length,Packet_Type,Traffic_Type,Payload_Data,Malware_Indicators,Anomaly_Scores,Alerts_Warnings,Attack_Signature,Action_Taken,Severity_Level,Device_Information,Network_Segment,Geo_City_location_Data,Proxy_Information,Firewall_Logs,IDS_IPS_Alerts,Log_Source,Prediction.

SEQUENCE DIAGRAM:

A sequence diagram in Unified Modelling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

V. MODULES

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such asBrowse and Train & Test Data Sets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Datasets Accuracy Results, View Prediction Of Cyber Attack Type, View Prediction Of Cyber Attack Type Ratio, Download Predicted Data Sets, View Cyber Attack Type Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT CYBER ATTACK TYPE, VIEW YOUR PROFILE.

VI. SYSTEM TEST

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS:

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

System Test: System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing: White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing: Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.

Unit Testing: Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach: Field testing will be performed manually and functional tests will be written in detail.
Test objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Integration Testing: Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.
The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

User Acceptance Testing: User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

OBJECTIVES

- Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
- It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
- When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN
A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

- Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
- Select methods for presenting information.
- Create document, report, or other formats that contain information produced by the system.
- The output form of an information system should accomplish one or more of the following objectives.
- Convey information about past activities, current status or projections of theFuture.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action
- Sample Test Cases

Module: Service Provider

Test Case ID	Description	Pre-Conditions	Test Steps	Expected Result	Actual Result	Status (Pass/Fail)
SP_TC_01	Login with valid credentials	Service Provider account exists	1. Go to login page 2. Enter valid username and password 3. Click login	Successful login and redirection to dashboard	Successful login and redirected correctly	Pass
SP_TC_02	Login with invalid credentials	Service Provider account exists	1. Go to login page 2. Enter invalid username or password 3. Click login	Error message displayed	Error message "Invalid credentials" shown	Pass
SP_TC_03	Browse and Train Data Sets	Logged in as Service Provider	1. Navigate to Browse and Train Data Sets 2. Select dataset 3. Click Train	Dataset successfully trained	Dataset trained without errors	Pass
SP_TC_04	View Trained and Tested Datasets Accuracy in Bar Chart	Datasets trained and tested	1. Navigate to View Accuracy 2. Select dataset	Bar chart displayed with accuracy details	Bar chart displayed correctly	Pass
SP_TC_05	View Prediction Of Cyber Attack Type	Datasets trained and tested	1. Navigate to Prediction 2. Select dataset	Predicted cyber attack type displayed	Correct prediction displayed	Pass
SP_TC_06	Download Predicted Data Sets	Predictions available	1. Navigate to Download Predictions 2. Select dataset 3. Click Download	Predicted dataset downloaded	Dataset downloaded successfully	Pass
SP_TC_07	View All Remote Users	Logged in as Service Provider	1. Navigate to View Remote Users	List of all remote users displayed	List of users shown correctly	Pass

Module: View and Authorize Users

Module: Remote User

Test Case ID	Description	Pre-Conditions	Test Steps	Expected Result	Actual Result	Status (Pass/Fail)
RU_TC_01	Register new user	None	1. Navigate to registration page 2. Enter user details 3. Click Register	User registered successfully	User registered and added to database	Pass
RU_TC_02	Login with valid credentials	User registered and authorized	1. Go to login page 2. Enter valid username and password 3. Click login	Successful login and redirection to user dashboard	Successful login and redirected correctly	Pass

Test Case ID	Description	Pre-Conditions	Test Steps	Expected Result	Actual Result	Status (Pass/Fail)
RU_TC_03	Login with invalid credentials	User registered	1. Go to login page 2. Enter invalid username or password 3. Click login	Error message displayed	Error message "Invalid credentials" shown	Pass

VII. CONCLUSION

The current study examined artificial intelligence applications to overcome cyber security challenges. The research findings indicate that artificial intelligence is progressively converting into an indispensable technology to enhance information security performance. Individuals are not capable anymore of fully secure project-level cyber-attacks, and artificial intelligence offers the desired analytics and threat intelligence that security practitioners might use to minimize the likelihood of an infringement and strengthen the security structure of an enterprise. Since more technologies computing in cyber security is the capacity to evaluate and eliminate risk faster. Several individuals are concerned about cybercriminals' capability to perform incredibly advanced cyber and technological attacks. Moreover, artificial intelligence can contribute to the detection and classification of hazards, the structuring of incident management, and the detection of cyber-attacks before their occurrence. Consequently, despite potential negatives, artificial intelligence would contribute to the evolution of cyber security and support enterprises in establishing an enhanced security strategy.

This study further sought to investigate artificial intelligence and its ongoing development in offering e-government services and then highlight the need to accommodate strategies regarding cyber security for adopting innovative social and technical processes in government serving the community. The eventual objective of smart city governments is to establish and strengthen relationships with most stakeholders, as their involvement strengthens e-government efficacy which fortifies cyber security. Public services should be administered using innovative AI technologies and e-governance in convenient modes to eliminate the barriers between stakeholders and city governments, while state officials can still sustain the model for better support. While e-government is progressing, the citizens and those in authority or advocating mechatronics are lagging. That creates disparities in cyber security standards for something in the virtual environment, potentially turning performance into a much more difficult experience with several grooves to monitor. With an elevation in the initiatives identified in this research, stakeholders' involvement and awareness of e-governance and cyber security may rise, enabling benefits associated with the virtual environment.

REFERENCES

[1] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, ''Effectiveness of artificial intelligence techniques against cyber security risksapply 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 forcyber attacks detection,'' in *Proc. 9th IEEE Int. Conf. Intell. Data AcquisitionAdv. Comput. Syst., Technol. Appl. (IDAACS)*, vol. 2, Sep. 2017,pp. 853–858.

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

[4] F. Fransen, A. Smulders, and R. Kerkdijk, ''Cyber security informationexchange to gain insight into the effects of cyber threats and incidents,''*Elektrotechnik Informationstechnik*, vol. 132, no. 2, pp. 106–112,Mar. 2015.

[5] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, ''Cybersecurity awarenessin the context of the industrial Internet of Things: A systematic literaturereview,'' *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: Anoptimization-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 ofcyberattacks,’’ 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: Researchadvances, 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 intelligenceand problems of ensuring cyber security,’’ *Int. J. Cyber Criminol.*,vol. 13, no. 2, pp. 564–577, 2019.