# Literature Review

Generative AI has emerged as a powerful technology providing potential benefits to the various industries including cyber-security. The advancement of Large Language Model (LLM) such as ChatGPT and Gemini have marked significant milestones. However, it has raised significant concerns regarding the ethical implications and potential misuses of GenAI in cybersecurity. Security leaders and organizations have faced both benefits and challenges for implementations of GenAI. The benefits could have been increased productivity, skills enhancement, operational efficiency and cost and at the same time raised concerns about data security, vulnerability and ethical considerations. Establishing guidelines for proactive collaboration with the business stakeholders is crucial for the successful implementation of GenAI in cybersecurity to ensure safe and secure standards. A detailed framework which addresses bias mitigation, transparency, fairness and accountability for ethical AI implementations is essential to guide security leaders are making responsible decisions. A thorough risk assessment is critical to identify potential security threats and vulnerabilities with proper mitigation strategies. As a part of the project, we will develop and implement how GenAI works.

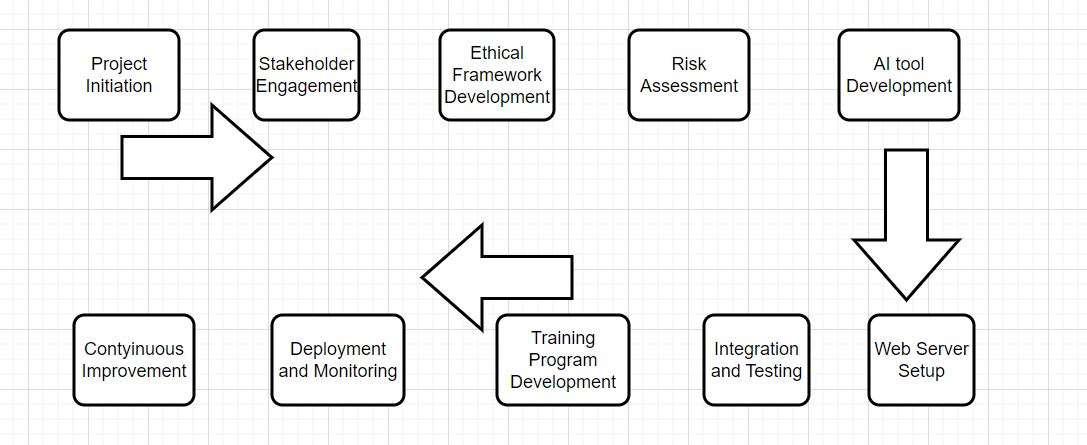


Fig: flowchart of whole process

# Project aim

The aim of the project is to provide security leaders with the appropriate knowledge, approaches and strategies to navigate the rapid evolution of Generative AI in cybersecurity, addressing both short-term Skepticism and long-term promises. This includes preparing framework of proactive collaboration with the business stakeholders through ethical guidelines for the safe and secure uses of Gen AI that align with the organization’s goals. This project also aims to provide a proper framework for the ethical implementation of GenAI such as ChatGPT and Gemini, conduct thorough risk assessments to identify potential threats and vulnerabilities in cyber security and other sectors and develop robust mitigation strategies. Additionally, it seeks to encourage organizations to provide collaborative training programs for both technical and non-technical staff for the aim of being familiar with the use of GenAI, promoting a culture of teamwork among cybersecurity experts, data scientists, and business stakeholders. Ultimately, this project includes the development of GenAI tools and deploy into the websites hosting in AWS web server. The main aim of deploying AI into the website is to detect the threats and vulnerabilities in the cybersecurity of the website.

# Introduction

The project “Generative AI: Navigating Short-Term Skepticism and Long-Term Promise” will address about the challenges and opportunities presented by generative AI in cybersecurity. The main objective of project to balance the current skepticism surrounding GenAI and its long-term potential mainly in the context of cybersecurity applications. The primary goal of the project is to develop a comprehensive strategy for security leaders to effectively integrate GenAI into their cybersecurity practices along with managing associated risks and ethical issues. This project addresses about the gap between the current skepticism and about GenAI’s immediate impact and its promising long-term potential in enhancing cybersecurity measures. In this we are going to discuss about the problems of lack of clear guidance for security leaders on how to navigate the rapid growth of GenAI in cybersecurity and how could we get benefited from GenAI in long runs. Many organizations are struggling to balance the potential benefits of GenAI such as increased productivity and reducing skills gaps. Apart from that we must be careful about the arising disadvantages, risks and ethical considerations because of GenAI.

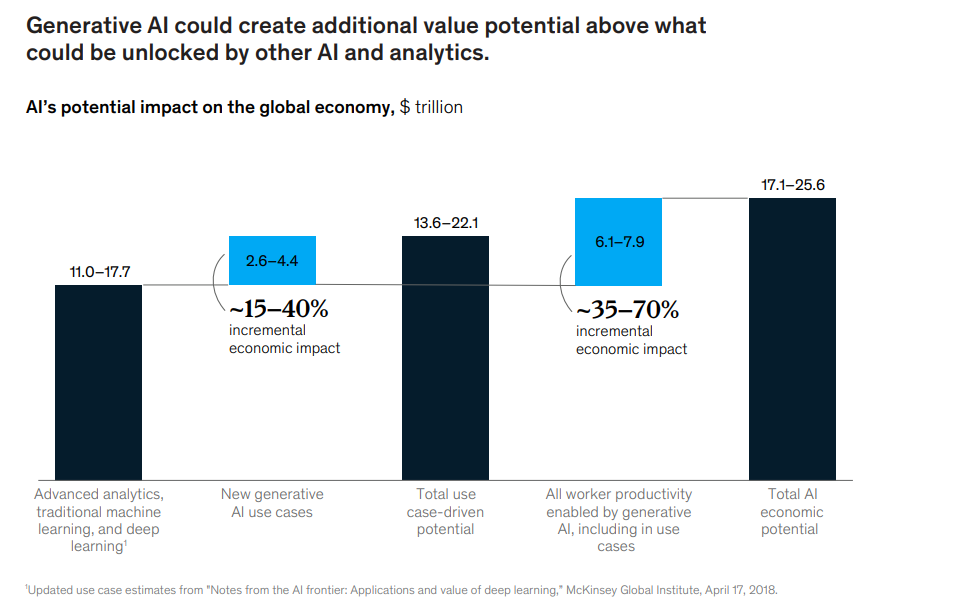
Here we have discussed about the problems arises on effectively integrating GenAI due to short-term skepticism and uncertainty about long-term benefits.

1. Lack of clear implementation strategies: organizations or stakeholders are struggled to create a comprehensive strategy for implementing GenAI into their cybersecurity framework. This includes where and how to implement, prioritization area and how to measure the success.
2. Ethical and security concerns: There are significant areas that we may need to be careful about while implementing GenAI including issues related to data privacy, biasness in decision-making and security risks.
3. Skills Gap and Workforce Adaptation: Many organizations and business area are lack of hand-on experience on implementing GenAI.
4. Risk Assessment and Mitigation: there’s a lack of clear understanding of risk associated with GenAi in cybersecurity especially implementation and potential vulnerabilities. Thay need skilled and trained people to face the considering risks.
5. Regulatory compliance: Many organizations are uncertain about make sure the use of GenAI in cybersecurity because of current and future regulatory requirements and there is rapid nature of changing in feature of GenAI.
6. Hard to convince stakeholders: Many organizations are facing challenges in convincing stakeholders and other team members about the long-term value of AI in cybersecurity, particularly looking at the current skepticism and associated risk.

# Problem from a Business Perspective

Generative AI such as ChatGPT and Gemini have been playing the important role to transform the industries by democratizing access to skills and enhancing productivity. Many businesses are integrating these technologies to drive innovation, efficiency improvement and filling skills gaps. However, rapid implementations of these technologies into business have raised several challenges

1. Intellectual Property Concerns: “The use of generative AI in creative industries raises significant legal issues such as copyright infringement and the ownership of AI-generated works” (Lucchi, 2023). Companies must navigate these complexities to avoid legal issues and ensure compliance with intellectual property laws. For example: the ChatGPT is AI based system that generates results according to training data into the system and user input, so it is difficult to identify the specific authors.
2. Economic Disruption: “Although with the help of generative AI it is possible to create new jobs and improve the quality of life, the negative effect might concern the loss of jobs and the transformation of traditional industries” (Chui et al., 2023). Generative Ai could identify and prioritize the sales leads by evaluating customers profiles and their priority and customers preferences of choosing products using AI so the organization can make a business plan by evaluating such data. Employers need to weigh this positive angle of AI and its capacity to spur innovation with the fact that AI is likely to radically alter the jobs that are available. When AI work together with the workers it may increase the productivity and accelerate the working period, many others may need to left the job at the same time.



Source: article (McKinsey & Company, 2023)

1. Managing Expectations: In the case of generative AI, more particularly, there is a need to manage expectations in the short-term while keeping an eye on their long-term possibilities. This is because to avoid disillusionment and attain sustainable adoption it is necessary to promote the strategies that are achievable in the business arena.   
   “For example: the use ChatGPT in business and similar LLM has becomes essential tools in business management used in customer service, data analysis, marketing and many other fields” (Rane, 2023). However, they must face the complexity of ethical dilemmas to technical limitations. Balancing innovation and responsibility is crucial to maximize the benefits of such AI in business. Other challenges of Gen AI similar to ChatGPT and Gemini in the business managements are limitation in contextual understanding, lack of industry base knowledge, ethical considerations and bias, data privacy, Integrity, security vulnerability etc.

# Problem from a Technical Perspective

From a technical point of view, the implementation of generative AI in cybersecurity and other fields involves several challenges:

1. Security Threats and Vulnerabilities: The use of generative AI in cybersecurity creates new risks and attacks on security field. It is crucial for organizations to evaluate the risks likely to be faced to come up with proper measures of preventing the risks that are likely to affect the systems and data.
2. Ethical Implementation: For this reason, it is important that rules of ethics are set for the use of generative AI. This entails putting in place structures that will govern the use of AI tools in a responsible, safe, and value system compliant manner.
3. Data Quality and Bias: The effectiveness of generative AI models depends heavily on the quality and diversity of the data used for training GenAI. Addressing issues related to data bias and ensuring the ethical sourcing of data are critical for the reliable deployment of AI systems.
4. Technical Expertise and Collaboration: Successful implementation of generative AI requires collaboration between cybersecurity experts, data scientists, and business stakeholders. Developing training programs to enhance the skills of both technical and non-technical staff is essential for fostering a collaborative environment and ensuring the secure use of AI technologies.

By addressing these business and technical challenges, organizations can harness the potential of generative AI while mitigating risks and ensuring ethical and secure implementation.

# Other cybersecurity related issues

In this project we will develop AI and integrate into website and the website will be hosting on AWS web server. The main purpose to integrate AI into website is for the security purpose. The AI will be designed to detect vulnerabilities of website and make it secure. During this process several cybersecurity issues may arise. Some of them are listed below:

1. Data protection and privacy: Implementing and processing AI tool chatbots or nay other AI, it may store and access sensitive user data. Poor encryption and access control may result in unauthorized access and breaches.
2. Web application security: misconfiguration in AWS, such as inadequate firewall setting and publicly access resources can lead the application to attack.
3. Social engineering attacks: “Social engineering attacks means the manipulation of individuals informing actions for revealing confidential information from individuals” (Gupta et al., 2023). In the context of cybersecurity this can be attempted to for unauthorized access, sharing sensitive data such as password or credit card number.
4. Phishing attack: “Phishing attack is type of cybercrime where attackers pose trustworthy entities to extract information from victim” (Gupta et al., 2023). Advanced AI, such as ChatGPT, Gemini etc can potentially be exploited by these attackers to make their fishing attempts more effective and harder to detect.

A diagram of a cybersecurity

Description automatically generated

Fig: Roadmap of GenAI and ChatGPT in cybersecurity and privacy (Gupta et al., 2023)

To address these cybersecurity concerns we can consider the following ideas:

To address the cybersecurity related issues, we can use AI to detect the vulnerability. Apart from that AI can help fix other related issues:

1. Password protection: “By training GenAI over large password datasets, we can make algorithms of identifying structure and patterns in commonly used passwords, so GenAI assists in passwords security assessments” (Dhoni and Kumar, 2023). Gen AI can also be used in users’ behaviour patterns such as password usages, login patterns, password changes etc. that may help Ai to detect unusual or abnormal behaviour that may point to unauthorized access to the system thus helps in potential security violations.
2. Vulnerability scanning and filtering: “The GenAI can be trained to compromise false positives which allow them to learn to generate filters that distinguish actual vulnerabilities from benign and hence reduce false positives in vulnerability scanning” (Dhoni and Kumar, 2023). Gen AI can also be used to effectively scan various programming languages for vulnerability and detects insecure code.
3. Threats hunting queries: LLMs like ChatGPT, Gemini etc can be used to create threat-hunting queries like queries for malware research and detection tools, that enhance response and detection time. They can make a job easy to security group by automatic analysing security incidents.
4. Amazon location service: implement amazon location service to track users’ location securely that helps chatbots to provide location-based responses. Identifying users’ location helps to distinguish the actual intention of the users.
5. AWS CloudFront: implement AWS CloudFront to securely handle the users’ requests. CloudFront assist to pass the original client IP address to the application we are using.
6. Other security protection layers: we can use other security protection layers such as VPC, internet getaway, load balancer, TSL, AWS WAF etc.

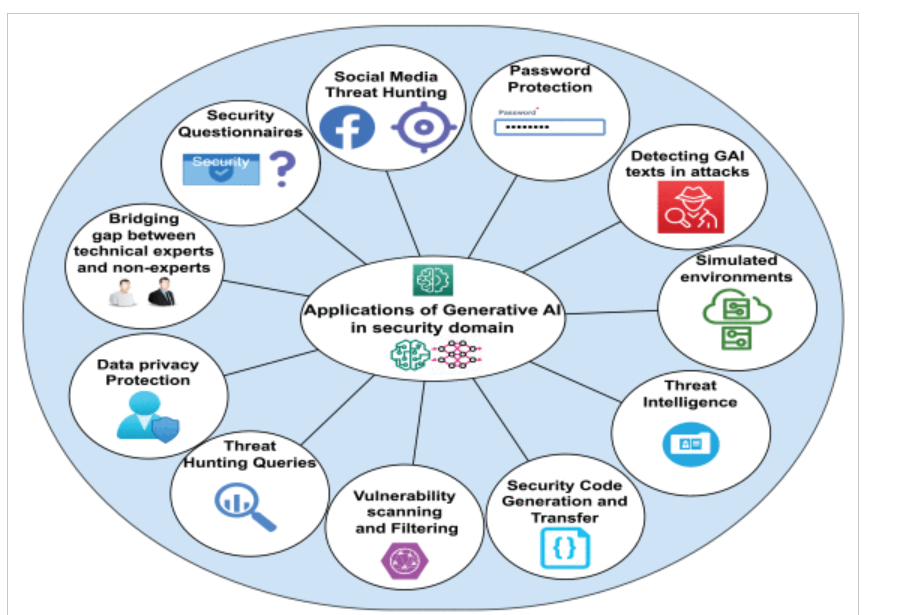


Fig: Application of AI in cybersecurity (Dhoni and Kumar, 2023)

# To solve these problems, the project will propose

1. Recommendations for active collaboration between security leaders and business stakeholders for ethical and secure use of GenAI.
2. Framework creation for GenAI implementation in cybersecurity.
3. Risk assessment and mitigation plan for applicating GenAI in cybersecurity.
4. Designing framework of collaborating training and awareness programs to both technical and non-technical staff.

This project is mainly conducted for an industry partner such as large organizations and business sectors, whoever is planning to use GenAI into their Cybersecurity practises. The security leaders, IT professionals and whole business stakeholders might be benefited through this project report. Here we have discussed about some benefits:

1. Clear guidelines for implementing GenAI into cybersecurity practises.
2. Risk management idea and idea about ethical AI implementation.
3. Ideas on how to convince security team, IT team and business team to implement Gen AI.
4. Awareness, understanding and important of GenAI across the organization cybersecurity.
5. Long-term benefits of GenAI in cybersecurity.
6. Developing specific GenAI tools or applications.

This project will not include particularly following ideas.

1. Implementing the recommendations directly within the real-world organization.
2. Provide legal advice on AI regulations.
3. Address GenAI implementing apart from cybersecurity contexts.

This project aims to provide a balanced perspective on GenAI in cybersecurity, acknowledging the current skepticism while preparing organizations to harness its long-term potential. By focusing on ethical implementation, risk management, and collaborative approaches, the project will equip security leaders with the tools and knowledge needed to navigate the evolving landscape of GenAI in cybersecurity

# Technical Requirements

This project has two important milestones:

**Milestone 1: data collection and project descriptions**

In terms of technical requirements for this project, we should have deep understanding of large language models (LLM) like ChatGPT and Gemini and their applications in cybersecurity. A strong foundation in cybersecurity principles and threat detections is essential for developing risk management strategies and mitigations plans. Similarly, knowledge of ethical AI implementations and governance framework is necessary for ethical AI implementation frameworks. For the security component we will deploy VPC attached with internet gateway, load balancer to distribute incoming traffic across AWS web server and we can use TLS, DDoS or AWS WAF for the security purposes. Then, we will do the security penetration testing on a system and see the results on cyber security concerns.

**Milestone 2: AI tool development and deployment**

In this milestone we are going to develop AI and deploy into websites. The technical requirement for this milestone is the subscriptions of Microsoft Azure / AWS web server. For this milestone we have deployed WordPress into AWS web server to run website and completed the task of website design and development. Other technical requirements are to develop a AI and integrate into website. The technical requirements for this task are strong knowledge of programming language python and running code into VS code. Proper arrangements of LLM into the AI system is essential to show the proper functioning of AI like other GenAI ChatGPT and Gemini. Apart from that the requirements are the security tools for the website so that the AI tool should be able to detect and report vulnerabilities and threats and restrict such unidentical activities. For that purpose, we can we web applications firewall, transport layer security etc.

# Specification of Requirements

Developing chatbots used in customer service is a part of our project. This will help us to understand practically the short-term limitations of generative AI followed by long-term benefits.

## Functional Requirements

The Generative AI ChatGPT, Gemini, Chatbot must be able to understand and response customer queries in a natural language in a relevant topic to the specific industry. It should be well equipped with the latest information base to provide correct information and resolutions. The system must be able to handle multiple concurrent conversations and seamlessly escalate complex issues to human agents when necessary. Integration with existing customer relationship management (CRM) systems is essential for maintaining context and customer history. Also, such AI should be able to detect the vulnerability issues regarding the cybersecurity.

**Usability Requirements**

The Generative AI should be intuitive and user-friendly, accessible across various devices and platforms supporting multiple languages and offering various options like text, voice, and visual interactions. They should be able to understand context of the conversation and maintain conversation flow, that help to provide clear and concise responses. There should always be implemented a feedback mechanism to continuously improvement of GenAI performance based on user interactions.

**Reliability Requirements**

The GenAI such as ChatGPT, Gemini, Chatbot and any other AI tools must operate with high availability and should be able to provide feedback as per the customers’ expectations. It should be able to handle sudden increase in user traffic without significant degradation in performance. The system must have robust error handling and fallback mechanisms to ensure continuous operation even when faced with unexpected inputs or system failures. The data must be backed up frequently and have proper disaster recovery plans so that there is no data loss or the time it takes to recover from such a loss.

**Performance Requirements**

The GenAI should be an always-on and available to answer questions as quickly as possible, ideally within 2 seconds of the question being asked. It must support concurrent users and should be able to increase their performance with the increasing in number of users. The system should be optimized for low latency and efficient resource utilization, ensuring smooth performance even during peak hours.

**Security Requirements**

Security of the customer data is important, and any form of customer data leak must be prohibited in the GenAI, this includes all forms of communications should be encrypted, secure authentication methods should be used in addition to the compliance with data protection laws. The GenAI must be privacy preserving, meaning that it should only gather and store necessary information and there should be frequent security checks and penetration tests to find and fix potential vulnerabilities. Additionally, the system should have measures against misuse of the AI, for example, such as generating harmful or biased content.

**UML diagram:**

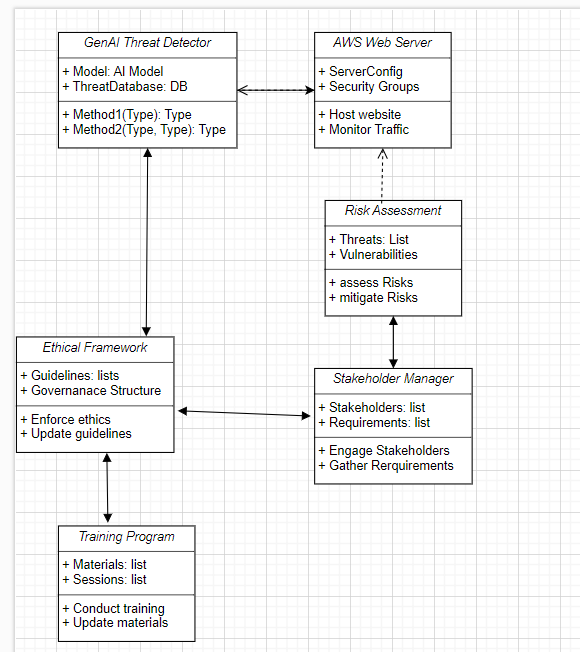
****

Fig: UML diagram

# Selection of Network and Security Technologies

The selection of network and security technologies to address the requirements of GenAI system implementations is essential. The identification, selection, and justification of appropriate network and security technologies to solve the problem of implementing Generative AI while addressing cybersecurity concerns should focus on the following key areas:

**Secure AI Platform**

Select a secure AI platform such as robust and secure cloud-based infrastructure should be implemented specifically designed for developing and deploying GenAI. Amazon web server and Microsoft azure are recommended for their scalability, reliability and comprehensive secure features. The platform should include robust authentication and access control mechanisms, end-to-end encryptions and secure APIs for integration with existing system.

**TLS (Transport Layer Security) for GenAI**

“Transport layer security plays an important role to ensure secure communication because of end-to-end encryptions” (Granjal, 2013). The design of TLS security model is helpful for pre-trained large language model such as ChatGPT, Gemini. TLS helps to maintain the privacy of the information exchanged between device and the GenAI server.

**OAuth 2.0 and OpenID Connect**

“OAuth 2.0 and OpenID Connect can be used to manage authentication and access control” (Thorgersen and Silva, 2021). OpenID Connect can be used to authenticate users securely and obtain information about the user, such as their identity and profile information. This protection also helps to protect against DDoS (distributed denial-of-service) attacks and ensure high availability, employ cloud native services like AWS shield or Azure DDoS protection.

**Web Application Firewall (WAF)**

“Web application firewall can help protect GenAI applications from common web attacks such as SQL injection, cross-site scripting etc” (Gupta et al., 2023). WAF inspect incoming traffic and filtered out malicious requests from reaching to the GenAI applications. For example: WAF detect and mitigate malicious bot traffic targeting to GenAI applications. Overall, by deploying WAF in front of GenAI applications, organizations can enhance security postures for their AI applications, protect sensitive data and maintain availability and performance of GenAI services.

# Logical/Physical network design

A diagram of a cloud computing process

Description automatically generated

Fig: Network Design

In the above figure, AI associated to the website detects the threats and vulnerabilities in the cybersecurity. The website will be hosted on AWS webserver. In addition, while implementing chatbot a user sends an enquiry message through a website, the chatbot will respond to the message from customers. In between those processes, chatbot will generate messages from information sources such as the information stored into the chatbot system or information available in the company website and response back in NLP processing. All these systems and data is stored and monitored by AWS cloud services.

# Design of Network / Security Architecture:

A diagram of a computer network

Description automatically generated

Fig: Network/security design

**Network Architecture/Protocols/Algorithms**

While deploying customer service chatbots on websites hosted on AWS cloud servers, the network architecture plays a crucial role for ensuring secure and efficient communication between clients and servers. Here is a description of the key components of the network architecture:

1. AWS Cloud: The entire system is deployed on the AWS cloud infrastructure, which provides scalability, reliability, and a wide range of services to support the deployment of applications and services.
2. Virtual Private Cloud (VPC): A VPC is created to logically isolate the network resources of the system within the AWS cloud. It allows you to define a virtual network environment with its IP address range, subnets, route tables, and network gateways.
3. Internet Gateway: An Internet Gateway is attached to the VPC to enable communication between instances in the VPC and the internet. It allows inbound and outbound traffic to and from the internet, facilitating the chatbot's interaction with users on the website.
4. Load Balancer: A load balancer is used to distribute incoming traffic across multiple AWS web servers hosting the customer service chatbot. This helps in load distribution, improves availability, and provides fault tolerance by ensuring that no single server is overwhelmed with traffic.
5. Public Key and Private Key:

* Key Infrastructure (PKI) is implemented in the network architecture to secure communications and authenticate entities. Public keys are used for encryption and verification, while private keys are used for decryption and signing.
* Public and private key pairs are used for establishing secure connections, such as SSL/TLS connections, between clients and servers. The public key is shared openly, while the private key is kept secure and known only to the server.
* Public and private keys play a crucial role in ensuring secure communication channels and protecting sensitive data transmitted over the network.

**Security Architecture/Protocols/Algorithms**

In the deployment of customer service chatbots on websites hosted on AWS cloud servers, a comprehensive security architecture is essential to protect the system from various threats and vulnerabilities. Here is a description of the key components of the security architecture:

1. Transport Layer Security (TLS):

* TLS is implemented to secure communication between clients (e.g., website visitors) and servers (AWS web servers hosting the chatbots).
* TLS encrypts data in transit, ensuring that sensitive information exchanged between clients and servers is protected from eavesdropping and tampering.
* By using TLS, the security architecture ensures the confidentiality and integrity of data transmitted over the network.

1. Distributed Denial of Service (DDoS) Protection:

* DDoS protection mechanisms are implemented to defend against DDoS attacks that aim to disrupt the availability of the website and customer service chatbots.
* Utilizing AWS Shield, a managed DDoS protection service, helps safeguard the system from volumetric and application layer DDoS attacks by detecting and mitigating malicious traffic.

1. AWS Web Application Firewall (WAF):

* AWS WAF is deployed to protect the web application (customer service chatbot) from common web exploits and vulnerabilities.
* It allows security rules to be defined to filter and monitor incoming web traffic, blocking malicious requests before they reach the web servers.
* AWS WAF works in conjunction with the load balancer to provide an additional layer of defence against SQL injection, cross-site scripting (XSS), and other security threats.

with all those above-mentioned network and security architecture, we can enhance security of the website and AI tools. Even tools will be able to notice unethical cyber threats analysing the intension of the users. Including above mentioned security protocols and algorithms and implementing network access control lists within the VPC we can inbound and outbound traffic at the traffic at the subnet level. Configuring ACL we can restrict traffic based on IP addresses and ranges that will help to effectively restrict access from unauthorised access.

# Network and Security Policies

**Password Policies**

While implementing Gen AI tool, password policy plays an important role to mitigate cybersecurity risks. When assessing cybersecurity issues, the following password policies would be the best:

1. Increase password length and complexity
2. Enforce password uniqueness
3. Implement multi-factor authentication
4. Secure password storage and transmission
5. Implement account lockout policies
6. Regular password audits

**Disaster Recovery and Business Continuity Plan**

Comprehensive Disaster Recovery and business Continuity Plan for GenAI Application and associated systems.

1. Introduction

In the case of a major disruption, this Disaster Recovery Plan (DRP) describes how to restore the GenAI application and associated systems (Townsend, 2022). Assuring operational continuity and reducing downtime, data loss, and interference with business activities are the main objectives. The first step in disaster recovery, according to Elder, J. & Elder, S. (2019, 76–78), is prevention. The business will take all reasonable precautions to lessen the likelihood of a disaster during the prevention phase. They claim that the business must consider what steps must be done to prevent harm, damage, or injury from occurring. Elder, J. & Elder, S. (2019, 78–81) state that incident response is the second phase in which the business will stop additional harm and begin to address the issue. It is said that having a single point of contact and a clear chain of command is beneficial in the event of a disaster. This individual will oversee carrying out the crisis communications, conducting situational analysis, managing the emergency response, and putting the response plan into action. The third stage, according to Elder, J. & Elder, S. (2019, 81–82), is business continuity. The stage known as "business continuation" occurs after the crisis has been contained but there are still tasks to be completed before the business can resume regular operations. The organization should think about how it will obtain the required materials, what its personnel will perform, and how it will restore business services when getting ready for this part of the plan. A recovery plan is developed when every phase is completed.

1. Objectives

Ensure Data Integrity: Protect and recover data to ensure business continuity.

Minimize Downtime: Restore the GenAI application and associated services as quickly as possible.

Maintain Communication: Ensure effective communication during and after a disaster.

Compliance: Meet regulatory requirements and maintain cybersecurity standards.

1. Scope

The Disaster Recovery Plan covers:

* GenAI Application
* Supporting IT infrastructure (servers, APIs, databases)
* Data management (customer data, proprietary information)
* Communication processes and systems.
* Business operations across various potential disruption scenarios.

1. Disaster Scenarios

* Natural Disasters: Earthquakes, floods, hurricanes
* Cyber-Attacks: All possible cyber-Attacks including Ransomware, data breaches, DDoS and so on.
* Hardware Failures: Server crashes, network failures
* Human Errors: Accidental deletion, misconfigurations
* Software Failures: Bugs, performance issues

1. Roles and Responsibilities

Disaster Recovery Team (DRT): A dedicated team responsible for executing the DRP.

Disaster Recovery Coordinator: Oversees the entire recovery process.

IT Recovery Lead: Manages IT systems and infrastructure recovery.

Data Recovery Specialist: Focuses on data integrity and restoration.

Communication Manager: Handles internal and external communications.

6. Preparation and Prevention

* Regular Backups: Schedule daily backups of GenAI application data, including customer data and training datasets. Store backups in secure, off-site locations.
* Redundant Systems: Implement failover systems and load balancing to ensure high availability.
* Update and Patch Management: Regularly update and patch GenAI software and underlying systems.
* Employee Training: Train staff on disaster recovery procedures and their roles in a disaster scenario.
* Documentation: Maintain up-to-date documentation of all systems, configurations, and recovery procedures.

7. Recovery Procedures

* Incident Detection and Notification:
* Detect and assess the severity of the incident.
* Notify the Disaster Recovery Team and key stakeholders.
* Assessment and Strategy:
* Evaluate the impact on the GenAI application and related systems.
* Develop a recovery strategy based on the type and extent of the disaster.
* Execution of Recovery Procedures:
* Data Recovery:
* Restore data from backups.
* Verify data integrity and completeness.
* System Recovery:
* Restore IT systems and infrastructure from backups or redundant systems.
* Address any hardware or software issues.
* Application Recovery:
* Reinstall or repair the GenAI application.
* Ensure all configurations and integrations are intact.
* Testing:
* Conduct thorough testing to verify that systems and applications are fully functional.
* Communication:
* Communicate with stakeholders, including customers and internal teams, about the status of the recovery process.
* Establish multiple communication channels (e.g., email, SMS, social media, and phone hotlines) to ensure that messages can be delivered even if one channel is unavailable.
* Prepare pre-approved messaging templates for various scenarios, ensuring that accurate and consistent information is delivered quickly.
* Designate a spokesperson and develop a media management plan to handle press inquiries and public statements.
* Provide regular updates and estimated timelines for recovery.
* Post-Recovery:
* Review and document the recovery process and any issues encountered.
* Conduct a post-incident analysis to identify lessons learned and areas for improvement.
* Update the Disaster Recovery Plan based on the findings and new insights.

8. Testing and Maintenance

* Regular Testing: Conduct regular drills and tests of the disaster recovery procedures to ensure readiness.
* Plan Updates: Review and update the DRP annually or following significant changes to systems or infrastructure.
* Feedback Loop: Incorporate feedback from tests and real incidents to refine the DRP.

#### 9. Business Continuity Strategies

* **Disaster Recovery as a Service (DRAAS)**: Without the requirement for specialized infrastructure, DRAAS offers a managed disaster recovery solution that guarantees an organized, safe, and effective recovery.
* **Zero Trust Data Security**: Zero trust security frameworks guarantee rigorous access control and ongoing verification, irrespective of the user's location or network, to safeguard data. Install identity and authorization management (IAM) solutions to make sure that only authorized users have access to sensitive information and systems (Snedaker, 2013). Use behavioural analytics and continuous monitoring to identify and address irregularities quickly, stopping illegal access and data breaches.
* **Operational Continuity**: To enable employees to continue working from off-site locations, establish remote work protocols, such as secure VPN access, collaboration tools, and remote desktop solutions. Determine and set up backup locations for operations (such as data centres or backup offices) so they are ready to go live in case the primary location is compromised. reassigning employees to other positions or locations as necessary to maintain vital business operations. Create a customer communication strategy to update clients on the state of operations, including any anticipated disruptions and the timeframe for recovery (Snedaker, 2013).

* **IT Infrastructure Resilience**: To keep services, data, and apps accessible in the event of an interruption, an IT infrastructure must be resilient. To guarantee that vital IT services are still accessible if core systems fail, implement redundant servers, network components, and storage systems. By using load balancing, you may prevent overloading and guarantee high availability by dividing traffic among several servers. Utilize cloud or hybrid cloud solutions to offer resilient, scalable infrastructure that can change to meet evolving business requirements. To avoid malfunctions and guarantee that systems are operating at peak efficiency, do routine maintenance and updates on IT infrastructure.

10. Compliance and Regulatory Requirements

Verify that the Disaster Recovery Plan conforms with all applicable cybersecurity and data protection laws, such as the General Data Protection Regulation, and requirements unique to the industry.

11. Conclusion

To minimize the effects of disruptions on the GenAI application and guarantee business continuity, a well-organized disaster recovery plan is necessary. Maintaining an efficient DRP requires testing, upgrades, and staff training on a regular basis. The company can continue to provide its services, uphold its good name, and guarantee long-term success even in the face of unanticipated obstacles by concentrating on data protection, IT resilience, operational continuity, and compliance.

# Deliverables

This project report will deliver following outcomes:

# Industry Analysis for GenAI

The word cybersecurity means a sets of technologies, processes and practices to protect and defend data, network, software and other devices from being attacked, damaged and unauthorized access. In these days the issues related to cybersecurity is very vast, leading to significant growth to cyberattacks for different purposes results that the important of securing IoT. “National institute of Standard and Technologies also encourage to the use more proactive and adaptive approaches towards real-time assessments, continuous monitoring and data analysis to identify, protect against, detect to, and catalogue cyberattacks to prevent future security incidents” (Kaur et al., 2023).

For all those cybersecurity issues, integrating AI tool that can provide analytics and intelligence to protect against cyber-attacks by tracking variety of cyber threats in advance to the problems. For this reason, AI can be used to automate secure tasks and support to the work of human security teams. Now a days, AI-based cybersecurity tools have been emerged to help security teams to identify risk and improve security. For this purpose, NIST has proposed cybersecurity framework to protect, detect, react and defend against cyber-attack.

A diagram of security and safety

Description automatically generated

Fig: NIST cybersecurity framework (Kaur et al., 2023)

The importance of cybersecurity protection is in all industries. For example: Health industry, IT industry, Government website, Automotive industry, banking industry etc where large number of sensitive data are stored, and high number of customers interaction includes. For securing such critical information belongs to individuals it is demanded that cybersecurity protection should be strong. For such security purpose we can integrate AI to provide extra layer for the security.

**Healthcare Industry**

Hospitals and healthcare institutions are the important industry for cybersecurity problems and solutions. Where the sensitive machines are joined to detect the diseases and large number of critical data from patients are stored. So, health industry has the high numbers of chances to face cybersecurity issues. Failing to secure the patients records private, the organization could face substantials penalties and may face reputational disadvantages. Losing access to medical records and lifesaving medical devices must be the priority for medical institutes.

**Telecommunications Industry:**

Telecommunication industry is also the important industry where large numbers of sensitive data are stored. Few years ago, Optus faced the similar kind of cyberattack and loosed access to customer information. In that data breaches Optus 10 million customers data have been stolen in 2022. This was not the first time that Optus loses their data, and it will be the last as well.

**IT Industry:**

The IT industry, being at the forefront of technological innovation, faces unique cybersecurity challenges. Companies within this industry manage vast amounts of data, including intellectual property, customer information, and sensitive internal communications. The constant evolution of technology also means that IT companies are prime targets for cyberattacks such as phishing, malware, and Distributed Denial of Service (DDoS) attacks. Failing to secure these assets can lead to significant financial losses, loss of competitive advantage, and damage to reputation. For example. In 2017, Equifax, a major consumer credit reporting agency, suffered one of the most significant data breaches in history. “Hackers exploited a vulnerability in the company’s web application software to gain unauthorized access to sensitive personal information of approximately 147 million people, including names, Social Security numbers, birth dates, addresses, and driver’s license numbers” **(**Federal Trade Commission, 2024). The breach exposed the inherent risks in the IT industry, particularly the importance of timely software patching and robust cybersecurity practices.

AI can be leveraged to enhance cybersecurity in the IT industry by providing real-time threat detection, automated responses to potential breaches, and advanced analytics to identify vulnerabilities before they are exploited.

**Government Websites:**

Government websites are critical infrastructures that store and manage sensitive information related to national security, public services, and citizen data. These websites are frequent targets of cyberattacks, including data breaches, defacements, and cyber espionage. The consequences of such attacks can be severe, potentially leading to the compromise of confidential information, disruption of public services, and erosion of public trust. For example. In 2015, the U.S. Office of Personnel Management (OPM) was the victim of a significant cyberattack, resulting in the breach of personal data belonging to over 21 million current and former federal employees. “The attackers, believed to be state sponsored, gained access to highly sensitive information, including Social Security numbers, fingerprints, and background investigation records. This breach highlighted the vulnerabilities of government websites and the critical need for enhanced cybersecurity measures” (Evan and Shimon 2015). Integrating AI into the cybersecurity framework of government websites can significantly improve their defences. AI can monitor for suspicious activities, detect anomalies in real-time, and assist in promptly responding to potential threats, thereby safeguarding critical government data and maintaining the integrity of public services.

**Banking Industry**

The banking industry is one of the most targeted sectors for cyberattacks due to the high value of financial data and transactions involved. Cyber threats such as fraud, identity theft, and ransomware pose significant risks to banks and their customers. A successful cyberattack on a bank can result in substantial financial losses, legal repercussions, and a severe loss of customer trust. For example. In 2016, hackers successfully carried out a sophisticated cyberattack on the Bangladesh Bank, leading to the theft of $81 million. The attackers infiltrated the bank’s systems and sent fraudulent transfer requests via the SWIFT network, diverting funds to accounts in the Philippines. The heist exposed weaknesses in the banking industry’s cybersecurity, particularly in securing international financial transactions (ARS STAFF 2016).AI could have played a crucial role in detecting the fraudulent activities by analysing transaction patterns and flagging anomalies for further investigation, potentially preventing the loss of funds. By proactively identifying and mitigating threats, AI helps banks protect their customers’ financial assets and maintain the security of their operations.

For this project we have chosen Automotive industry, where we will discuss about the cybersecurity problems, solutions and related issues here:

We have seen the significant rise in cybersecurity issues in Automotive Industry in recent years. in this task report we will discuss about the importance of AI in cybersecurity in Automotive Industry (Water Tunnel Car Wash company) as a reference example. Implementing AI in such industry have provided significant benefits to the organizations and has also helped to solve the privacy and security issues.

Cybersecurity related issues and solutions using GenAI tool to Automotive industry:

1. **Data privacy and security concerns:** Ensuring data security and privacy is one of the biggest issues facing the automotive industry, especially for businesses like Water Tunnel Car Wash. Customer transactions are involving more and more sensitive personal information exchanged, including names, contact details, payment information, and even vehicle-related data, as the industry gets more digitalized. This data is frequently kept in databases and accessed by a variety of technologies, such as AI-powered chatbots intended to improve customer support. Nevertheless, there are a lot of hazards associated with processing and storing such data.

Insufficient protection of this sensitive data may result in serious privacy breaches, giving unauthorized parties access to customers' personal information. Such hacks may lead to identity theft, monetary losses, and serious harm to the business's standing. The application of AI to cybersecurity offers a proactive strategy to reduce these risks by continually and instantly monitoring for any irregularities or attempts at illegal access. AI technologies can automatically identify possible security risks, allowing for quick action to stop data breaches.

1. **Network Security and Vulnerabilities**

Network security is a significant issue in the automotive sector. For several functions, including as customer support, payment processing, and operational logistics, modern automakers mainly rely on networked systems. However, because of network flaws including shoddy software, unprotected Wi-Fi networks, and inadequate encryption, cybercriminals frequently target these networked systems.

Ransomware, for example, is a type of hack that can cripple an entire network and prevent access to vital data and services unless a ransom is paid. By using machine learning algorithms to find odd patterns of behaviour inside the network, artificial intelligence (AI) can play a key role in locating and addressing these vulnerabilities in the network. By examining historical events and present danger landscapes, AI can also anticipate possible attack vectors, enabling businesses to fortify their network defences prior to an attack.

1. **Secure AI Integration**

Care must be taken when integrating AI into an automotive company's cybersecurity architecture. Even though artificial intelligence (AI) has many advantages, it also poses new security risks. For example, there is a chance that hostile actors will exploit AI algorithms to get beyond security safeguards. Companies need to take a multi-layered security approach to combat this, which involves ongoing algorithm changes, continuous performance monitoring of AI, and secure AI development methods.

Because AI technologies offer dynamic threat detection and response capabilities, they may also be used to protect the systems that they are a part of. AI-driven systems, for instance, can automatically modify security procedures in reaction to new threats, guaranteeing that the business's cybersecurity defences continue to be strong even in the face of constantly changing cyberthreats.

1. **Regulatory Compliance and Ethical Considerations.**

Like many other industries, the automotive sector is governed by stringent laws pertaining to cybersecurity and data protection. Maintaining customer trust and avoiding legal ramifications necessitates compliance with rules such as the California Consumer Privacy Act (CCPA) in the US and the General Data Protection Regulation (GDPR) in Europe. By automating the tracking of data usage, access controls, and permission management, artificial intelligence (AI) can help ensure compliance and lower the risk of regulatory violations.

Equally crucial is the moral use of AI in cybersecurity, though. Businesses need to make sure AI solutions are transparent and protect client privacy when they are built and deployed. Customers must be informed about the collection, storage, and use of their data. Additionally, judgments made by AI-powered systems, like those pertaining to security precautions, must be transparent and equitable.

The Water Tunnel Car Wash company serves as an example of how AI integration into the automotive cybersecurity framework considerable potential has must improve data privacy, network security, and overall operational resilience. Automotive firms preserve regulatory compliance, safeguard sensitive consumer data, and create a more reliable and secure digital environment by using AI to proactively handle cybersecurity concerns. However, to fully reap the benefits of AI while minimizing associated hazards, significant thought must be paid to its ethical and secure application.

# Website Design and Development

Regarding the technical progress of the project till now, we have developed and designed a website for Automotive industry specific to WaterTunnel car wash company. For developing websites, we deployed Wordpress certified by Bitnami by using aws web server involving several steps. The main reasons for choosing aws cloud service for deploying wordpress are security and cost-effectiveness. When we completed the process of launching instances in EC2 we received a public IPv4 address and login username and password for the wordpress website.

A screenshot of a computer

Description automatically generated

Fig: Launching Bitnami WordPress in AWS.

When creating websites then we collected different resources from online sources and some of them are designed by yourself. The website contains everything that needs to be a perfect website. The website is all about company’s information and car wash features. The website includes service details, Wash Menu, contact details etc. Here are some glimpses on our websites.

A blue screen with white text

Description automatically generated

Fig: Company Website

A close-up of a website

Description automatically generated

Fig: Company Website

# AI Tool to Detect Vulnerabilities in Cybersecurity (In Progress)

Gen AI plays an important role in providing security layers for the website or any other application.as we already discussed about the problems, solutions, benefits and limitations of GenAI while detecting the vulnerabilities in cybersecurity. Here, our aim is to generate such AI tool which detects Vulnerabilities on the website that we already designed.

The AI will be based on the following algorithms:

* 1. Data collection:
* Gather website content including HTML, CSS, JavaScript and backend code for analysis.
* Extract security related metadata such as headers, cookies, and response codes.
  1. Input processing:
* Tokenize and purse the website code into analysable units.
* Normalise data to eliminate any inconsistencies.
  1. Vulnerability detection:
* Pattern matching: Identify known vulnerability pattern using predefined rule sets (e.g SQL injection, XSS, CSRF).
* Anomaly detection: Use AI/ML models to detect unusual patterns or deviations in the website’s structure and that may indicate new vulnerabilities.
  1. Security Compliance Check:
* Compare website configurations and code against industry security standards (e.g., OWASP Top 10) to ensure compliance.
* Generate a compliance report highlighting areas of concern.
  1. Recommendation Generation:
* Based on detected vulnerabilities, generate actionable security recommendations.
* Prioritize vulnerabilities by severity and impact.
  1. Reporting:
* Generate a detailed security report with findings, risk assessments, and recommended actions.
* Provide options for automatic or manual fixes based on severity.
  1. Deployment:
* Integrate the Al tool into a continuous integration/continuous deployment (CI/CD) pipeline.
* Deploy the Al tool on AWS to enable scalability and access control.
  1. Feedback Loop:
* Continuously update the Al models with new vulnerability data and improve detection algorithms based on user feedback.

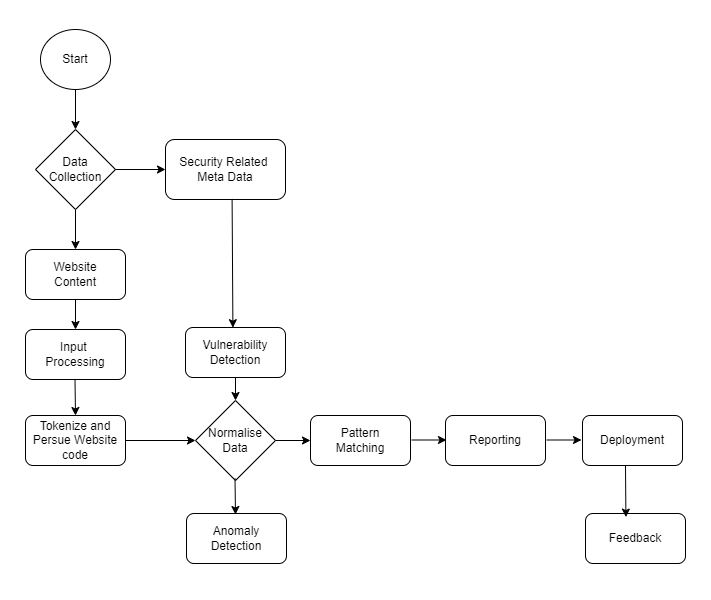


Fig: flowchart for GenAI Tool

# Integrating Chatbot into Website

For this task we have chosen Automotive industry i.e WaterTunnel car wash company. We will also evaluate organization’s benefits, stakeholder’s overview and customer’s reaction upon using chatbot. This task will develop a comprehensive strategy for security leaders to effectively integrate chatbots into their organization’s system along with managing associated risks and ethical issues. In this task we will also discuss about the problems on lack of clear guidance for IT leaders and other technical and non-technical staff on how to use and implement chatbots into their organization’s security system and how could we get benefited from such type of GenAI in long runs. Many organizations are struggling to balance the potential benefits of using chatbots as customer service provider such as increased productivity, cost effective, consistency and availability. Apart from that we must be careful about the implementation strategies, ethical and security concerns, skills gap and customers adaptations.

The figure below shows the flow charts of customer service chatbots working process.

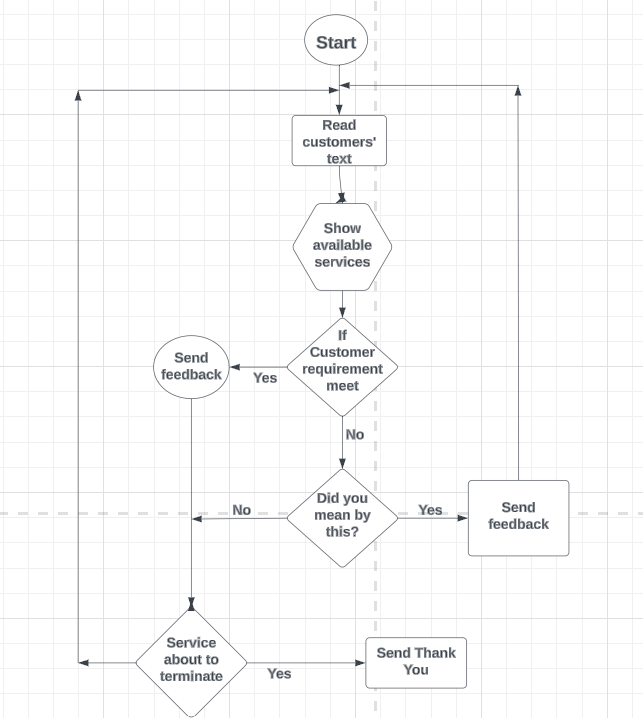


Fig: flowchart of Chatbots working process

The flowchart shows when the customers send an enquiry message, the chatbot reads the text message and replies to the message that shows the available services in the format of “Hello! How can I help you today”? If the customers ask about price, then chatbots reply “our basic car wash package starts from 10$” and so on. If the customers’ requirement does not meet the criteria, then ask a feedback question,did you mean by this type of car wash (wash menu such as exterior wash, interior wash or both etc)? If the customer says yes, send feedback and if the customer says no then inform them the service is about to terminate and send them a “Thank you” message at the end.

To complete this task, we have divided the following sub tasks which are as follows

# Industry Analysis for GenAI Chatbots

We have seen the significant rise in use of customer service chatbot in Automotive Industry in recent years. in this task of report we will discuss about the use of chatbot as customer service in Automotive Industry (Water Tunnel Car Wash company) as a reference example. Using chatbot in such industry have provided significant benefits to the owner and has also helped to cover wide range of customers. In this topic we will discuss about the current trends, challenges and opportunities of using chatbots in Automotive industry in more details.

**Current trends**

The use of chatbot as a customer service is rising in every industry. chatbots is very popular in healthcare industry, IT industry, tourism and hospitality, finance and business etc. apart from that Automotive industry is not far away from that. Here we will further discuss the current trends of using chatbots as a customer service in Automotive Industry.

1. Personalized customer interactions: Chatbots has been using as a personalized customer interactions in this Industry. automotive industries are implementing GenAI chatbots for highly personalized customer experiences where the personal details of every customer have stored in a system safely. These chatbots analyse the customer data and service history and provide the service recommendations and other useful information.
2. 24/7 availability: the increasing trend of use of chatbots boost because of their availability. They can interact with customers at any time and customers can get update of service availability at any time. Apert from the more interactions with customers also helping the to grow Automotive Industry.
3. Multilingual support: the chatbots who can interact in many languages are in trend in such Industry. This is because such chatbots can cover wide range of customers such as native and non-native speakers from different regions ultimately that helps in grow of Automotive Business.
4. Integration in vehicle system: The system of chatbots can deploy into vehicle systems that helps to find actual update of what’s wrong with the vehicle and what need to be done to repair it. Such kind of chatbots is very useful in finding actual maintenance issues.

Picture below shows clearly how GenAI chatbot works as a customer service in Automotive Industry. In this project we will create a chatbots for customer service in the same format as shown below and deploy it into the website based on Automotive Industry.

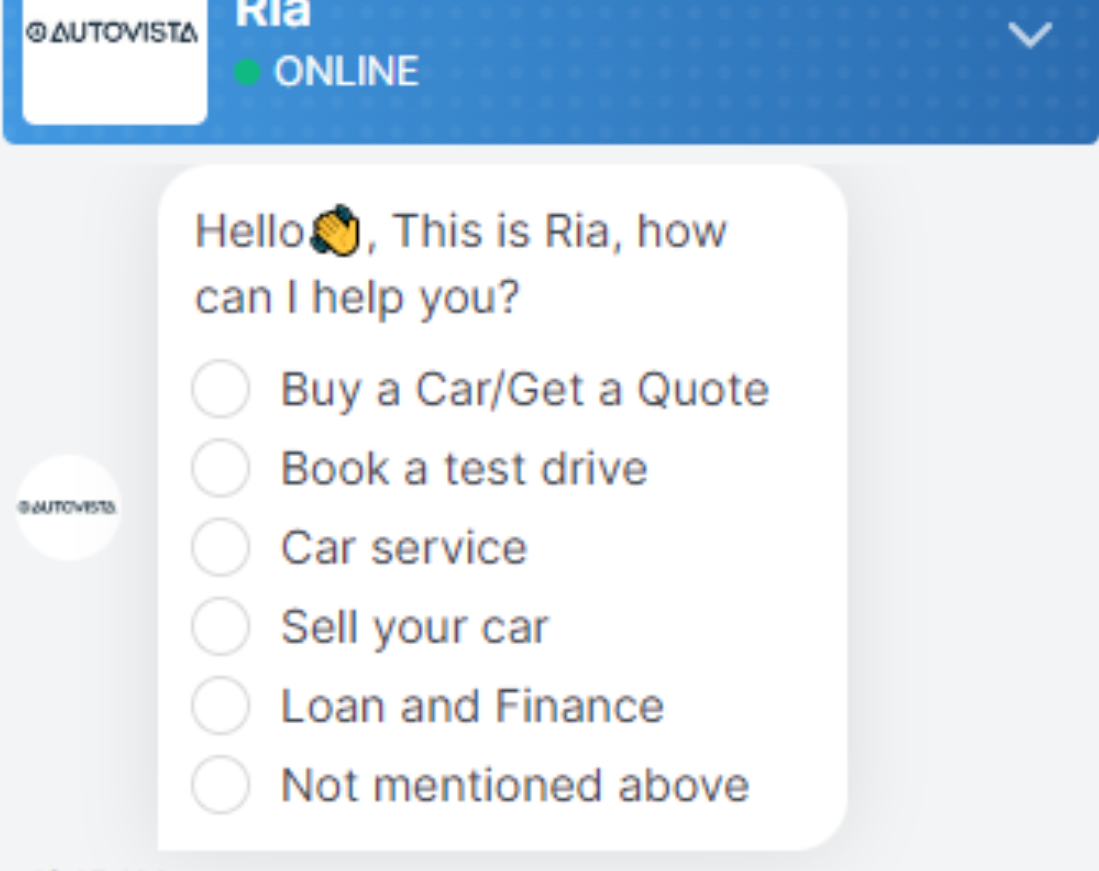
****

Fig 1: source google

**Challenges**

Despite of having very useful benefits of using chatbots as a customer service, we could face some noticeable challenges while implementing it. Here we will discuss about the challenges caused by chatbots, that we need to be aware of its implementations.

1. Data privacy and security concerns: the first and main challenges while implementing chatbots as a customer service is data privacy and security. While interacting with customers, the customers may need to provide their personal information to the chatbots that stored into the chatbots system. Such information need to keep safe and secrete for customers privacy. Sometimes the third person steal the personal information from such type of chatbots system.
2. Accuracy and reliability: Another challenge arises while using chatbots is accuracy and reliability. The information provided by the chatbots must be accurate and reliable to customers. Sometimes chatbots may not provide information for complex queries that creates dissatisfactions to customers and reliability issues.
3. Difficulties in Integrations with system: Integrations of chatbots systems into companies’ system may need expertise into the same field and may have expensive in the budget. While integrating chatbots into companies’ system the chatbot can excess the private information of company that may arise the big concerns on data security.
4. Continuous learning and updating: the chatbots may need to update regularly otherwise they may provide outdated and misinformation to customers. The update could have been new programming systems, features, update upon company such as companies’ new police, vehicle information, customers benefit etc. That may have costly as well as may create conflict of interest among stakeholders either it is implement or not.

**Opportunities**

Despite of having some challenges on implementing customer service chatbots it provides great opportunities to grow business. Here are some opportunities provided by chatbots after its implementations:

1. Improve customer interactions: as we discussed above about its availability. It is available all-time times and customers can interact at any time that helps in covering more customers, that helps in business growth. Apart from that chatbots can analyse customers preferences, interest and their behaviours through interacting them, analysing data stored in system industries can create a market strategy and improve in their service and product.
2. Cost reduction: implementing chatbots can provide an opportunity of reducing cost. Chatbots can handle large number of enquiries in a significant time that may take long time for human for the same work. So that other people can handle other more complex task.
3. Expansion into new market: as we discussed chatbots can interact with many customers in many languages that help in expanding the business into new market easily. Chatbots can handle the enquiries upon car dealership, maintenance, pricing and troubleshooting etc which more than enough to grow business into new market.

Figure below shows the clear information of benefits of using Chatbots in Automotive Industry.

**A screenshot of a computer

Description automatically generated**

Fig 2: Source google

**Current capabilities**

1. Natural language understanding: “Gen AI chatbots can understand and respond to natural languages that fixed into its programming, also can interact wide ranges of customer inquiries in the natural languages, in the same way as human” Adamopoulou and Moussiades (2020, p. 100006). Such understanding makes customer easy to interact and solve the problem of standing into long line for services and reduced the waiting time.
2. 24/7 availability: chatbots can provide all time customer service support, addressing simple to moderate inquiries without human support. This feature is very supportive to the business in Automotive service. For instance: if someone has left their vehicle to the service and wants some update about what time it is going to be ready, they can inform anytime with the help of chatbots.
3. Multilingual capabilities: chatbots can communicate in multiple languages and can cover wide ranges of customer into the automotive business. Such kind of chatbots can cover broader range of customers such as native and non-native speakers from different regions and help to support the business internationally.
4. Integrate backed systems: “Chatbots can access and provide information from company’s internal data bases and systems and can offer real-time updates on services, scheduling appointments and vehicle information” Wang et al. (2022, p. 102535). For example: how long does it take to be ready customer’s vehicles and how long they need to be wait for next service.
5. Service appointment scheduling: customer support chatbots can assist in scheduling appointment service online, check the availability day, and receive reminder. Apart from that it can provide real-time update of vehicles repairs and maintenance.

**Limitations**

1. Emotional intelligence: current chatbots are lack of true emotional intelligence, which may lead to same emotional responses in different situations. Current chatbots are lack of emotional supports to the customer services.
2. Handling complex situations: Gen AI chatbots can interact limited queries that fixed into its system. Furthermore, chatbots can generate responses based on training data into its system, they may struggle with creative problem-solving situations. They may provide same answers in different queries in that situations human communication may needed.
3. Potential misinformation: “Chatbots as a customer service need to be updated regularly otherwise, they may provide inaccurate or outdated information” Hasal et al. (2021, p. e6426). Such misinformation could have been providing incorrect information about features, update and specifications that may lead misunderstanding to customers.
4. Privacy and security concerns: while using customer service chatbots, customer need to provide their personal data and information that stored into the chatbots system. That may lead to privacy and security issues because of cyber threats.
5. Maintenance and updates: chatbots may require regular update and training to improve their performance better. They may not handle unexpected enquiries from customers because they have fixed limited program into their system. So, they may not provide details explanations and advice that human expert can offer.

**Potential future developments**

1. Enhanced contextual understanding: future chatbots are likely to understand the situations of the customers and react according to the customers demand and can provide more accurate, natural and relevant responses.
2. Emotional intelligence: the future chatbots are expected to recognize the emotions of the customers and react accordingly. For example: if the customers are angry, chatbots should be able to calm down them in the same way how human customers service provider do. Overall, future chatbots should be able to understand human expressions.
3. Integration with IoT: when chatbots is connected to the IoT devices within the vehicles then it would be easy to understand the actual conditions of vehicles, what is the actual problems, maintenance alerts etc.
4. Voice recognitions: it is expected to develop a chatbots who can understand the customers voice message to interact with. It will be preferable to with through a voice message rather than texting if the chatbots are able to two-way communications.
5. Sales assistance: it is expected that the chatbots can assist in sales process of Automotive industry such as helping customers selecting and purchasing vehicles, providing financial suggestions and even providing virtual test drives.

While successfully navigating the short-term skepticism and long-term promises of using GenAI chatbots in the automotive customer service sectors, the company should follow the following criteria to mitigating risks and building trust with their customers:

1. Implement enough training and monitoring systems to make sure the accuracy and appropriate responses to the customers.
2. Company should prioritize data privacy and security in chatbot system while designing and implementing chatbots.
3. There should be clear guidelines for the limitations of what chatbots can do and there should always be human to assist customers for more complex issues.
4. Regularly gather the customers feedback and update working system of chatbots accordingly.

Considering above mentioned current capabilities, limitations and future developments here we have designed the SWOT analysis of customer service chatbot used in automotive industry.

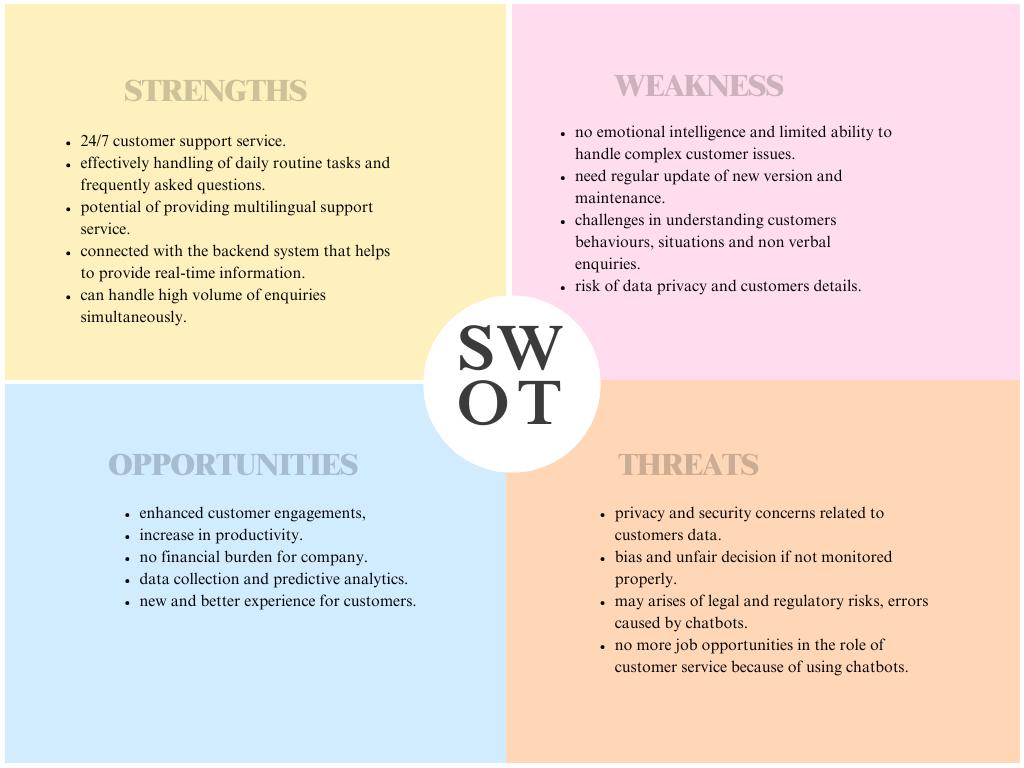


Fig: SWOT analysis of customer service chatbots used on Automotive Industry.

**Training Needs Analysis**

To effectively utilize the GenAI chatbots within the organizations, it is important to assess the training needs for both technical and no-technical staff. Here we will describe about the training needs analysis and skills gaps between the technical and non-technical staff that will help us to identify what training needed them.

Training Needs Analysis:

1. Identify the organizations objectives: it is necessary to identify the organizations’ objective regarding the implementations of chatbots and training needed for their staff. The general trends of implementing customer service chatbots is to improve the customer experience, escape out from automatic routine tasks, enhancing data analysis capabilities etc. so it is necessary to finalize all these tasks are needed to be done by chatbots or not. If so, let the staff know how chatbots works, how it assists them and let them to be familiar working together with GenAI chatbots.
2. Evaluate Current Skill Levels: Evaluate the current skills of the technical and non-technical staff regarding the GenAI implementations. Conduct surveys and interviews to assess the current understanding and skills related to GenAI among both technical and non-technical staff. Identify gaps in knowledge about GenAI principles, ethical considerations, and practical applications. Then you will be able to identify the skills gaps regarding the AI implementation. That help to sketch out to what training needed them.
3. Determine Required Skills: when you evaluate the current skills then you can determine what skills they have and what skills needed them for the effective GenAI implementation. In general, technical staff focus on skills such as model management, data preparation, and output monitoring and non-technical staff, emphasize understanding GenAI capabilities, ethical use, and effective communication with technical teams.
4. Set Training Objectives: there should be clear objectives of the training program when you provide training them such as AI knowledge, collaborations between Machine Learning and other team members, and ensuring ethical use of GenaAI.

**Skills Gap Analysis**

1. **Technical Staff:** among the technical staff who know about the GenAI chatbots implementations still may have skill gaps in the following area.
   * Model Management: modelling management in chatbot implementations is designing, building and maintaining the conversational model that chatbots uses to the customers. It involves dialogue flow, intent and entities, setting up responses and managing over all behaviour of the chatbots. Technical staff needed these Skills in training, supervising, and managing GenAI models to ensure accurate and ethical outputs.
   * Data Handling: data handlings in chatbots is how chatbots manage, utilize and process the data to understand users’ input, provide response and improve their performance over time. Competence in preparing and managing data for GenAI applications, including understanding privacy and security considerations.
   * Output Monitoring:Output monitoring helps to ensure the chatbots are providing accurate and relevant response to the user’s input. Monitoring chatbots outputs, staff can identify any errors, inconstancy and misunderstandings in the responses and takes correct steps to solve these issues. Ability to monitor and evaluate chatbot responses to ensure alignment with organizational values and messaging.
2. **Non-Technical Staff**: among the non-technical staff they may have followed skills gap for the GenAI chatbots implementations:
   * AI Literacy: AI literacy meaning the understand and knowledge that individuals have about AI concepts, technologies and applications. The non-technical staff may not be aware of basic understanding of GenAI technology, its potential applications, and limitations.
   * Ethical Considerations: Awareness of ethical issues related to GenAI, such as bias, privacy, and responsible use. Non-technical staff may not be aware of how biasness could have been the AI system. Without understanding ethical considerations of biasness and fairness the staff may not to understand the importance of biases training data and decision-making processes. Without understanding the importance of privacy regulations, the non-technical staff may mishandle the sensitive users information leading to privacy breaches and introduce compliance issues.
   * Communication and Collaboration: Non-technical staff may lack of skills to effectively communicate with technical teams and contribute to the development and supervision of GenAI applications.

By evaluating comprehensive Training Needs Analysis and Skills Gap Analysis, organizations can design targeted training programs that address specific needs, enhance overall competency, and ensure the successful integration of GenAI chatbots into business processes. This approach not only bridges current skills gaps but also prepares the workforce for future technological advancements.

Here we have recommended the training requirements for both technical and non-technical staff regarding the use of GenAI Chatbots within the organizations.

**Training Requirements for Technical Staff**

1. Model Management and Supervision:
   * Training vs. Supervising: Understand the distinction between training GenAI models and supervising their outputs. Technical staff need to be skilled in supervising the results of language models to ensure they align with company values and messaging. Apart from that, the technical staff need to be well known about the programming language and tools to deploy. Develop and maintain chatbots. Similarly, understanding of NLP is most important for developing chatbots that can understand and response ton natural language to the customers.
   * Data Preparation and Handling: Learn how to prepare and manage data effectively for GenAI applications, including dealing with legacy data and ensuring data quality and privacy. Data preparation could be collecting data that used to train chatbots such as chat transcripts, customer interactions questions answers sample, and other data source that helps chatbots to provide feedback users’ queries correctly. Technical staff need to delete row data that used to train chatbots that causes noise and errors providing the updated information to customers.
2. Prompt Engineering: technical staff should develop skills in crafting effective prompts that guide GenAI chatbots to produce accurate and relevant responses. This includes establishing personas, providing context, and using modifiers to control the output at the same time use simple languages that is familiar to targeted audience.
3. Security and Risk Mitigation: technical staff who is involve into the implementations of chatbots should be aware of security best practices and mitigation strategies to ensure the protections of sensitive information of customers and mitigate the potential threats. Encryptions, authentication and authorizations, secure communications etc are the basic skills that need to have technical staff for chatbots managements and implementations.
4. Output Monitoring and Filtering: Implement filtering systems to monitor and cleanse chatbot outputs before they reach end-users, ensuring that responses are appropriate and aligned with organizational standards. Technical staff should he skilled in monitoring the quality of chatbots responses to ensure that they are accurate, relevant and useful to users. Set up the performance matrices to measure the performance of matrices and review regularly to identify the areas for improvements.

**Training Requirements for Non-Technical Staff**

1. AI Literacy and Ethical Use: the non-technical staff who is involved into the implementation and development of chatbots should have the fundamental understanding of AI and how chatbots works. This includes natural language processing, machine learning, and how chatbots interacts with customers to provide information and assistance. They also should be aware of potential biasness in chatbots and understand the importance of fairness and equity in chatbots interactions. They also understand the importance of protecting users’ data and maintain privacy and security in users’ interactions.
2. Communication and Collaboration: Enhance skills in communicating effectively with technical teams and contributing to the supervision and refinement of GenAI applications.
3. Understanding GenAI Capabilities and Limitations: Non-technical staff should be aware of what GenAI can and cannot do, including its potential applications and limitations in the workplace. If the customers are not satisfied with the chatbots interactions, then the staff should be able to interact with users in place of chatbots.
4. Practical Application and Use Cases: Learn how to apply GenAI tools in everyday tasks, such as customer service, marketing, and HR, and understand appropriate and inappropriate uses of the technology.

# Chatbot deployment and Testing

While integrating chatbot into the website we have made and named chatbot through FastBots.ai and import data from website. When integrating designed chatbot into our website we used embed script provided by FastBots as simple as we used plugin for easier integration. Then we monitor interaction, gather insights and update the chatbots for proper functioning:

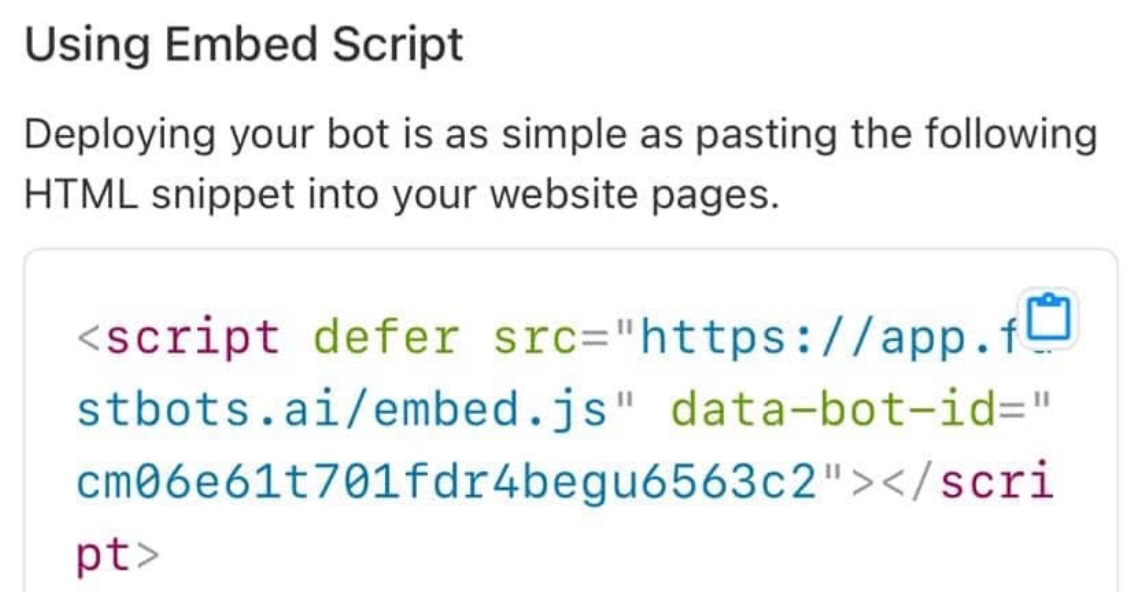


Fig: Embed script to link chatbot into website.

The figure below shows the proper functioning of chatbot and provide all the information belongs to the website.

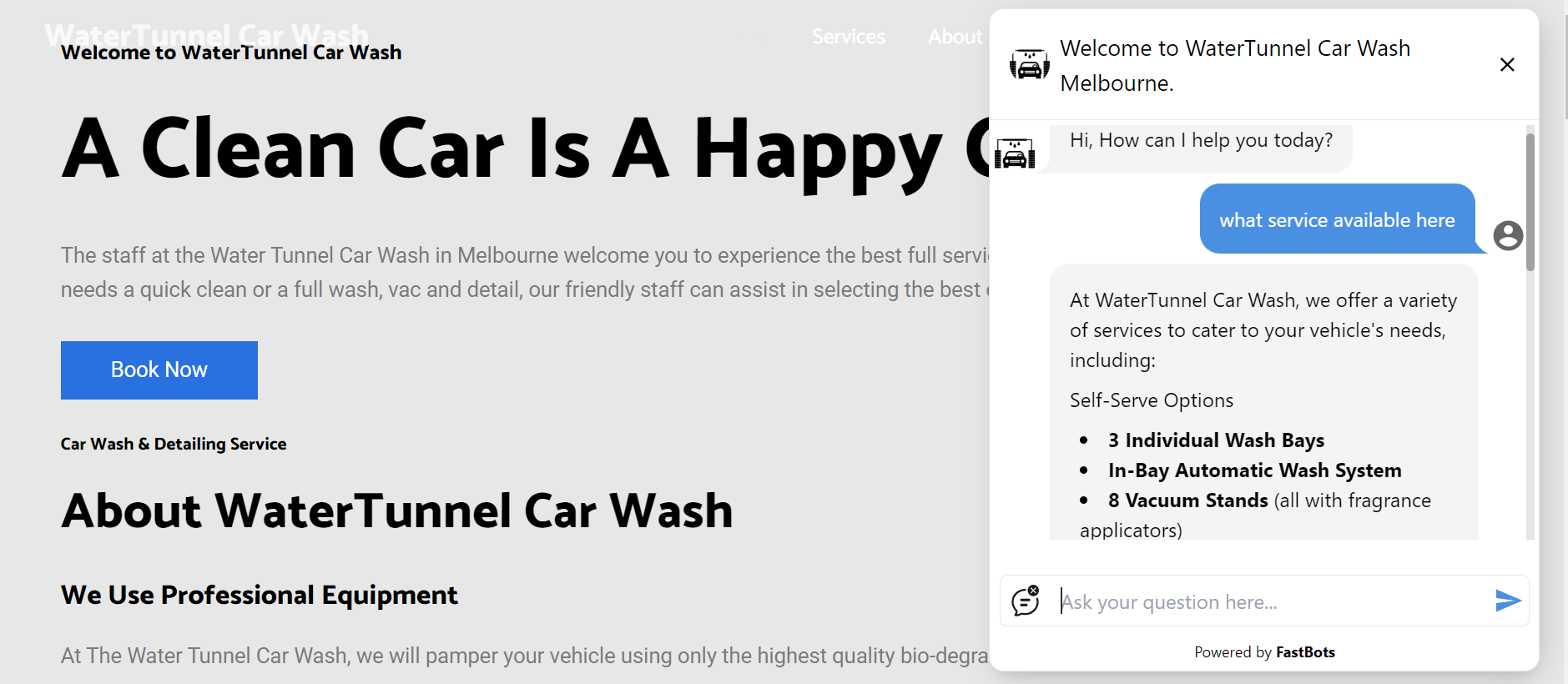


Fig: integration of chatbot into website

# Updated project plan

|  |  |  |
| --- | --- | --- |
| Task | Description | Deliverables |
| Industry Analysis for GenAI | Research current trends, challenges, and opportunities in GenAI implementation for cybersecurity. | Detail industry analysis report. |
| Stakeholder Identification and Analysis | Identify key stakeholders within the organization who will be impacted by implementing GenAI in cybersecurity. | -Stakeholders identification report  -Stakeholder matrix (influence/interest) |
| Ethical AI Framework Development | Create a framework for ethical AI implementation specific to GenAI implementation. | Ethical AI framework document |
| Website design and development | Develop and design website and deploy into AWS web server. | Show designed website. |
| Integrating AI into website hosting on AWS web server. | Design AI tool to detect vulnerabilities in cybersecurity and deploy into the website. | Show the results from security/ penetration testing on a system. |
| Risk Assessment and recommend security control to solve the problem | Identify and evaluate potential risks associated with GenAI implementation cybersecurity | - Risk assessment matrix - Risk mitigation strategies report |
| Collaboration Strategy Development | Develop strategies for proactive collaboration between security leaders and business stakeholders. | -Collaboration framework document  -Communication plan |
| Training Needs Analysis and awareness program | Assess the training requirements for both technical and non-technical staff regarding GenAI. | -Skills gap analysis  -Training need assessment report |
| Deploy and testing of chatbots into website | Create and test chatbot into website. | Testing strategy and test case |
| Final Recommendations | Combine all findings and recommendations into a final report. | Executive summary |

**Reference:**

Adamopoulou, E. and Moussiades, L., 2020. Chatbots: History, technology, and applications. *Machine Learning with applications*, *2*, p.100006.

Ahmad, N. and Alsmadi, I., 2021. Machine learning approaches for IoT security: A systematic literature review. Internet of Things, 14, p.100365

Al Fikri, M., Putra, F.A., Suryanto, Y. and Ramli, K., 2019. Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency. *Procedia Computer Science*, *161*, pp.1206-1215.

Alshamrani, S. Myneni, A. Chowdhary and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851-1877

Alwahedi, F., Aldhaheri, A., Ferrag, M.A., Battah, A. and Tihanyi, N., 2024. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. Internet of Things and Cyber-Physical Systems, 10, p.100016.

ARS STAFF 2016, *Information-Technology*, viewed 22 August 2024, <https://arstechnica.com/information-technology/2016/05/1b-bangladesh-heist-officials-say-swift-technicians-left-bank-vulnerable/>

Asaad, R.R. and Saeed, V.A., 2022. A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. *Applied computing Journal*, pp.227-244.

AustLii, *Viewdb,* viewed 19 August 2024, (<https://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/taaa1979410/>)

Blank, R. and Gallagher, P., 2012. Nist special publication 800-30 revision 1 guide for conducting risk assessments. *National Institute of Standards and Technology*.

Chui, M., Hazan, E., Roberts, R., Singla, A. and Smaje, K., 2023. The economic potential of generative AI.

Dhoni, P. and Kumar, R., 2023. Synergizing generative ai and cybersecurity: Roles of generative ai entities, companies, agencies, and government in enhancing cybersecurity. *Authorea Preprints*.

Dwivedi, Y.K., Hughes, L., Cheung, C.M., Coombs, C., Doyle, R., Dubey, R., Eirug, A., Grover, V., Gupta, B., Gustafsson, A. and Hinsch, C., 2024. Generative AI (GenAI) – Opening Pandora's box: Towards a research agenda focusing on darker sides, challenges, implications and future prospects. International Journal of Information Management, 75, p.102742

Elder, J. & Elder, S. 2019. ‘Faster Disaster Recovery The Business Owner’s Guide to Developing a Business Continuity Plan’. Hoboken, New Jersey, USA. John Wiley & Sons Inc. E-book, viewed 23 August 2024, <https://ebookcentral.proquest.com/lib/xamkebooks/reader.action?docID=5741229&query=Business+Continuity>

Evan and Shimon 2015, *Politics,* viewed 21 August 2024, <https://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html>

Federal Trade Commission 2024, *Enforcement,* viewed 24 August 2024, <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>

Furnell, S. and Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. Computers & Security, 31(8), pp.983-988.

Gallery, C., Retail innovation 2: The future of online selling. In *Fashion Business and Digital Transformation* (pp. 216-254). Routledge.

Granjal, J., Monteiro, E. and Silva, J.S., 2013, May. End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication. In *2013 IFIP Networking Conference* (pp. 1-9). IEEE.

Gupta, M., Akiri, C., Aryal, K., Parker, E. and Praharaj, L., 2023. From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access*.

Gupta, M., Akiri, C., Aryal, K., Parker, E. and Praharaj, L., 2023. From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access*.

Hasal, M., Nowaková, J., Ahmed Saghair, K., Abdulla, H., Snášel, V. and Ogiela, L., 2021. Chatbots: Security, privacy, data protection, and social aspects. *Concurrency and Computation: Practice and Experience*, *33*(19), p.e6426.

Huang, K., Yeoh, J., Wright, S. and Wang, H., 2024. Build your security program for genai. In *Generative AI Security: Theories and Practices* (pp. 99-132). Cham: Springer Nature Switzerland.

Industry, *regulations-and-standards,* viewed 19 August 2024, <https://www.industry.gov.au/regulations-and-standards>.

Katsumata, P., Hemenway, J. and Gavins, W., 2010, October. Cybersecurity risk management. In *2010-MILCOM 2010 Military Communications Conference* (pp. 890-895). IEEE.

Kaur, R., Gabrijelčič, D. and Klobučar, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, p.101804.

Krishnamurthy, O., 2023. Enhancing Cyber Security Enhancement Through Generative AI. *International Journal of Universal Science and Engineering*, *9*, pp.35-50.

Legislation 2024, *Home -Acts,* viewed 19 August 2024,<https://www.legislation.gov.au/C2004A03712/latest/text>

Lucchi, N., 2023. ChatGPT: a case study on copyright challenges for generative artificial intelligence systems. *European Journal of Risk Regulation*, pp.1-23.

Möller, D.P., 2023. NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 231-271). Cham: Springer Nature Switzerland.

OAIC, *consumer-data-right,* viewed 19 August 2024, <https://www.oaic.gov.au/consumer-data-right/consumer-data-right-legislation,-regulation-and-definitions/consumer-data-right-legislation>

OAIC, *Privacy,* viewed 19 August 2024, <https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme>**.**

Rane, N., 2023. Role and challenges of ChatGPT and similar generative artificial intelligence in business management. *Available at SSRN 4603227*.

Safitri, E.H.N. and Kabetta, H., 2023, August. Cyber-Risk Management Planning Using NIST CSF V1. 1, ISO/IEC 27005: 2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization). In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 332-338). IEEE.

Snedaker, S., 2013. *Business continuity and disaster recovery planning for IT professionals*. Newnes, viewed 20 August 2024, <https://books.google.com.au/books?hl=en&lr=&id=vT8TAAAAQBAJ&oi=fnd&pg=PP1&dq=cybersecurity+business+continuity+plan&ots=d2uAj9138-&sig=bu9fbT6qoOioIWEsrnlxEZouoh8#v=onepage&q&f=false>

Thorgersen, S. and Silva, P.I., 2021. *Keycloak-identity and access management for modern applications: harness the power of Keycloak, OpenID Connect, and OAuth 2.0 protocols to secure applications*. Packt Publishing Ltd.

Townsend, R. 2022. *What is a Disaster Recovery Plan and Why is it Important? Nexstor. WWW document. Updated 31 August 2022*, viewed 21 August 2024, <https://nexstor.com/what-is-disaster-recovery-plan/>.

Wang, X., Lin, X. and Shao, B., 2022. How does artificial intelligence create business agility? Evidence from chatbots. *International journal of information management*, *66*, p.102535.