[redacted]

Project title

PROJECT ON A STARTUP NAMED TIGEREX

Software Requirement Engineering

[redacted]

[redacted]

[redacted]

1. PROBLEM DOMAIN

1.1 Background to the Problem

Nowadays internet plays a very vital role. As we are all in lockdown in home for COVID-19, we are doing our almost all necessary jobs in online. We are paying to the stores, making transactions thru bills, communicating thru social apps and much more. However, do we ever think that our data, logs or images in online can be vulnerable, our phones security features can be tempered or our credit cards pin can be cloned? There were many reports in 2020, where there were many cases of online trafficking, online harassment, bullying, online hijacking, cyber-attack in corporate website's firewall and many more. Well, keeping those questions in our mind, we thought of making a versatile platform for ensuring safety in online world. A platform, which can detect as well as prevent the threats in online world around us. That is how Tigerex is made. Our main priority is to ensure our clients safety in online world. With the help of machine learning and deep AI, we will secure users sensitive credentials like browser cookies, trackers, left overs, pins and passwords and many more.

1.2 Solution to the Problem

Tigerex is introduced to eliminate threats in our online world. It uses user's data and scans if there remains any odd leftovers like additional bits, trackers etc. Then it checks them with its updated threat database and if finds any security breaches then it blocks them and sends notification to the user. It has multiple layers of encryption, which makes user's plain data nearly impossible to be accessible to the hackers and spammers. Thus how Tigerex is made appropriate for the users. Tigerex is available for various OS and versions also. Tigerex uses simple User Interface (UI), which makes it more user friendly. With 24/7 bot assisted customer service, users can easily claim their service according to their need. Cost of our service is also feasible. Users can pay their connection cost monthly with 0% interest for first 3 months. They can earn some bonus points for their usage as well as for some festivals also. In a whole to say, it serves users purpose according to the users demand.

2. SOLUTION DESCRIPTION

2.1 System Features

Functional requirements

Business requirements: The ultimate goal of this project is to give proper safety to the users against cyber-attacks and protect their private info. So that they can surf the internet with ease.

Administrative functions: The system will monitor the user's device. With the data stored in the cloud, the AI will use advance machine learning to detect and predict possible threats Or attacks. It will update firmware and software definitions likewise.

User requirements: If the user is surfing the internet, then all they need to do is keep our software active. The system will do rest of the jobs for them.

System requirements: For the software to run, the user needs to have desktop/laptop with an operating system (Windows/Linux/Mac OS) and for handhold devices it needs to be android/iOS. User will of course need a proper internet connection.

Non-Functional requirements

Reliability: Reliability is a top priority for a system. User can be assured to use it anytime as it will give 24/7 service. If they fall into any problem or not sure about something, they can use feedback from the support team.

Performance: System will maintain a standard quality of performance with proper response time/reaction.

Usability: The software will be easy to use with user a friendly interface to make the user feel easier to understand.

Supportability: Will have support across all platforms.

Scalability: As the user base grows, there will be more data to analyze for the system. But still the system will have enough resources to handle that computation.

2.2 UML Diagram

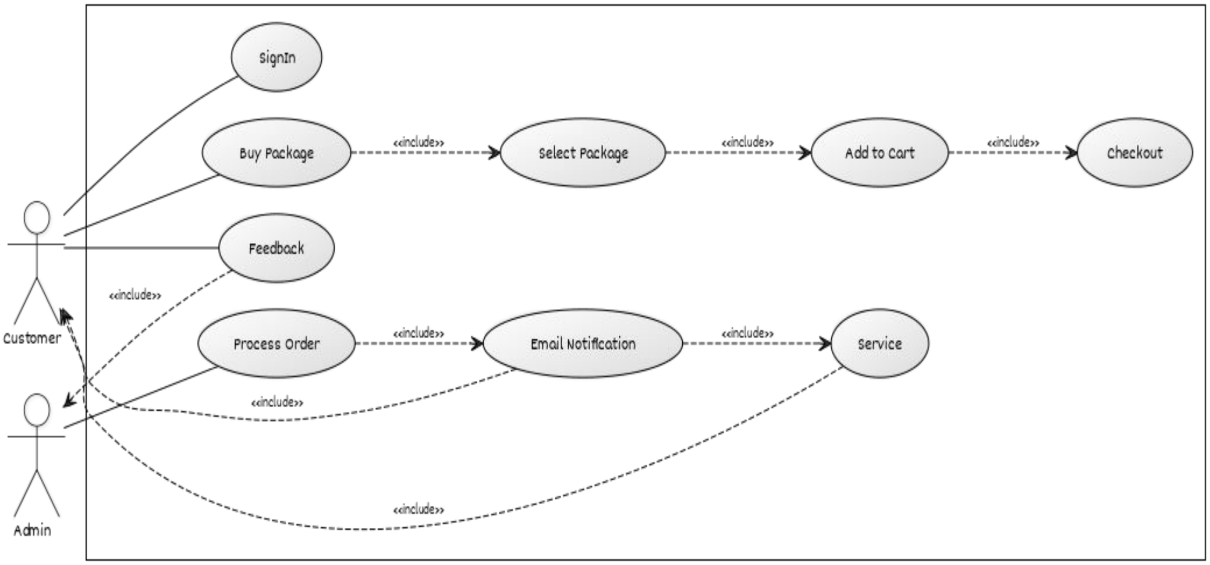

Figure-1: Use case diagram of basic functionality of the system.

3. Social Impact

It was surprised to hear that people do not see cybersecurity as an industry focused on social impact. Perhaps all the us with privilege should consider more closely the impact technology has on the lives the others. The Internet has been the most democratizing force on the globe since electrification – and previously the printed word. More than half the globe is connected. Nearly all the the world's economy relies on the Internet. And all sectors the our lives interface with it for all people. At the same time, a disturbingly large portion the our world lives in poverty. Even more the the world lives right around the boarder the the poverty line. This is an economic problem and now a security problem for the globe. Identity theft, fraud, and the full monetization the the individual is at devastating risk. People, their information, their digital personas, and their secrets are the targets. When we think the hacking, we tend to believe that this is a problem that only affects the rich. To put it another way, those with agency are the targets. After all, they are the best targets they have the money.

While on the face the it that may seem true, those with agency are protected by the institutions that serve them. Fraud prevention services, credit monitoring, insurance these institutions and many more are inherently integrated into the lives the those with agency. Other important functions are for sale and can be afforded by those with the means to purchase. But those without agency operate their lives without the protection the those institutions and services. This puts them into jeopardy. I can understand why many may not associate social impact with cybersecurity. It isn't obvious. And it may not even be the motivation the many who work in the field. But that does not mean that the outcome isn't real. It doesn't mean that our work does not directly impact the safety and security the a connected society.

For years, technology policy advocates have worked on addressing the digital divide that is the gap between those with access to quality internet and those without. Yet, security never seems to find its way into the conversation. But access to the internet alone is not the only important factor. Cybersecurity is critical especially for those on the margins the society who may never recover from an attack.

As security practitioners, researchers, entrepreneurs and investors, we need to change the conversation. Cybersecurity is not a luxury good. It isn't just something for the wealthy to access. If we treat it that way intentionally or not we run the risk the putting already vulnerable classes the people in real peril. We also run the risk the damaging the virtue the Internet and a connected society.

We need to move the conversation forward. Cybersecurity leaders in industry, government, and investment capital have to start elevating the human impact the our work. This isn't because we need to look cool at dinner parties – it is because we believe in a free and safe society for everyone – everywhere.

4. Development Plan

1. Secure internal network and cloud services

Company's network should be separated from the public Internet by strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies. Additional monitoring and security solutions, such as anti-virus software and intrusion detection systems, should also be employed to identify and stop malicious code or unauthorized access attempts. Internal network After identifying the boundary points on company's network, each boundary should be evaluated to determine what types the security controls are necessary and how they can be best deployed. Border routers should be configured to only route traffic to and from company's public IP addresses, firewalls should be deployed to restrict traffic only to and from the minimum set the necessary services, and intrusion prevention systems should be configured to monitor for suspicious activity crossing the network perimeter. In order to prevent bottlenecks, all security systems have deploy to the company's network perimeter should be capable of handling the bandwidth that provides. Cloud based services Carefully consult the terms of service with all cloud service providers to ensure that the company's information and activities are protected with the same degree of security would intend to provide by own. Request security and auditing from the cloud service providers as applicable to the company's needs and concerns. Review and understand service level agreements, or SLAs, for system restoration and reconstitution time. It should also inquire about additional services a cloud service can provide. The services may include backup and restore services and encryption services, which may be very attractive to small businesses.

2. Develop strong password policies

Generally speaking, two-factor authentication methods, which require two types of evidence that It are who It claim to be, are safer than using just static passwords for authentication. One common example is a personal security token that displays changing passcodes to be used in conjunction with an established password. However, two-factor systems may not always be possible or practical for the company. Password policies should encourage the employees to employ the strongest passwords possible without creating the need or temptation to reuse passwords or write them down. That means passwords that are random, complex and long (at least 10 characters), that are changed regularly, and that are closely guarded by those who know them.

3. Secure and encrypt the company's Wi-Fi

Wireless access control

The company may choose to operate a Wireless Local Area Network (WLAN) for the use of customers, guests and visitors. If so, it is important that such a WLAN be kept separate from the main company network so that traffic from the public network cannot traverse the company's internal systems at any point.

Internal, non-public WLAN access should be restricted to specific devices and specific users to the greatest extent possible while meeting the company's business needs. Where the internal WLAN has less stringent access controls than the company's wired network, dual connections where a device is able to connect to both the wireless and wired networks simultaneously should be prohibited by technical controls on each such capable device .All users should be given unique credentials with preset expiration dates to use when accessing the internal WLAN.

Wireless encryption

Due to demonstrable security flaws known to exist in older forms of wireless encryption, the company's internal WLAN should only employ Wi-Fi Protected Access 2 (WPA2) encryption.

4. Encrypt sensitive company data

Encryption should be employed to protect any data that the company considers sensitive, in addition to meeting applicable regulatory requirements on information safeguarding. Different encryption schemes are appropriate under different circumstances. However, applications that comply with the Open PGP standard, such as PGP and Gnu PG, provide a wide range of options for securing data on disk as well as in transit. If It choose to offer secure transactions via the company's website, consult with the service provider about available options for an SSL certificate for the site.

5. Regularly update all applications

All systems and software, including networking equipment, should be updated in a timely fashion as patches and firmware upgrades become available. Use automatic updating services whenever possible, especially for security systems such as anti-malware applications, web filtering tools and intrusion prevention systems.

6. Set safe web browsing rules

The company's internal network should only be able to access those services and resources on the Internet that are essential to the business and the needs of the employees. Use the safe browsing features included with modern web browsing software and a web proxy to ensure that malicious or unauthorized sites cannot be accessed from the internal network.

7. If remote access is enabled, make sure it is secure

If the company needs to provide remote access to the company's internal network over the Internet, one popular and secure option is to employ a secure Virtual Private Network (VPN) system accompanied by strong two-factor authentication, using either hardware or software tokens.

8. Create Safe-Use Flash Drive Policy

Ensure employees never put any unknown flash drive or USBs into their computer. As the U.S. Chamber's Internet Security Essentials for Business 2.0 states, small businesses should set a policy so that employees know they should never open a file from a flash drive they are not familiar with and should hold down the Shift key when inserting the flash drive to block malware.

5. Marketing Plan

Tigerex is mainly a complete cybersecurity solution for web, desktop, mobile phones and for every handheld devices. It works like a web that monitors the target devices and keeps them protected. As the number of internet users are increasing day by day, thus the necessity of a cybersecurity solution is also increasing. Our first priority is to ensure safety for the targeted users to avoid any kind of threats. Users can easily use our system and services worldwide to keep themselves safe. Users' credentials, biometric info and many critical data are secured thru our products and services. Tigerex wishes to reach as many countries as possible thru its latest cloud technology. It uses AI to store threat data's and then uses those data's to block the threats also. With machine learning it analyses the threat metrics and updates firmware and software definitions automatically. Costs of the products and services are so liberal to make the users feel at ease. With 0% interest for first 7 months, Tigerex also comes affordable when you don't want to pay full at once. So, what are you waiting for? Grab your desired package now and keep you and your data safe from unwanted breaches. We may hire a professional marketer to promote our portal. Social media is an integral part of any marketing strategy. Therefore we can use social media to promote our portal. Facebook can be used, where promotion can be done by making groups. This way of promotions cost effective than hiring a professional since we have to pay them in order to promote our software. So, this can be a long term and a continuous plan for promotion of our software and promotion of our software by a professional can be a short term plan since it is costly.

6. Cost and Profit Analysis

Below we have provided the cost and profit analysis.

Development Cost

Cost	2020	2021	2022	2023	Total
Software	700000				700000

Training		7000	7000	7000	21000
Software Licence	25000				25000
Data Reservation Cost	10000				10000
Marketing Cost	10000	7000	5000	2000	24000
Total Development					780000

Cost saving

Computer Cost Decreases		80000	90000	95000	265000
Labour cost decrease		6000	6200	6600	18800
Conference Reservation Increased		150000	178000	190000	518000
Non-Conference Reservation Increased		160000	180000	191000	531000
Total cost saving					1332800

Final Profit (Total saving cost – Total development cost) = 552800.

Here, Total development cost is 780000 and the total amount of cost that is saved is 1332800, giving us a profit of 552800.

.

The End