Cybersecurity Chatbot: SICI

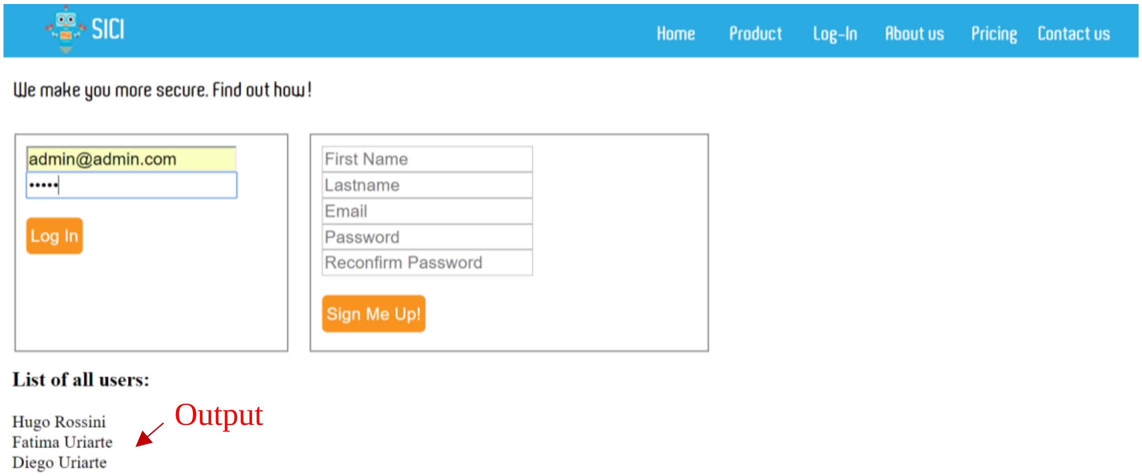
1. Summary

The adoption of smart cities is on the rise, increasing the potentially vulnerable attack surface area for cybersecurity threats. Latin America is rapidly becoming one of the biggest consumers of the smart city model. We have identified that there is a gap in the Latin American market-cybersecurity concerns are not being sufficiently addressed thus putting residents at risk. Our cybersecurity chatbot (SICI): *Solución Innovadora para Ciudades Inteligentes*/*Innovative Solution for Smart Cities*, is a potential solution to vulnerability that will empower smart city residents with information about cybersecurity threats. By using existing machine learning techniques and platforms, our product's main functionality would seek to inform users of: (i) security threats to their accounts; (ii) major cybersecurity attacks that may impact them; and (iii) provide answers to questions regarding cybersecurity. We believe that our chatbot is an innovative step forward towards the development of effective responses to assist in preventing, identifying, and responding to cyber threats.

2. Web Development

Userid/password for admin login:

User: admin@admin.com Password: 12345



We make you more secure. Find out how!

admin@admin.com

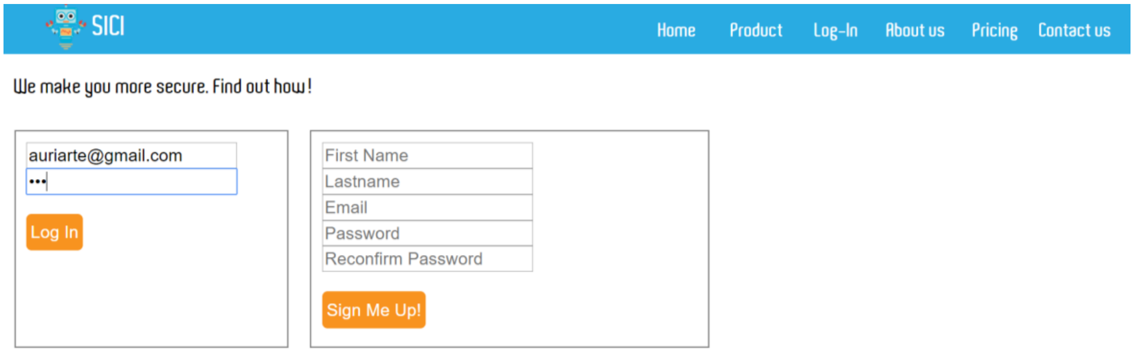
•••••

List of all users:

Hugo Rossini
Fatima Uriarte
Diego Uriarte

Output

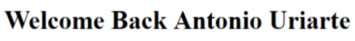
Userid/password for regular user login:



We make you more secure. Find out how!

auriarte@gmail.com

•••

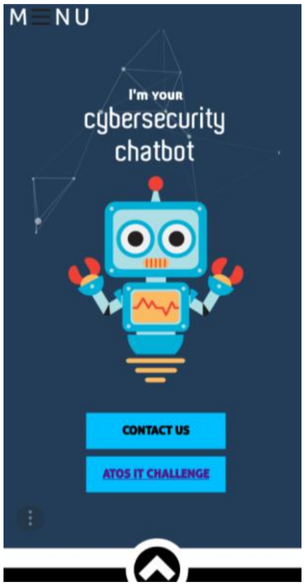


Welcome Back Antonio Uriarte

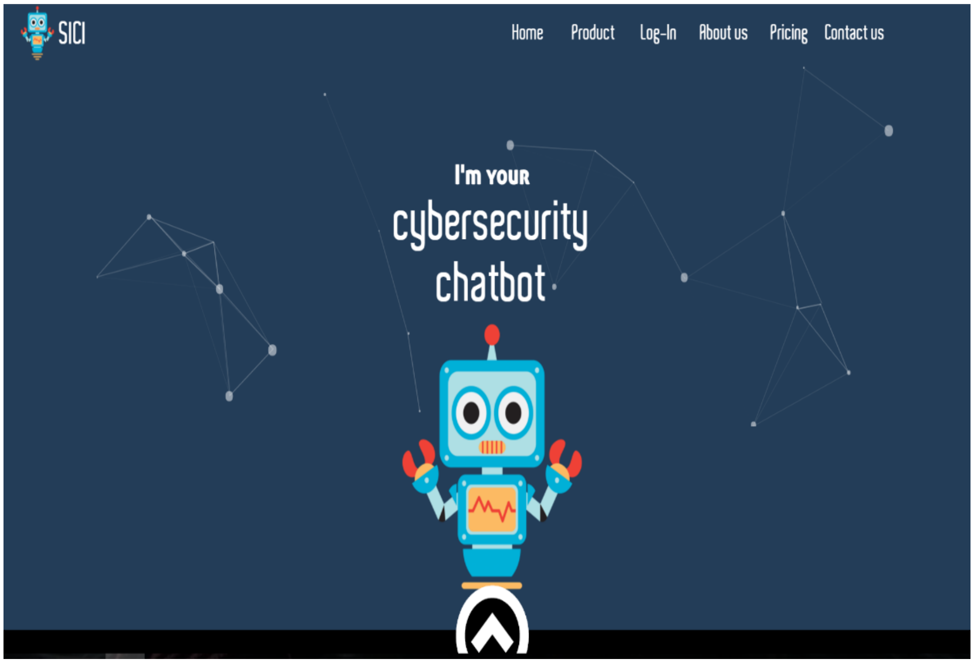
Output

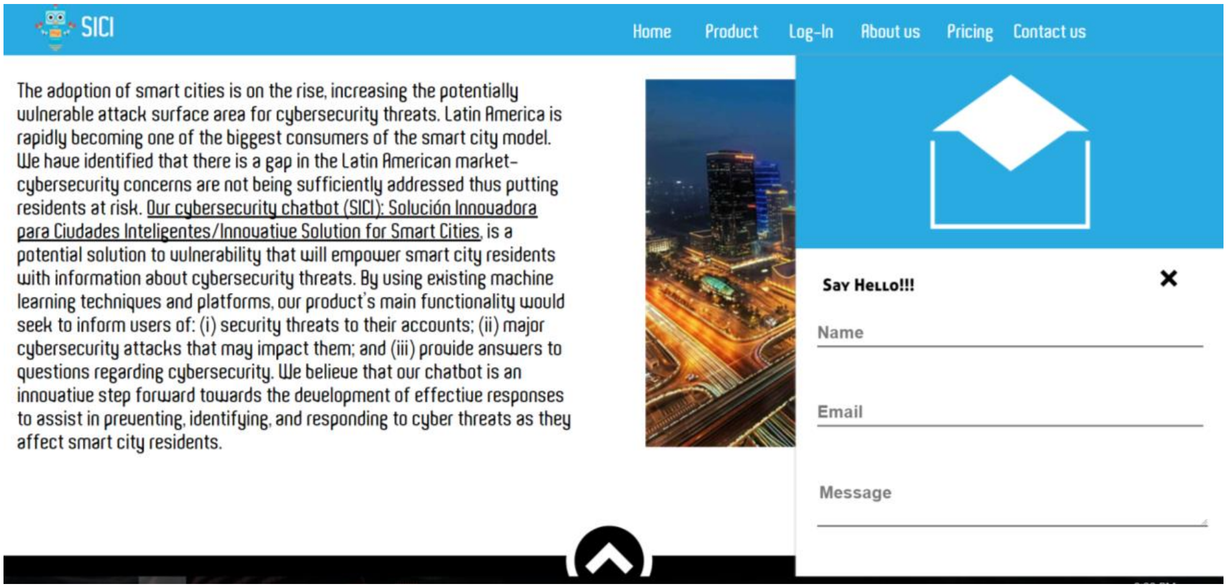
Domain: http://www.sicichatbot.info/
(Since Homework 2 has not been graded already, I'm adding a folder "Final Project" that contains SICI website) IP address: 54.243.23.136

Cellphone | **Personal Computer**



Responsive Design and Mobile First





The adoption of smart cities is on the rise, increasing the potentially vulnerable attack surface for cybersecurity threats. Latin America is rapidly becoming one of the biggest consumers of the smart city model. We have identified that there is a gap in the Latin American market-cybersecurity concerns are not being sufficiently addressed thus putting residents at risk. Our cybersecurity chatbot (SICI): Solución Innovadora para Ciudades Inteligentes/Innovative Solution for Smart Cities, is a potential solution to vulnerability that will empower smart city residents with information about cybersecurity threats. By using existing machine learning techniques and platforms, our product's main functionality would seek to inform users of: (i) security threats to their accounts; (ii) major cybersecurity attacks that may impact them; and (iii) provide answers to questions regarding cybersecurity. We believe that our chatbot is an innovative step forward towards the development of effective responses to assist in preventing, identifying, and responding to cyber threats as they affect smart city residents.

3. Description: Minimum Viable Product

As the push for smart city development and adoption continues, we have observed that much emphasis has been placed on the benefits, with a much lesser emphasis placed on the security risks. Smart cities, in particular, have been championed as a cost-effective solution for providing public services in areas that previously experienced difficulties in providing those services. Latin America is a prime example of an area where the smart city model is rapidly growing, but at the expense of overlooking the security risks affiliated with Internet of Things (IoT) devices and increasingly interconnected networks.

Our product seeks to provide smart city users, particularly citizens, with the knowledge and tools necessary to secure themselves and to understand the all possible implications of new technological adoptions. By leveraging existing machine learning techniques and platforms, our product's main functionality would seek to inform users of:

1. Security threats to their accounts;
2. Major cybersecurity attacks that may impact them; and,
3. Provide answers to questions regarding cybersecurity.

While scoping the feasibility of our product, we have determined that there exists a number of open-source frameworks and datasets that we will leverage in the development phase to design a chatbot that functions to provide alerts, educate and answer user questions, and monitor security risks.

To train our chatbot in cybersecurity, we will utilize open-source threat intelligence feeds. These available repositories will allow us to develop an initial chatbot that can answer basic user questions about cybersecurity as well as detect common security threats. There currently exists chatbots that alert users, such as Twilio and Dropbox's Securitybot, that we will investigate to aid the development of our alert functionality. Our intention is that through use of our product and discussions with stakeholders in our target area, Latin America, we will gain access to more datasets, which will enable customization of the chatbot monitoring and alert system to users by their specific location.

Technical Feasibility

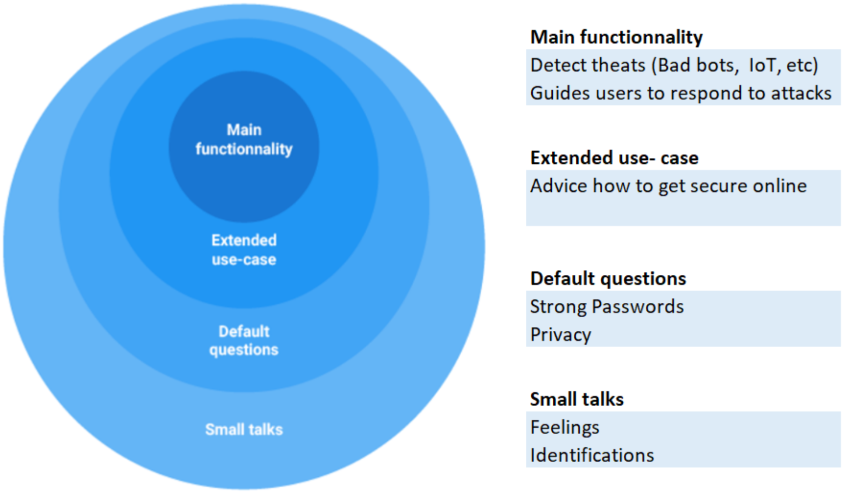
There are a number of potential open-source frameworks such as IBM Watson Bluemix that provides the tools for constructing chatbots that can be deployed to instant messaging clients such as FB messenger, Skype, Slack. Although, we haven't found any powerful open source framework that can be used for language recognition, there are some frameworks like LUIS by Microsoft, or IBM Watson that offer free usage tiers. For initial development, we plan to use evaluate and use these sources in the development phase to design and train our chatbot.

There are a number of potential open-source threat intelligence feeds and trackers on GitHub such as Malware Domain and Ransomware Tracker List. To start, we will use machine learning techniques to train our chatbot to monitor and detect cybersecurity threats since it is basically a binary classification problem. For instance, Abeshu and Chilamkurti (2017) used deep learning based IoT network for attack detection in the cyberspace and found that it can be a resilient mechanism to small mutations or novel attacks because of its high-level feature extraction capability. They showed a successful adoption of artificial intelligence to cybersecurity, and designed and implemented the system for attack detection in distributed architecture of IoT applications such as smart cities. We would like to follow their path in detecting cybersecurity threats while also comparing models using different machine learning algorithms such as support vector machine, decision trees, neural networks, deep learning, among others. This will teach our chatbot about an array of cybersecurity threats. We will also give our chatbot an alerts functionality to let the user know when it detects something, based on what its learning. By doing that, we will implement our first and second functionality: identifying security threats and alerting the user of cybersecurity attacks.

Additionally, we plan to add the functionality of providing answers to questions regarding cybersecurity by leverage neuro-linguistic programming techniques. We believe that retrieval based models could be a good option for our chatbot since they have a repository of predefined responses they can use. Also, our chatbot will use machine learning algorithms to learn and answer customer queries continuously. Through further research and interviewing cybersecurity experts, we will seek to anticipate user questions to further train our chatbot to respond to cybersecurity specific questions.

Our bot functionalities are the following:

Bot Functionalities



Main functionnality
Detect theats (Bad bots, IoT, etc)
Guides users to respond to attacks

Extended use- case
Advice how to get secure online

Default questions
Strong Passwords
Privacy

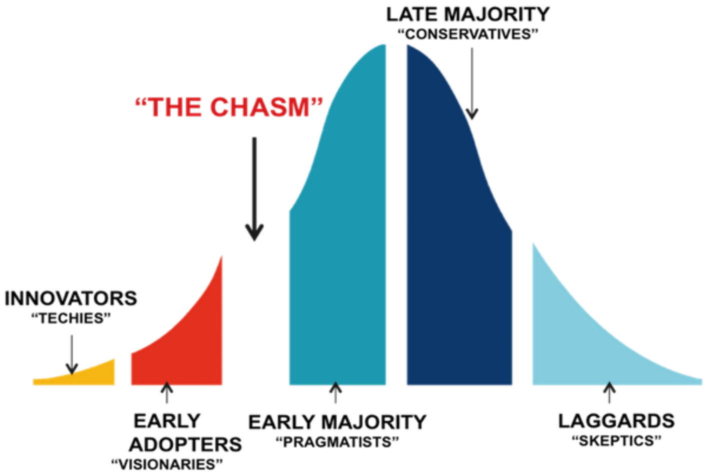
Small talks
Feelings
Identifications

4. Costumer Segment

As the use of IoT expands Internet connectivity to a much wider scale, new threats will become more obvious as heterogeneous technologies are connected together, introducing a higher degree of risk. As mentioned before our target customer is typified by citizens of smart cities mainly in Latin-America who want to utilize IoT devices (such as TVs, webcams, home thermostats, remote power outlets), but are worried about their security and privacy (early and late majority in Technology Adoption Curve).

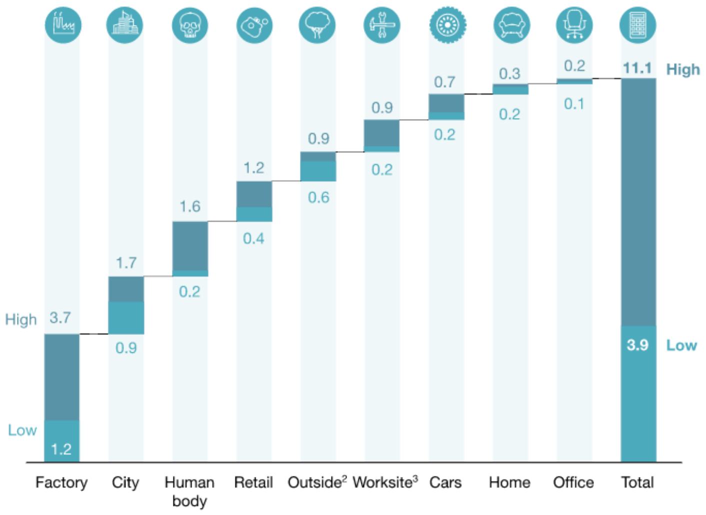
Our target customer can be categorized as those that fall within the “chasm” to “late majority” category on the technology adoption curve. This customer waits and observes the impact to early adopters before they try new technology. Early adopters are those in their mid to late twenties who are willing to innovate to protect their security and privacy.

Technology Adoption Curve



The potential market size of our target customer niche is associated with the development of smart cities and smart devices. According to Mckinsey, consumers own an average of four IoT devices that communicate with the cloud and that 127 new devices connect to the Internet every second. McKinsey also estimates that the IoT could have an annual economic impact of $3.9 trillion to $11.1 trillion by 2025 across many different areas, including factories and cities. Furthermore, by 2020, Gartner predicts that there will be over 26 billion Internet of Things devices in use.

Potential Economic Impact by Segment
(2015 billion dollars)



Source: McKinsey

With the establishment of smart cities and the adoption of smart devices, there are some risks associated with our customer niche. These risks include: (i) speed of change and digital agenda, and a (ii) low consideration for cybersecurity hygiene and practices. In relation to the first risk we believe that smart city adoption is a clear trend. Particularly in Latin-America, the smart city market is expected to grow 19.4% per year, reaching US$758bn by 2020, according to consultancy firm Markets & Market. Currently, there are 8 smart cities in Santiago, Ciudad de México, Bogota, Buenos Aires, Rio de Janeiro, Curitiba, Medellin, and Montevideo. In order to mitigate the risk of the lack of culture of cybersecurity, we plan to use partnerships with governments and to develop a powerful marketing strategy using some insights of behavioral economics to attract users and change their behavior and opinions about the importance of cybersecurity.

As systems and devices associated with the IoT become more widely utilized, IoT-related cybersecurity and privacy issues will affect large numbers of households and communities. Our ecosystem involves different stakeholders: members of the public, organizations, institutions, government, universities, experts, research centers, etc. To assess their needs, we would like to interview crucial stakeholders for the product development phase.

Benefits for end users

For end users, our product will help them secure their private data more easily. Specifically, we prevent data from being leaked and misused by a third party.

When citizens interact with IoT devices and chatbots, personal data is also generated. In fact, such data reveals every aspect of the user’s life, including but not limited to personal residence, contacts, consumption habits, and personal identity. For example, when you ask Siri about the latest movie and the nearest movie theater nearby, data concerning your home address, your movie preference, and your daily plan is likely to be recorded and exposed.

In this sense, our product will monitor the environment when users are interacting with IoT devices and chatbots and send alerts to notify them of the possible attacks and risks. However, unlike the traditional pop-up windows and security alerts, which are often ignored by the users, our talking chatbot will catch user attention and answer their subsequent security questions. During such interaction, users can gain more information about possible attacks and make more informed decisions in permitting or denying data access to the other party.

5. Feedback of Value Proposition and Web Application

User 1: Gabriel Zamudio
Notes: Very well researched concept and idea, which considers a real issue of smart cities. Having in mind that we had the topic of "the right to be forgotten" in one of the earlier episodes of the IT Challenge you very well connect two topics which are at the heart of our digitalized society. The web application looks really good! Very impressive for a beginner in web development.

User 2: Javier Ponce
Notes: A nicely defined scope, not too ambitious but of immense value, with a clear need and a bit of a gap in the market. What are you doing for the Challenge prototype? A very interesting use case which especially in regard to increasing numbers of IoT devices is expected to have quite a customer base. On the other hand, it is not fully clear how the data processed by the AI will keep pace with the myriads of additional security threats showing up every day - both in sense of speed/time-to-market as well as on data size due to the vast number of possible attack vectors. In addition, how the various new IoT devices (and the threats coming with them) will be integrated into the solution quickly enough - we recommend making this part of your message a little bit more bold to increase confidence in the feasibility of your idea.

User 3: Cate Wang
Notes: Very complete set of information with all expected topics covered in detail - very much appreciated and impressive! The idea and benefit for both end users and business partners is clearly explained; so are the architectural overview, the business- and the project plan.