SURYA ENGINEERING COLLEGE,ERODE
Approved by AICTE,New Delhi & Affiliated to Anna University,Chennai)
Erode-Perundurai Highway Mettukadai,Erode-638107.
Ph.0424-2555018 Mobile No:9842511455 Email:secerode@gmail.com

NAAN MUDHALVAN IBM PROJECT

PROJECT TITLE

CHATBOT DEPLOYMENT WITH IBM CLOUD WATSON ASSISTANT

TEAM MEMBERS

- C.PRAVEEN
- M.MANIRATHNAM
- K.MANORANJITH
- J.SUNILKUMAR
- P.SANJAY

ABSTRACT :

ChatBot can be described as software that can chat with people using artificial intelligence. These software are used to perform tasks such as quickly responding to users, informing them, helping to purchase products and providing better service to customers. In this paper, we present the general working principle and the basic concepts of artificial intelligence based chatbots and related concepts as well as their applications in various sectors such as telecommunication, banking, health, customer call centers and e-commerce. Additionally, the results of an example chabbot for donation service developed for telecommunication service provider are presented using the proposed architecture.

I INTRODUCTION :

Chatbots have been touted as the 'Next Interaction Layer', which implies that the way we currently consume information by interacting with websites/apps will in many cases be replaced by chatbots (conversations). Chatbot platforms continue to thrive despite some initial backlash, and their adoption has actually accelerated as a result of the COVID-19 pandemic [1].

Chatbot research has mostly focused on improving the underlying Natural Language Processing (NLP) precision [2], [3], such that chatbots are more proficient in understanding and responding to user queries. With chatbots gaining traction and their adoption growing in different verticals, e.g. Health, Banking, Dating, etc., and users sharing more and more private information with chatbots; studies have started to highlight the privacy risks of chatbots [4]-[6].

, e.g. storage encryption and multi-factor authentication. While security basics are definitely needed, the more ad- vanced and implicit privacy risks of open-ended queries posed by users have not been addressed in literature.

II PRIVACY PRESERVING CHATS:

1. Chatbot Basics

In an ideal world, given a user query in natural language, a bot would respond as follows:

1) Understand the user's intent;

2) Retrieve the relevant content from its Knowledge base (KB):

3) Synthesize the answer and respond to the user (again, in natural language);

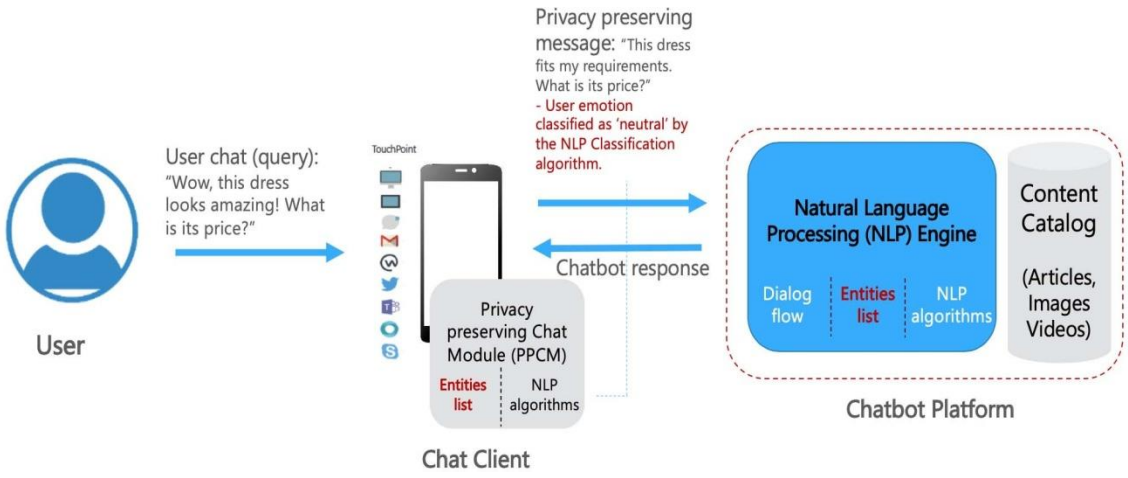
4) Retain the conversation context to answer any follow-up questions by the user

Unfortunately, numerous technical limitations prevent us from enabling the above workflow. Enterprise chat- bots today (eg, the ones based on IBM Watson As- sistent, AWS Lex, Microsoft LUIS, Google Dialogflow) first need to be trained by providing a set of questions, question variations, and their corresponding answers. The questions can be grouped into intents Question variations, referred to as utterances in hot terminology. refer to sample variations in which the same question can be posed by end-users. The iden is to provide sto 10 such utterances (for each question) as input, based on which the bat will hopefully be able understand 50 different variations of the question. Most bot engines perform intent matching and sentiment analysis using a mix of statistical (eg tdf, Bag-of-Words) and Deep Learning (eg, Transformer) techniques.

the chatbot returns a fallback answer. For all others, the engine returns the corresponding confidence level along with the response.

III ENTITY BASED PRIVACY PRESERVATION

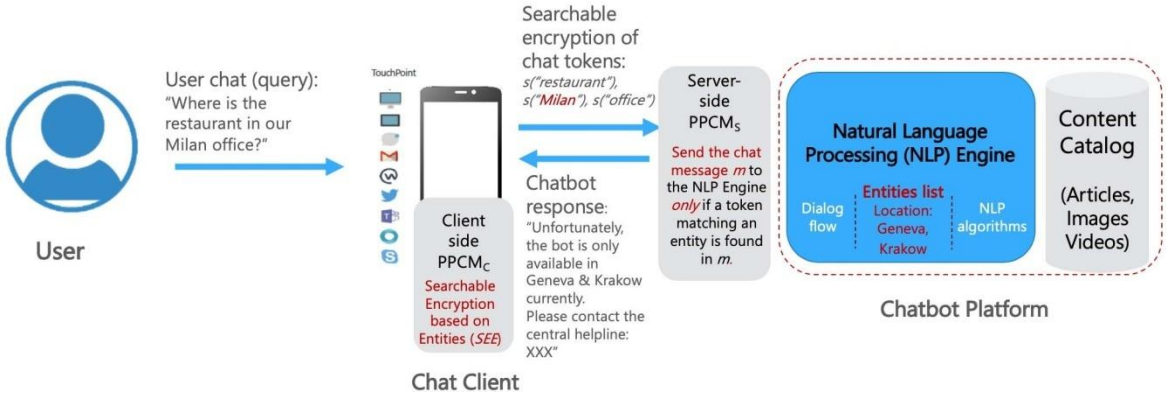
In this section, we outline the entity based privacy preservation approach. Together with 'intents' and 'ut- terances, an essential part in customizing chatbots is to provide 'entities [8]. Entities refer to the domain specific vocabulary, e.g. they can refer to the office locations. in the context of the HR Bot outlined in Use-case 2; and can be used to customize the chatbot responses according to user (query) location. The entities based approach is applied on the client/app side by a module referred to as the Privacy Preserving Chat Module (PPCM). The PPCM design is dependent on knowledge of the original chatbot content and the underlying NLP techniques used by the chatbot platform. For instance, with reference to Use-case 2, the PPCM needs to be aware of the entities list used in the original chatbot design (allowed office locations), such that it can apply the necessary privacy preserving measure(s) accordingly



PPCM Architecture Highlighting Entity Based Privacy Preservation

IV VALIDATION :

We validated the proposed entity based privacy preservation approaches on a Help Desk chatbot avail- able for employees in our Geneva and Krakow offices. The chatbot was developed on IBM Watson Assistant. and has around 400 intents covering a range of topics related to office equipment, transportation, restaurants, leisure, etc. facilities. The chatbot has been live for more than 6 months now and we noticed that the chatbot is equally popular among new employees, employees on short term assignment, and regular employees based in Geneva and Krakow giving us a test audience of around 5000 unique users. We report some observations based on analyzing the first 10000 posed queries. The results validated our hypothesis that many employees still talk to a chatbot as they would to a human being. Rather than asking direct questions, they start their queries by providing some context first. Below are a few sample queries (edited to remove company specific info)



Distributed PPCM Highlighting Entity Based Search Encryption

V CONCLUSION :

We outlined two approaches in this paper to perform privacy preserving conversations based on (chat) entities which approach to apply depends on the transparency of the chatbot design and implementation architecture (client/app side only vs. distributed deployment). We hope that the proposed approaches will lead to increased enterprise adoption of chatbots, by addressing the grow- ing issue of privacy risks in chatbots.

CHATBOT MERITS:

- 24*7 Availability
- Reduce Errors
- Reduces Operational Costs
- Increase Sales and Engagement
- Lead Genaration

CHATBOT DEMERITS:

- NeedsUnderstanding of Natural Language
- High Misunderstanding
- Not Satisfied Angry Customer
- Inability to Handle Complex Issues