SLA AS A MECHANISM TO MANAGE RISKS RELATED TO CHATBOT SERVICES

Co-authored by Krishna Gondaliya

Sergey Butakov

Pavol Zavarsky

Project report

Submitted to the Faculty of Graduate Studies,

Concordia University of Edmonton

in Partial Fulfillment of the

Requirements for the

Final Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

April 2020

SLA AS A MECHANISM TO MANAGE RISKS RELATED TO CHATBOT SERVICES

Krishna Gondaliya

Approved:

Sergey Butakov [Original Approval on File]

Sergey Butakov Date: April 6, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci Date: April 17, 2020

Dean, Faculty of Graduate Studies

SLA as a mechanism to manage risks related to chatbot services.

Krishna Gondaliya
Information Systems Security Management
Concordia University of Edmonton
Edmonton AB, Canada
kgondali@student.concordia.ab. ca

Sergey Butakov
Information Systems Security And Assurance Management
Concordia University of Edmonton
Edmonton AB, Canada
sergey.butakov@concordia.ab. ca

Pavol Zavarsky
Information Systems Security And Assurance Management
Concordia University of Edmonton
Edmonton AB, Canada
pavol.zavarsky@concordia.ab .ca

***Abstract*— Intelligent Chatbot services become one of the mainstream applications in user help and many other areas. Apart from bringing numerous benefits to users these services may bring additional risks to the companies that employ them. The study starts with the review of the scale of chatbot industry and common use cases by focusing on their applications & industry tendencies. Review of functionality and architecture of typical chatbot services shows the potential risks associated with chatbots. Analysis of such risks in the paper helped to build a checklist that security managers can use to assess risks prior to chatbot implementation. The proposed checklist was tested by reviewing a number of Service Level Agreements (SLA) of real chatbot providers.**

Keywords*— *Chatbot, SLA, Privacy, Information Security, Risk, Framework, Artificial Intelligence.

I. INTRODUCTION

Intelligent chatbot services have made their way to the mainstream of web-based user services and they are here to stay. Some obvious evolutionary steps – like audio- or video-chatbots are yet to be mainstream, but they are already being tested. Regardless of the communication means this technology is coming with significant benefits but can also bring additional IT related risks to the companies that are using them. The research below aims to study these risks associated with chatbot services and to look for a set of managerial control mechanisms to address some of the most common threats and vulnerabilities. The main question to answer will be how potential users can effectively evaluate and select the best suitable chatbot service providers from the risk management prospective.

Chatbots have become popular due to the widespread use of messaging services and the advancements of natural language understanding. Every month more than 3 billion people use chatbots directly or indirectly [1]. Advancements in computer architecture and Machine Learning (ML) allow scalable and accurate learning from very large training datasets. Businesses have been investing in chatbot technology to ensure competitive advantage by improving customer service and decreasing costs by 40% [1] [2]. A chatbot is an artificial intelligence (AI) software that can replicate human-like conversation, with a user in natural language through informing applications, websites, mobile apps or phone [3]. The importance of the chatbots is regularly portrayed as one of the most developed and promising articulations of connection between people and machines. Nonetheless, from an innovative perspective, a chatbot just speaks to the normal development of a Question Answering framework utilizing Natural Language Processing (NLP). Formulating responses to questions in natural language is one of the most typical NLP applied in various enterprises' user applications [3].

II. REVIEW OF RELATED WORKS

Customer service chats and industrial social media platforms are progressively managed by intelligent agents, many of which have been developed with human identities and even personalities. Even though the technology itself is not new, reliable linguistic functionality, availability through Software as a Service (SaaS), and the addition of intelligence through machine learning has increased its popularity. Between 2007 and 2015, chatbots were participating in a third to a half of all online interactions and the rate at which new chatbots are being deployed has increased since then. NLP helps chatbots to organize and structure information to perform tasks like interpretation, summarization, named element acknowledgment, relationship extraction, topic segmentation, etc. [4].

An NLP gives capability of natural language to computer and allows communication to happen between user-to computer or human-to-machine and computer-to- computer or machine-to-machine using human natural languages. There are three analyses to understand natural language i.e. parsing, semantic interpretation, and knowledge-based structures. The memory of a chatbot - its Database - consists of an organized, manually created list of suitable replies given for possible questions that may come up from the user's end. A vast range of questions has to be covered by an efficient chatbot and it should also have more than one answer to the same kind of question to avoid redundancy of replies [3]. Each reply should be semantically connected in the conversation to the history of conversation and context of the questions. However, confidentiality and of privacy might be compromise during the communication. There are many layers of data protection available for chatbot services and companies that employ chatbots. These layers include technical protection of the network and system level as well as managerial mechanisms such as policies and Service Level Agreements (SLA). SLA defines various aspects of the service – quality, availability, responsibilities, etc. – as agreed between the service provider and the service user. This research aims to bind security in the SLA as a measurable and agreeable parameter between intelligent bot service provider and the chatbot service subscriber.

A. Overview

The chatbot market is observing a quick development rate because of utilization of versatile informing applications, has empowered the advancement of an intuitive stage to fabricate solid relations with the clients, activating business

sector development and triggering market growth. The rising penetration of AI technology for developing user-friendly decision support systems also supports market growth and development. The innovation is broadly utilized in language interpretation, data analysis, and learning securing applications, making it an ideal combination for the advancement of chatbot arrangements [3].

In 2017 many companies have seen many customer service leaders use chatbots with customer and internally. The Travel, Hospitality and Finance Services Industries have been at the forefront, with companies such as American Express and the Dutch Airlines KLM among the first to launch the chatbots for customer services. A leading Swedish bank piloted a Digital agent chatbot in its internal IT functions conducting over 4000 conversation with 700 employees to resolve issues and challenges related to chatbots to serve better to their retail customers [5]. These examples show growing adoption of intelligent chatbot services and this tendency will obviously continue in the future. Chatbots are widely used, and they are expected to save companies up to $11 billion by 2023, according to a Juniper estimate [6].

B. *Scale of the chatbot industry*

A chatbot can be useful in providing services in a variety of scenarios. These services may even include life-saving health messages, it may also include weather forecast or to purchase a new laptop, smartphone, and anything else in between. Many of the big organizations are spending good amount of energy and money for research on personal assistants.

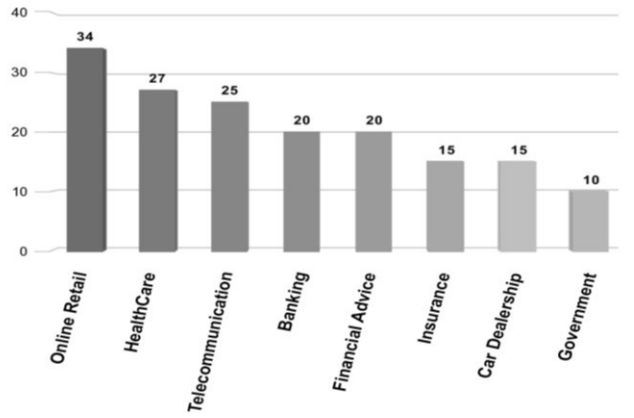

Fig 1: Percent of respondents by chatbot in 2017. (Adopted from [7])

Chatbots has become a preferred option in the popular sector to describe the essentials of an organization or solving queries owing to the fact that every time face-to-face conversation with the required banking technical/managerial support is not feasible. The global chatbot market in BFSI was valued at $357 million in 2017, and is projected to reach at $2,186 million by 2024, growing at compound annual growth rate of 29.7% from 2018 to 2024 [2] [5]. Grand View Research has segmented the chatbot market scope based on end users, applications/business models, types, product landscape, verticals, and regions [9]. According to 2017 worldwide overall Statista questioning, around 20% of respondents declared they would prefer to answer the questions from AI by means of a chatbot or a virtual assistant in regard to banking [7].

The vast variety of chatbot services can be grouped by different criteria as follows [5] [9] [10]:

Types of chatbots Application/Business Model

- Chatbots for Service
- Chatbots for Social media
- Chatbots for Payment and Order processing
- Chatbots for Marketing

Types of chatbots by application:

- Standalone
- Web-based
- Messenger-based/Third party.

This research will concentrate on Web-based and Messenger-based (customer service) chatbots.

C. *Problems with intelligent chatbot services*

Since the service market is crowded with 2,000+ chatbot vendors and many of them put security and risk considerations at the bottom of their priority lists, there are many problems with the chatbot services surfaced recently. For example, Ticketmaster's global customer base was affected by a data breach discovered on 2017. The company confirmed that malicious software in the Inbenta chatbot, which it uses to provide customer service, was gathering information and sending it to a third party. Ticketmaster disabled Inbenta's software across its websites as soon as it discovered the breach [11]. In a data breach of Delta Airlines' chatbot, hackers appear to have stolen customer payment data from both Delta Air Lines and Sears by targeting a third-party chatbot provider [12]. Although chatbots have evolved as a business solution, there are significant associated risks like information leaks, denial of service, incorrect advising, etc. that must be addressed.

D. *Chatbot-related threats*

The chat services by automated programs, known as chatbots, may pose serious threats to online users. Chatbots can be exploited in online systems to send spam, spread malware, and mount phishing, sphere phishing, DDoS and man-in-the-middle attacks, data gathering, injecting falsified messages, spreading unreliable information, etc. Efforts to combat some of these threats have focused on two different approaches: 1) keyword-based filtering; and 2) human interactive proofs. The keyword-based message filters, used by third-party chat clients, suffer from excessive false negative rates because chatbot developers regularly update chatbots to avoid published keyword lists. The use of human verifications, such as CAPTCHAs, is also inefficient because bot operators support chatbots in passing the tests to log into chat rooms [13].

E. *Review of the Risk associated with chatbots*

A typical core chatbots' components that have vulnerability and risk associated with them [4]. Unfortunately, at the moment there is no standardized terminology and protocols that are common to chatbot industry thus descriptions may vary from one framework to another. According to Gartner, any chatbot should have the ability to "read" or parse human language text –it is basically a pre-requisite for understanding the natural sentence.

Mechanisms that allow such "understanding" can be the attractive targets for a hacker [14]. There are several studies that are trying to develop the ideal software or application of a chatbot, that can have a natural conversation and indistinguishable from humans. Enabling effective control mechanism should be helpful in addressing these threats. One of the managerial controls to deal with these threats is carefully crafted / reviewed SLA with the chatbot service provider.

F. Service Level Agreements

According to Gartner, developing a proper SLA prior to establishing the chatbot service user-vendor relationship is essential [14]. The survey [14] shows that SLA forms the basis for a clear definition and enforcement of user expectations. In addition to typical SLA features the ones crafted for SLA should include focus on making sure that chatbots do not proliferate unethical human behavior by machine learning algorithms, such as discrimination, or bias in decision making; The survey also assessed the issue of trust between user and providers [14]. In addition, various researchers / developers suggested the following concerns to be addressed by SLAs with chatbot providers:

- Customers have poor experiences with chatbots and are unable to accomplish their objectives when contacting a company [15] [16].
- Level of trust? Reduced opportunism? Level of reputation? [13][14].
- Availability, Accessibility in case of problems, Failure frequency (Contingency plan IR [Incident Response], DR [Disaster Recovery], BC [Business Continuity]) [17].
- Confidentiality agreement [12].

III. Proposed Approach

A. Risk Evaluation Framework

The framework is designed to assist the customers in selecting the right provider by addressing service level parameters that include availability, reliability, and the risk of an outage for each service provider. This is the rationale as to why considering risk assessment framework to be available at a point before the SLA contract is to be signed. Figure 2 shows where the risk evaluation framework fits in reaching to an SLA [18].

The results of the analysis revealed that while customers consider the impact of service outages to be very serious in their organization. Furthermore, the analysis revealed that it is very important that SLA addresses service reliability, availability, cost, number of instance types (number of different server configurations available), response time, and data storage. Continuous maintenance of services, Service Level Monitoring (SLM), are quality parameters that are also important to the customers because critical functions of their business directly depend on the quality of service [28]. In Table 2 explained link between risk and potential controls together. This will be a core of the framework. The results depict that is that applicable to SLA or not? Or maybe what to look for in the SLA. level of service customer expects from a vendor, laying out the metrics and component by which service is measured which are elaborated in Table 4.

Authors [30] used a modification of the WPM (Weighted Product Model), which compares three providers by calculating the difference of their parameters. The method uses WPM to compare all possible pairs of providers by multiplying the ratios of service levels provided by each pair. First calculate the ratio for each criterion, where each ratio is raised to the power of relative weight of the corresponding criterion. Equation 1 shows WPM used in our decision making.

$$P(CK/CL) = \prod (cKj/cLj)wj \qquad (1)$$

Where CKj is the service value of parameter j for provider K and wj is the weight for each parameter based on customer's priorities. If the ratio P (CK/CL) is greater than or equal to the value 1, then it is concluded that CK is more desirable than CL. In some service level parameters such as availability, reliability, a number of instance types and data storage higher values are better, but the chatbot provider with lesser response time and lower cost for service are more desirable. So, for parameters like response time and cost invert them in Equation 1, i.e. instead of using CKj, use 1/ CKj. Eventually, the implemented mathematical equation reduces the complexity of calculations to a large extent because it is performed only for eligible chatbot providers. The initial step filters out other providers.

B. Finding and Results

The study and analysis of chatbot provider here (Table4) compared 3 chatbot providers (Provider 1, Provider 2, Provider 3) to determine their performance, and Provider 2 topped the list in terms of SLA score, customer satisfaction and performance.

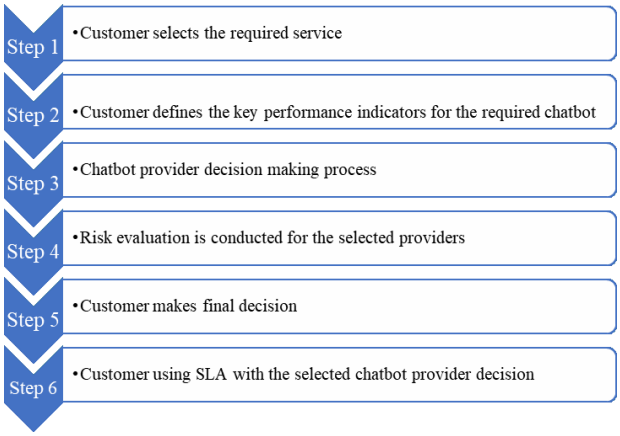

Fig 2: Role of risk evaluation framework in the process of SLA

The project proposed risk-based methodology to test SLAs Components in order to effectively help potential users of chatbot services to evaluate and select the best suitable services for its business needs while minimizing potential risks. Best practices suggested by NIST, GTAG and ISACA were linked to SLA parameters to establish the assurance for chatbot users in chatbot provider's commitment and responsibility in securing and protecting customer data, as well as know-how.

TABLE: 1 RISK ASSOCIATED WITH CHATBOT SERVICES

Risk	Description	Source
Identity problem and Identity theft	An attacker can get access to user private information if • the attacker is able to represent itself to the chatbot as a legit user • the attacker can get inject data or substitute the interface of the chatbot systems	[19] [20] [16] [21] [24] [26]
Unintentional misbehavior	Lack of common sense, silly or in-appropriate responses, tend to make poor decisions, unable to think clearly, Displays shortage of naturalness or spontaneity.	[22]
Malware attacks	Malware can affect any of the three parties – chatbot subscriber site, chatbot provider site or end user. In all three cases the attacks such as input/output manipulation, sensitive information exfiltration, identity thefts can present themselves as listed in this table.	[3] [13] [23]
Distributed denial of service (DDoS) attacks	DDoS can be just a HTTP flood – massive traffic hitting the chatbot provider server will lead to the chatbot availability even if the chatbot subscriber's service is fully functional.	[23]
Social Engineering Attack	Cybercriminals and black hat hackers can produce malicious chatbots that aim to socially engineer victims into clicking links, downloading infected documents or sharing sensitive data.	[13] [20] [23] [24]
Input/String Manipulation	Hacker can inject a fake text chatbot into a legitimate communication.	[20] [25]
Monitoring Issues	Monitoring availability of presence parameters. It is of the utmost importance that chatbot has a system that is transparent and holds agents/chatbots accountable for their actions. Without such a system, organization will be at higher risk of our data (and even our lives) being hacked and even manipulated.	[26] [27]
The Exploitation of Third-Party Services	This risk includes • Use of chatbots to attack on third party services. • Attacks on third party services that chatbot is using to force chatbot to stop operations or to feed falsified information to the user. For example, some public sources of information can be manipulated to force chatbot to use this information.	[21] [28]
Template Manipulation	Patters of chatbot responses may be manipulated while delivered to chatbot service. Encryption of the all chatbot communication is essential. For maximum security, chatbot communication should be encrypted, and chatbots should be deployed only on encrypted channels.	[12] [29]
Communication Layer Security	Data is being transferred over HTTP through encrypted connections protected by Transport Layer Security (TLS) or Secure Sockets Layer (SSL).	[21]
Partition or splitting the user input sentence	Chatbot should not expect a user to communicate using perfect grammar and syntax. Any company giving a chatbot authority to advice users will need to ensure that the chatbot has access to a large volume of communication patterns and up to date information on the services in order to understand instructions and questions and provide helpful and relevant responses. In case the chatbot is unable to provide a correct advice, a clear disclaimer and potential human intervention trigger should be considered.	[8] [28]

TABLE: 2 LINK B/W RISKS AND PONTENTIAL CONTROLS

Risk	Potential Control (From NIST)	Applicable to SLA Y/N	What to look for in the SLA?	Potential Control Mechanisms				
				NIST Control Name	*Sample CNTL NO.*	*Related Controls*	*Description*	*References*
Identity problem and Identity theft	The Organization manages Information system identifiers	Yes	Confidentiality	Identifier Management	IA-4	AC-2, IA-2, IA-3, IA-5, IA-8, SC-37	Selecting, Assigning, Preventing, Disabling the identifier	FIPS Publication 201; NIST Special Publication 800-73, 800-76, 800-78
Unintentional misbehavior	Corrective Controls	No	Data Dispersion	Incident Handling	IR-4	AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6	Coordinates incident handling activities with preparation, detection, eradication	Executive Order 13587; NIST Special Publication 800-61
Malware attacks	The Organization, Technical and Prevention Controls	Yes	Data Security lifecycle	Information System Monitoring	SI-4, SI-7, SC-5, SI-3, SC-12	SC-13, SC-23, CM-3, MP-2, SA-4	Types of packets to protect information system component, Attacks and indicators	NIST Special Publication 800-83
Distributed denial of service (DDoS) attacks	The Organization, Technical and Prevention Controls	Yes	Data Security lifecycle	Denial of service Protection	SC-5, SI-3	SC-13, SC-23	Perform periodic scans of the information system	NIST Special Publication 800-83

Risk	Potential Control (From NIST)	Applicable to SLA Y/N	What to look for in the SLA?	Potential Control Mechanisms				
				NIST Control Name	*Sample CNTL NO.*	*Related Controls*	*Description*	*References*
Input/String and Templet Manipulation	The information system implements	No	Integrity	Cryptographic Protection	SC-13, CM-11, CP-9, IA-3, IA-7	AC-2, AC-3, AC-18, AU-9, AU-10, MA-4, MP-2, SA-4, SC-8, SC-12, SC-28, SI-7	The protection of classified and controlled unclassified information	FIPS Publication 140; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov
Monitoring Issues	The organization, General and Management and Framework Controls	Yes	Security protocols, 3rd party Monitoring Service	Cryptographic Protection	SC-13, RA-5, SC-6	CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2	Scans for Vulnerability in the information system and hosted application, Deploys monitoring devices, Resource availability	NIST Special Publication 800-40, 800-70, 800-115. Web: http://cwe.mitre.org, http://nvd.nist.gov.
The Exploitation of Third-Party Services	The Organization	Yes	Integrity, Confidentiality	Supply Chain Protection	PS-7, SA-12	AT-3, CM-8, IR-4, PE-16	Reduce the likelihood of unauthorized modifications at each stage, Third-party organizational personnel conduct assessments of systems, components, products, tools, and services	NIST Special Publication 800-35
Communication Layer Security	Technical and Corrective Controls	Yes	Security protocols	System & Communications Protection Policy and Procedures	SC-1	PM-9	System program policy with communications protection procedures	NIST Special Publication 800-12, 800-100
Partition or splitting the user input sentence	Corrective and Detective Controls	No	Customer Satisfaction, Availability	Software Usage Restrictions, Application Partitioning	CM-10, SC-2	SA-4, SA-8, SC-3	Privileged user access, use of separate authentication	None
User Behavior Analytics (UBA)	Framework and Application Controls	Yes	Customer Satisfaction	Criticality Analysis, Adaptive Identification and Authentication	SA-14, IA-10	AU-6, SI-4	Supply chain protection activities such as attack surface reduction, use of all source intelligence, and tailored acquisition	None

TABLE: 3 SAMPLE OF 3 SLAS ANALYSIS & COMPARISON

SLA Component	Provider c1	Provider c2	Provider c3
Availability / Uptime Guarantee	Accurate	Accurate	Moderate
Back-door access	Yes	Yes	Yes
Use of security protocols (end to end encryption)	Service Credit	Service Credit	N/A
Hosting platform issues	Public dashboard	Public dashboard	Public dashboard
Unencrypted communications	Limited	Limited	Limited
Customer-led penetration testing (simulate cyber-attack)	Yes	Yes	Yes
Reporting uptime	Based on appropriate law	Promptly	Per contractual terms
Impersonation of individuals	Limited	N/A	Limited
Data alterations	No	No	No
Authentication and Authorization	Yes	Yes	Yes
User Behavioral Analytics (UBA)	Promptly	Promptly	Promptly

After use of Equation 1 to compare eligible chatbot providers, where CKj is the service value of parameter j for chatbot provider K given in Table 4 and wj is the weight for each parameter using Table 3.shows the results of WPM for chatbot providers (C1, C2, and C3) for the requirements of customer [30].

TABLE: 4 COMPARISON BETWEEN ELIGIBLE PROVIDERS FOR CUSTOMER.

Customer	WPM results
P(C1/C2)	0.9997
P(C2/C3)	1.0559
P(C3/C1)	0.0662

The results show that C1 is more desirable than C2, and C2 is more desirable than both C1 and C3, because C2 are greater than 1. The potential customer can conclude that C2 is the best option between eligible providers for customer [30]. According to the test, majority of the SLA component should not cooperate with risk and cost. The goal is to realize benefits from chatbots while optimizing resources and managing risk. However, even these strategies entail some risks, for instance, points out that it is difficult to manage and coordinate the work of several providers.

IV. Conclusion

The proposed research outlined risk factors associated with SaaS providing chatbot services. By looking at the risks and associated control mechanisms the paper suggested ways to manage these risks by SLA management. Paper proposed a set of possible controls that can be provisioned in SLA to ensure chatbot provider compliance to the security requirements from the customer. Examples of such controls include organizational, managerial and technical. For example, as per table 2, issue of DDoS attacks on the 3rd party infrastructure should be addressed by the following provisions in the service SLA. To test the suggested SLA evaluation approach three SLAs for various chatbot service providers have been analyzed and compared. The comparison established a clear path on how the proposed approach can be used in practice. Proposed analysis allows the customer to be informed about the risks associated with the service before moving ahead to sign an SLA with the selected provider. There are various factors affecting risks, including the type of service and its pricing plans, quality levels, infrastructure, number of users, and many more. In order to achieve these goals, this paper presents an integrated SLA system analysis with controls for chatbot services.

References

[1] V. Hristidis, "Chatbot Technologies and Challenges," 2018 First International Conference on Artificial Intelligence for Industries (AI4I), vol. doi: 10.1109/AI4I.2018.8665692, pp. 126-126, 2018.

[2] A. Bhutani and P. Wadhwani, "Global Chatbot Global Size worth over $1.34bn by 2024," Global Global Insight, 26 August 2019. [Online]. Available: https://www.gminsights.com/pressrelease/chatbot-market.

[3] "Chatbot: What is a Chatbot? Why are Chatbots Important?" Expert System, 17 July 2018 . [Online]. Available: https://expertsystem.com/chatbot/.

[4] N. M. Radziwill and M. C. Benton, "Evaluating Quality of Chatbots and Intelligent Conversational Agents," 2017.

[5] "Chatbot Market Size To Reach $1.25 Billion By 2025 | CAGR: 24.3%," Grand View Research, August 2017. [Online]. Available: https://www.grandviewresearch.com/press-release/global-chatbot-market.

[6] "Juniper Research: Chatbots to Deliver $11bn in Annual Cost Savings for Retail, Banking & Healthcare Sectors by 2023," 03 July 2018. [Online].Available:https://www.businesswire.com/news/home/20180703005029/en/Juniper-Research-Chatbots-Deliver-11bn-AnnualCost.

[7] M. Greenfield, "Acceptance of artificial intelligence chatbots by customers worldwide, as of 2017," Hearst Magazines, [Online]. Available: https://chatbotsmagazine.com/chatbot-report-2018-global-trends-and-analysis-4d8bbe4d924b.

[8] L. Hidayatin and F. Rahutomo, "Query Expansion Evaluation for Chatbot Application," 2018 International Conference on Applied Information Technology and Innovation (ICAITI), no. 10.1109/ICAITI.2018.8686762, pp. 92-95, 2018.

[9] "Chatbot Market Analysis By End User, By Application/Business Model, By Type, By Product Landscape, By Vertical, By Region (North America, Europe, APAC, MEA), And Segment Forecasts, 2018 - 2025," Aug 2017. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/chatbotmarket.

[10] K. Tajane, S. Dave, P. Jahagirdar, A. Ghadge and A. Musale, "AI Based Chat-Bot Using Azure Cognitive Services," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1-4, 2018.

[11] "Ticketmaster Blames Malware-Plagued Chatbot for Data Breach," 28 June 2018. [Online]. Available: https://www.tomshardware.com/news/ticketmaster-data-breach-uk-international,37383.html.

[12] M. Baker, "What's The Risk? 3 Things To Know About Chatbots & Cybersecurity," 19 September 2016. [Online]. Available: https://www.darkreading.com/vulnerabilities---threats/whats-the-risk- 3-things-to-know-about-chatbots-and-cybersecurity/a/d-id/1326912.

[13] N. Mohammad and H. O. Khadeer, "A Survey on Chatbot Implementation in Customer Service Industry through Deep Neural Networks," 2018 IEEE 15th International Conference on e-Business Engineering (ICEBE), pp. 54-61, 2018.

[14] K. Blum, "How to Manage Customer Service Technology Innovation," 12 March 2019. [Online]. Available: https://www.gartner.com/smarterwithgartner/27297-2/.

[15] "What Makes Users Trust a Chatbot for Customer Service? An Exploratory Interview Study," Springer International Publishing, no. no. DOI: 10.1007/978-3-030-01437-7_16, pp. 194-208, 2018.

[16] "Part Five in a Series: Managing Risks of Technologies Emerging as Business Opportunities: Chatbots," Schneiderdowns, 27 February 2019. [Online]. Available: https://schneiderdowns.com/our-thoughts-on/risk+advisory+internal+audit/technology/managing-risks-of-tech-emerging-as-biz-opps-chatbots.

[17] A. M. Rahman and A. a. Mamun, "Programming challenges of chatbot: Current and future prospective," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), no. 10.1109/R10-HTC.2017.8288910. , pp. 75-78, December 2017.

[18] B. Yadranjiaghdam, K. Hotwani and N. Tabrizi, "A Risk Evaluation Framework for Service Level Agreements," 2016 IEEE International Conference on Computer and Information Technology (CIT), no. doi: 10.1109/CIT.2016.93, pp. 681-685, 2016.

[19] "Chatbots have an identity problem. It's time we got things straight," 25 June 2018. [Online]. Available: https://hackernoon.com/chatbots-have-an-identity-problem-its-time-we-got-things-straight-fd0d3ac3fbb1.

[20] "Chatbot Security – What You Need To Know," [Online]. Available: https://inform-comms.com/chatbot-security-what-you-need-to-know/.

[21] A. Schlesinger, K. P. O'Hara and A. S. Taylor, "Let's Talk About Race: Identity, Chatbots, and AI".

[22] "What To Do When AI Chatbots Get It Wrong?," 10 February 2019. [Online]. Available: https://hackernoon.com/what-to-do-when-ai-chatbots-get-it-wrong-9c343be876c2.

[23] K. Matthews, 18 Sep 2018 . [Online]. Available: https://chatbotslife.com/your-chatbot-could-be-vulnerable-to-cybercriminals-288e9b47654d.

[24] J. Björnhed, "Using a Chatbot to Prevent Identity Fraud by Social Engineering".

[25] D. (. Kazemi, "wordfilter. npm.," 30 May 2017. [Online]. Available: https://www.npmjs.com/package/wordfilter.

[26] M. Tsvetkova, R. Garcia-Gavilanes, L. Floridi and T. Yasseri, "Even Good Bots Fight," 2016.

[27] "Chatbot Security Risks: What you need to know before starting an online chat," SiteLock LLC., 3 June 2019. [Online]. Available: https://www.sitelock.com/blog/chatbot-security-risks/..

[28] N. Dreyfus, "Beware of the legal risks surrounding the rise of chatbots," Expertguides, 09 Jan 2017. [Online]. Available: https://www.expertguides.com/articles/beware-of-the-legal-risks-surrounding-the-rise-of-chatbots/ARTWUSIC.

[29] G. M. D'silva, S. Thakare, S. More and J. Kuriakose, "Real world smart chatbot for customer care using a software as a service (SaaS) architecture," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), no. doi: 10.1109/I-SMAC.2017.8058261, pp. 658-664, 2017.

[30] P. Gulia and S. Sood, "Dynamic Ranking and Selection of Cloud Providers Using Service Level Agreements," International Journal of Advanced Research in Computer Science and Software Engineering,

[31] "Terms & Conditions," ONLIM, [Online]. Available: https://onlim.com/en/terms- conditions/.

[32] "Terms and Conditions," AIVO, 15 March 2019. [Online]. Available: https://www.aivo.co/en/terms/.

[33] "Service Level Agreement," Enterprisebot, 14 August 2019. [Online]. Available: https://enterprisebot.ai/legal/sla.

[34] G. J. Mirobi and L. Arockiam, "Service Level Management in cloud computing," International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)no. 10.1109/ICCICCT.2015.7475308, pp. 376-387, 2015.

[35] B. Yadranjiaghdam, K. Hotwani and N. Tabrizi, "A Risk Evaluation Framework for Service Level," 2016 IEEE International Conference on Computer and Information Technology, no. no. DOI 10.1109/CIT.2016.93, pp. 681-685, 2016.