Enhanced Security Framework On Chatbot Using Mac Address Authentication To Customer Service Quality

Richki Hardi, Ahmad Naim Che Pee, Nanna Suryana Herman

Abstract: The function of customer service includes serving customer complaints. The process is able to use as a control for customer satisfaction. The more consumers who are satisfied with the benefit of a product, the better the customer service will be. Currently, Chatbot has been widely used in companies to improve service and to simplify customer service. Its existence is beneficial in facilitating fast data access so that it can provide services to customers more quickly. Because of this easy access, companies are obliged to ensure that all devices they have are guaranteed security. Based on this reason, the researcher will increase the Security Framework on the Chatbot by using MAC address authentication which can only be accessed by the registered customer's hardware machine address, so that if it is accessed on a different hardware device (smartphone, laptop or tablet), then the chatbot menu will not be able to be run. MAC address authentication on hardware is expected to be the first stage to be authenticated by the system prior to software authentication such as hybrids such as matching name and password, unique code and email verification.

Index Terms: security framework, chatbot, customer service, authentication, MAC address.

1. INTRODUCTION

The presence of information technology is increasingly needed by society; almost all lines of life use technology as a tool [1]. currently, the chatbot has been widely used in companies to improve services. The use of chatbot applications can only be operated through mobile gadgets that are connected to the internet. Mobile gadgets are devices that can be carried and used everywhere, such as smartphones, laptops, tablets, and so on. In today's era, of course, these devices are already familiar to use in companies. Its existence is beneficial in facilitating fast data access so that it can provide services to customers more quickly. Because of this easy access, companies are obliged to ensure that all devices they have are guaranteed security. Data security in today's technology era is essential [2]. Even more crucial than previous periods, which had limited data access and archiving[3]. With proper security, it will have an impact on the smooth operation of the company and the sustainability of the company in the short, medium and long term [4].

Several types of security frameworks in the Chatbot are prepared to secure customer personal conversation data with customer service. The kind of security that has been done is quite good but needs to be improved from the hardware or machine side because security from the software or application side turns out to be able to run on different hardware devices. Based on this reason, the researcher will increase the Security Framework on the Chatbot by using MAC address authentication which is able only to be accessed by the registered customer's hardware machine address, so that if it is accessed on a different hardware device (smartphone, laptop or tablet), then the chatbot menu will not is able to be run. MAC address authentication on hardware is expected to be the first stage to be authenticated by the system before software such as hybrid authentication such as name and password matching, unique code and email verification. Numerous studies have attempted to explain about chatbot system and its security, namely: Chatbots have changed the way people think and live because chatbots can be present and ready to provide service assistance while being able to perform other tasks anytime and anywhere [5]. Several previous studies have examined how chatbots perform [6]. Compare several existing chatbots to find out their performance level. However, it hasn't included aspects of the user experience [7]. One way that can be done to deepen this aspect is to use a user-centred design approach where the user is involved in one or more of them [8]. This research is inseparable from utilising existing research, the results of the research [9]. Used as a benchmark for how the language needs to be used in chatbot design. As well as being referred to several evaluations that need to be considered from the research results, in the analysis and design of new chatbots such as ease of usage, clarity, naturalness, friendliness, robustness regarding misunderstandings, and willingness to use the system again [10]. A chatbot is a computer program that is able to run intelligent conversations with users via voice or text, often with short conversations [6]. The way to choose the best design idea is to evaluate the approach based on the usability heuristic, and hints from the Messenger platform [11]. Then in banking, the Chatbot system is a computer program designed to simulate an intelligent conversation of any banking-related questions with human users through auditory or textual methods, the smart chatbot system for this bank will provide appropriate responses to user requests. This is an intelligent system that will think like humans. This system will be beneficial in reducing the workload of employees. Provide fast and accurate answers to users [12]. Chatbots are one of the most basic and famous examples of intelligent Human-Computer Interaction (HCI). Chatbots get a lot better when some productivity applications like simple calculators or dictionaries or even games are embedded in them. And more than that the chatbot is able also to create memos, notes, set

- *Richki Hardi, Universitas Mulia, currently pursuing doctors degree program in Fakulti Teknologi Maklumat dan Komunikasi (FTMK) in Universiti Teknikal Malaysia Melaka (UTeM), Malaysia, Phone-+6281227224080. E-mail: richkihardi@ieee.org*
- *Ahmad Naim Che Pee, Universiti Teknikal Malaysia Melaka, Malaysia. E-mail: naim@utem.edu.my*
- *Nanna Suryana, Universiti Teknikal Malaysia Melaka, Malaysia. E-mail: nsuryana@utem.edu.my*

alarms and open programs on the user's computer or mobile phone on demand [13]. Before chatbots, there were only bots: The invention of chatbots ushered in a new era of technology, the era of chat services. Chatbots are virtual people who are able to effectively talk to any human with the help of textual skills in an interactive manner. There are now many cloud-based platforms available for developing chatbots such as Microsoft bot framework, IBM Watson, Kore, AWS lambda, Microsoft Azure bot service, Chatfuel, Heroku and many more. Still, all those techniques have some disadvantages such as Artificial Intelligence, NLP, services conversion, programming, etc [14]. Moreover, banking chatbots are one of the principal members of FinTech. Combining several AI technologies, chatbots are able to help or gradually replace the jobs of banking and financial personnel. Apart from reducing staff costs of financial institutions, it is able also to improve customer convenience, improve work efficiency, and improve service quality. However, for customers receiving financial services, trust, data security, and personal privacy are significant concerns. Chatbots have AI technology that is able to pose unpredictable security risks to customers, once a program is designed inappropriately, abused or maliciously. To protect customer data security and personal privacy, this paper designs and plans a Chatbot Security Control Procedure (CSCP) [15]. Chatbots are able to work at banks because they can be programmed to interact with humans, even more than that, "humanizing" interactions to make them appear more human. The chatbot system can also be secured just like most websites and applications, using two-factor authentication and encryption, etc [16]. According to a recent analysis of studies on mobile health services, architecture plays a simple role in data transmission. The system proposed in this study is capable of filtering and processing data through a predefined health framework chatbot to transmit various information to users and the health information system (HIS), as well as to provide accurate medical services. Unlike existing mobile health systems, chatbot-based mobile health systems not only provide general information but also interactively give the information required for users [17]. Then Van Cuong & Tan (2019) considering the development of science and technology of Internet Protocol cameras are increasingly popular and widely used, a chatbot framework is needed to help users get personal detection information from cameras that are able to observe 24/7 via Facebook messenger called Security Bot (Sbot). To build Sbot, a system that includes a camera network, Human Detection Server (HDS), and Sbot server is designed. In the method, Sbot transfers information between the user and HDS using the Facebook Messenger Platform, detects humans in real-time and updates the datasets captured from surveillance cameras [18]. Experimental implementation of smart home automation can be via the Facebook chatbot, as it allows users to access and control their home appliances remotely and literally from anywhere using the Raspberry Pi, Facebook chatbot and Google Maps API. The system describes the convenience of users in using Facebook Messenger to communicate and send commands easily. The advantage is that you can access Facebook from any internet-connected device to control your home device. For further work, some additional features that can be implemented are in terms of machine learning, voice commands and Natural Language Processing (NLP). This will allow a smarter approach to being able to understand user input [19].

Likewise with Clarizia et al. (2018), In recent years there has been a rapid development of the use of Chatbots in various fields, such as Health, Marketing, Education, Support Systems, Cultural Heritage, Entertainment and many others. Likewise, the student-based e-learning platform, which is a model for managing communication and providing correct answers to students. It aims to realize a system that is able to detect questions and use natural language processing techniques and domain ontologies and give the students appropriate answers via chatbots [20]. Chatbot is an instant message account that is able to provide services using an immediate message framework to provide conversation services to users in an efficient manner. Fast Chatbot with web and mobile applications that are less confusing and easy to install because there is no need to have an installation package. These packages are easy to manage and distribute. Chatbots are a rising trend, and chatbots are increasing business effectiveness by providing a better experience at a lower cost. Chatbots are an ecosystem and move quite fast, and over time new features of the platform have been added too [21]. With the increasing use of information technology in all domains of life, hacking is becoming more useful than ever. Likewise, in chatbots, hacking is possible; it is necessary to set up Networking Chatbot as an activity to detect collective and contextual security attacks [22]. The Intelligent Chatbot service is one of the leading applications in user assistance and many other areas. Apart from bringing many benefits to users, this service is able also to bring risks to the company. An overview of the functionality and architecture of a typical chatbot service shows the potential dangers associated with chatbots. Smart chatbot services have reached the mainstream of web-based user services, and they will remain. Some distinct evolutionary steps - like audio- or video chatbots aren't yet mainstream, but they are already being tested. Apart from the communication tool, this technology comes with significant benefits, but it is able also to carry additional IT-related risks for the companies using it [23]. Even though Chabot cannot entirely handle requests or customer service. Chatbots is able to be attacked and require serious consideration in their safety and security [24]. The Intelligent Chatbot service is one of the leading applications in user assistance and many other areas. Apart from bringing many benefits to users, this service can also bring risks to the company. An overview of the functionality and architecture of a typical chatbot service shows the potential risks associated with chatbots. Smart chatbot services have reached the mainstream of web-based user services, and they will remain. Some distinct evolutionary steps - like audio- or video chatbots aren't yet mainstream, but they are already being tested. Apart from communication tools, this technology comes with significant benefits but can also carry additional IT-related risks for companies using it [24]. The number of cyberattacks is increasing, the knowledge and tools to detect and analyze such attacks require a lot of effort. An organization must have experts who can handle it to investigate security and have a broad knowledge to be able to deal with information security incidents. The chatbot must be smart enough to have the help of a reliable security tool on the Internet. In such research, it is necessary to prepare the SOC (Security Operation Center), to detect incidents, analyze evidence intelligently with appropriate security tools and resolve it yourself or raise it to the relevant authorities [25]. In wireless networks, security issues require more serious attention, considering that the data transmission medium is broadcast radio waves. This is one reason for the vulnerability of security in wireless networks. An authentication policy was adopted to secure access, abuse, modification, and denial of services in the network and other resources [26]. MAC Address is a unique identifier consisting of various byte numbers assigned to most network adapters or Network Interface Card (NIC). Each network device has a MAC address that is different from one another. So by applying the MAC Address security, every network service user who wants to connect to the network must register his MAC Address. This is able to be used to minimize network service users who should not have access. The use of MAC Address filtering is able to limit the number of computers that is able to connect to the wireless hotspot by considering the IP Address and MAC Address registered [27]. Communication line security vulnerabilities will be more dangerous than using cables. For that, it is necessary to handle extra security on a wireless network [28].

1.1 Problem Statement

Based on the introduction above, the problem formulation is as follows:

1) How the security framework on the chatbot needs to be improved to minimize hacking attempts and unwanted risks using MAC Address Authentication?
2) Why is a MAC address needed to increase the security framework on chatbot?

1.2 Research Objectives

Among the research objectives are:

1) To investigate the level of security in the chatbot system so that that customer service is able to provide maximum service to the right customer.
2) To design a chatbot security system on the machine or hardware side, namely by authenticating the MAC address, so that only the correct user device is able to access the chatbot.
3) To describe the MAC Address authentication pattern on a chatbot system, a chatbot is able only to be run on registered hardware (smartphone, tablet, or laptop) so that when accessed using other devices, it disable to be run.

1.3 Research Scopes

The scope of research in this study is as follows:

1) Improve Security Framework to Chatbot by using MAC address authentication on customer hardware.
2) MAC address authentication or hardware machines on a chatbot is the first authentication done before authenticating the software to enter the chatbot page.

1.4 Hypothesis / Research Questions

The research questions in this study include:

1) How to minimize, eliminate risks and vulnerabilities and maintain the confidentiality of data on the chatbot by using MAC address authentication, so that the machine address becomes the main thing in checking the correctness of the user's hardware data?
2) How to create an internal security culture in the chatbot while still providing an authentication system in the chatbot software after authenticating the user's machine address or MAC address?

TABLE 1.
RELATIONSHIPS RP, RQ, RO, ANALYSIS AND RC

Research Problems (RP)	Research Questions (RQ)	Research Objectives (RO)	Data Analysis	Research Contribution (RC)
Many chatbots cannot be controlled due to the absence of security authentication so that the chatbots do not know the identity of the interacting customer, and have not been able to provide maximum service to customers.	How to minimise, eliminate risks and vulnerabilities and maintain data confidentiality on the chatbot system by using MAC address authentication, so that the machine address becomes the main thing in checking the validity of the user's hardware data?	To investigate the level of security in the chatbot system so that that customer service is able to provide maximum service to the right customer.	Security, the more companies are implementing services to customers using the chatbot system, the security of the system needs to be improved to minimize hacking attempts and unwanted risks.	Application of MAC Address authentication method in the chatbot security framework
Chatbots currently circulating on average are not supported by hardware security, which is able to check the correctness of the user's hardware (one to one), this is able to allow chatbots to run on devices that do not belong to the user (one to many)		To design a chatbot security system on the machine or hardware side, namely by authenticating the MAC address, so that only the correct user device can access the chatbot.	Authentication, in terms of system security, authentication is essential because by performing authentication, the system is able to determine the correctness of data from customers, especially on customer hardware authentication so that only the correct customer is able to access the chatbot.	
The culture of protecting data and creating security business processes on the chatbot system is still not optimal, so the hacking of customer communication on the chatbot is possible.	How to create an internal security culture in the chatbot while still providing an authentication system in the chatbot software after authenticating the user's machine address or	To describe authentication of MAC addresses on hardware, chatbots can be able to run on registered device (smartphone, tablet, or laptop) so that when accessed using other equipment,		The application of the chatbot system security business process uses authentication stages.

	mac address?	they unable be run.		

1. RESEARCH METHODOLOGY

This research will focus on the security framework in chatbots by prioritising checking the machine or physical address of the hardware.

2.1 Type of Research

This type of research is using qualitative and quantitative approaches, using case studies and looking at the field conditions by collecting data from information sources. The results of this study are able to be applied in similar situations in other locations. Case studies are conducted intensively with various data sources and are limited to time and location limitations. The case raised is Enhance Security Framework On Chatbot Using Mac Address Authentication To Customer Service Quality. The research period is one semester. In the workflow in Figure 2, 4 components of chatbot communication are explained, namely: 1). Chatbot, 2) User (human), 3) Input, 4) Feedback. The public stated that chatbots helped them save time in getting information. The ease of obtaining information is the main motivation for using chatbots.

2.2 Research Flow

Seen in Figure 1 is the flow used in this research, customers who will access the internet network or chatbot must pass security verification 2 (two) times, namely verification of the MAC address of the device using firewall filtering, as well as verification of users and passwords using the method login. The application of these multiple security models aims to minimize leakage of access rights in the chatbot system. If the customer only knows the user and password without registering the MAC address, then the client cannot access the internet network on the chatbot.

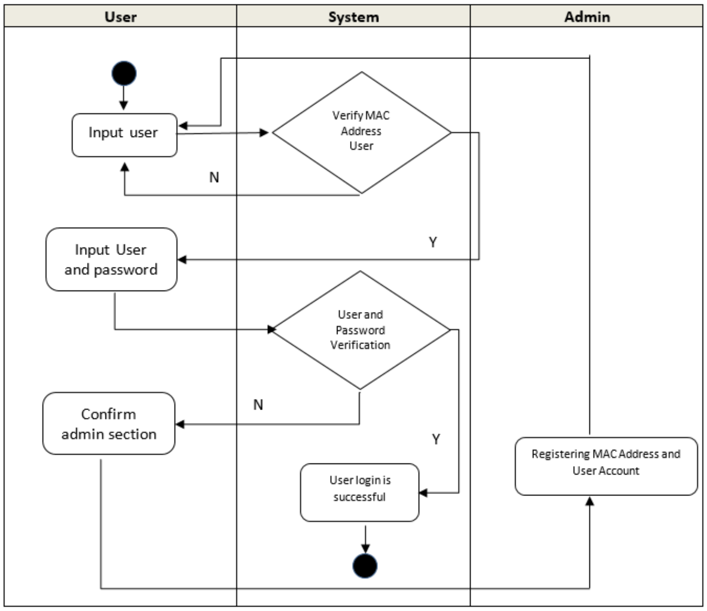

Fig. 1. Activity Diagram Security Framework

The following is figure 2 regarding the structure of the k-chart research:

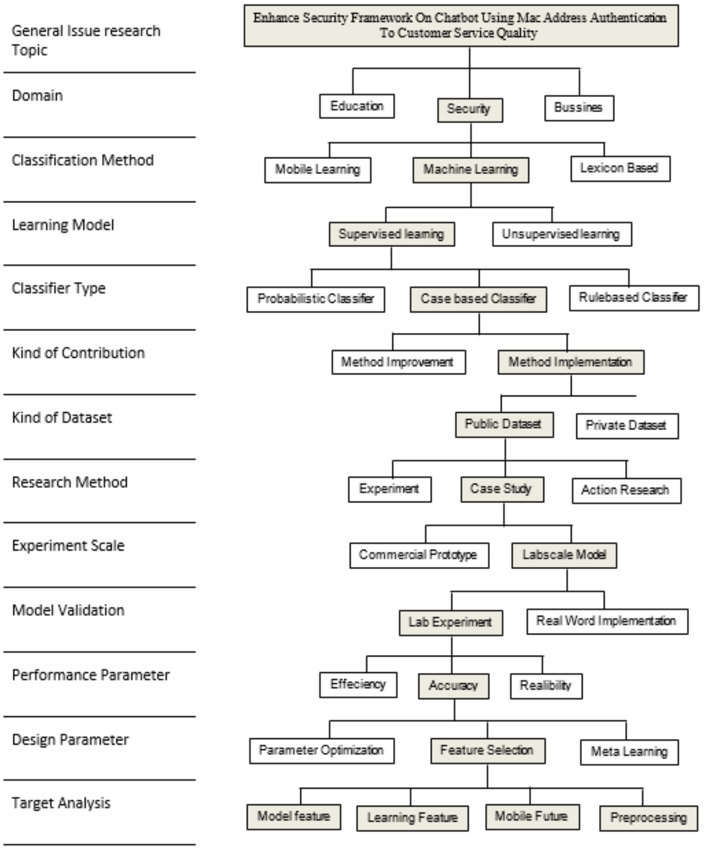

Fig. 2. K-Chart research

2.3 Interaction Stages

The following is figure 3 regarding the stages of interaction in the chatbot system:

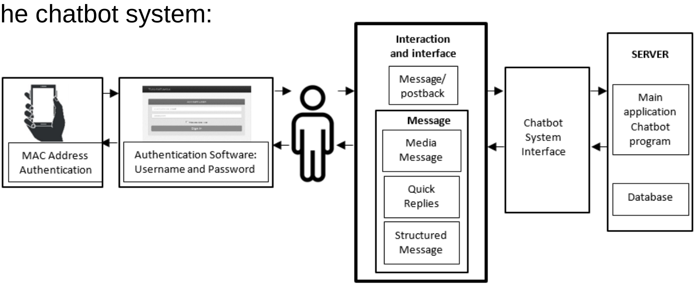
MAC Address Authentication
Authentication Software: Username and Password
Interaction and interface
Message/ postback
Message
Media Message
Quick Replies
Structured Message
Chatbot System Interface
SERVER
Main application Chatbot program
Database

Fig. 3. Stages of interaction

TABLE 1.
RISKS ASSOCIATED WITH CHATBOT SERVICES

Risk	Description	Source
Identity issues and identity theft	An attacker is able to gain access to a user's personal information if:: 1. The attacker is able to present himself to the chatbot as a legitimate user 2. The attacker is able to get data injection or replace the chatbot system interface	[29][29] [30] [31] [32]
Unintentional bad behaviour	Lack of common sense, ridiculous or inappropriate responses, prone to making bad decisions, unable to think clearly, Shows a lack of naturalness or spontaneity.	[33]
Malware attack	Malware can affect one of three parties - the chatbot customer site, the chatbot provider site, or the end-user.	[34]

	In all three cases of attacks such as input/output manipulation, exfiltration of sensitive information, identity theft can present itself.	
Distributed Denial of Service (DDoS) attack	A DDoS is able to be an HTTP flood - massive traffic coming to the chatbot provider's server will lead to the availability of the chatbot even though the chatbot's customer service is fully functional.	[35]
Social engineering attacks	Cybercriminals and black hat hackers can create malicious chatbots that aim to socially trick victims into clicking on links, downloading infected documents, or sharing sensitive data.	[35] [36]
Input or string manipulation	Hackers are able to insert fake text chatbots into legitimate communications.	[30]
Monitoring issues	Monitor availability of attendance parameters. The most important thing is that chatbots have a transparent system and hold agents/chatbots accountable for their actions. Without such systems, organizations will be at higher risk if our data is hacked and even manipulated.	[32] [37]
The exploitation of Third Party Services	These risks include 1. Use of chatbots to attack third party services. 2. Attacks on third-party services that chatbots use to force chatbots to stop operations or provide users with false information. For example, some public sources of information could be manipulated to force chatbots to use this information.	[31] [38]
Manipulasi Template	The chatbot response pattern can be manipulated when sent to the chatbot service. Encryption of all chatbot communications is essential. For maximum security, chatbot communications should be encrypted, and chatbots should be used only on encrypted channels	[39] [40]
Communication Layer Security	Data is being transferred over HTTP over an encrypted connection protected by Transport Layer Security (TLS) or Secure Sockets Layer (SSL).	[31]
Partition or split user input sentences	Chatbots shouldn't expect users to communicate using perfect grammar and syntax. If the chatbot is unable to provide correct advice, clear disclaimers, and potential triggers for human intervention must be considered.	[41] [38]

2.4 Expected outcomes:

Chatbots can run optimally, educating customers on the importance of protecting and protecting customer privacy data by implementing the Enhance Security Framework On Chatbot Using Mac Address Authentication. Benefits for customers: can only be accessed through the customer's hardware that has been registered, so if you use other than that device, the chatbot dialogue cannot be continued. This makes it possible to help secure customer chat data by filtering the proper hardware data. Benefits for the organization: helps make it easier for organizations or companies to obtain a valid customer identity, so that history and follow-up customer chats are able to be easily carried out.

2. Conclusion

Security Framework On Chatbot Using Mac Address Authentication To Customer Service Quality is an effort to increase security in using chatbots. MAC Address authentication is the first stage of security that will be checked by the system before proceeding to the next security stage. The physical address of the device that is owned by the device must be registered to interact with the chatbot. One device has one physical address and able only to be used by one person. It is a step to increase security on a chatbot and at the same time educate customers that device ownership is essential to be maintained and maintained.

Acknowledgment

The authors wish to thank Supervisors - Universiti Teknikal Malaysia Melaka. This research was supported in by a grant from Universitas Mulia.

References

[1] R. Hardi, “Genetic algorithm in solving the TSP on these mineral water,” in 2015 International Seminar on Intelligent Technology and Its Applications, ISITIA 2015 - Proceeding, 2015, doi: 10.1109/ISITIA.2015.7220008.

[2] J. Febrian Rusdi et al., “ICT Research in Indonesia,” 2019.

[3] Y. Hendriana and R. Hardi, “Remote control system as serial communications mobile using a microcontroller,” in 2016 International Conference on Information Technology Systems and Innovation, ICITSI 2016 - Proceedings, 2017, doi: 10.1109/ICITSI.2016.7858212.

[4] B. Sunaryo et al., “Mapping Mining Potential Using WebGIS,” SciTech Framew., 2019.

[5] B. Abu Shawar and E. Atwell, “Chatbots: are they really useful?,” LDV-Forum Zeitschrift für Comput. und Sprachtechnologie, 2007.

[6] K. D. Tillotson, “The implementation, analysis, and evaluation of a humanized information retrieval chat-bot,” ProQuest Diss. Theses, 2012.

[7] K. Kuligowska, “Commercial Chatbot: Performance Evaluation, Usability Metrics and Quality Standards of Embodied Conversational Agents,” Prof. Cent. Bus. Res., 2015, doi: 10.18483/pcbr.22.

[8] C. Abras, D. Maloney-Krichmar, and et al, “User-Centered Design BT - Bainbridge,” Bainbridge, 2004.

[9] J. Hill, W. Randolph Ford, and I. G. Farreras, “Real conversations with artificial intelligence: A comparison between human-human online conversations and human-chatbot conversations,” Comput. Human Behav., 2015, doi: 10.1016/j.chb.2015.02.026.

[10] V. Hung, M. Elvir, A. Gonzalez, and R. DeMara, “Towards a method for evaluating naturalness in conversational dialog systems,” in Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, 2009, doi: 10.1109/ICSMC.2009.5345904.

[11] J. Nielsen and R. Molich, “Heuristic evaluation of user interfaces,” in Conference on Human Factors in Computing Systems - Proceedings, 1990, doi: 10.1145/97243.97281.

[12] A. Dole, H. Sansare, R. Harekar, M. Mane, and A. Professor, “Intelligent Chat Bot for Banking System,” Int. J. Emerg. Trends Technol. Comput. Sci., 2015.

[13] A. Khanna, B. Pandey, K. Vashishta, K. Kalia, B.

Pradeepkumar, and T. Das, “A Study of Today’s A.I. through Chatbots and Rediscovery of Machine Intelligence,” Int. J. u- e-Service, Sci. Technol., vol. 8, no. 7, pp. 277–284, Jul. 2015, doi: 10.14257/ijunesst.2015.8.7.28.

[14] A. Patil, K. Marimuthu, A. Nagaraja Rao, and R. Niranchana, “Comparative study of cloud platforms to develop a chatbot,” Int. J. Eng. Technol., 2017, doi: 10.14419/ijet.v6i3.7628.

[15] S. T. Lai, F. Y. Leu, and J. W. Lin, “A Banking Chatbot Security Control Procedure for Protecting User Data Security and Privacy,” in Lecture Notes on Data Engineering and Communications Technologies, 2019.

[16] K. Letheren and P. Dootson, “Banking with a chatbot: A Battle between convenience and security,” QUT Bus. Sch. Sch. Advert. Mark. Public Relations; Sch. Manag., 2017.

[17] K. Chung and R. C. Park, “Chatbot-based heathcare service with a knowledge base for cloud computing,” Cluster Comput., 2019, doi: 10.1007/s10586-018-2334-5.

[18] T. Van Cuong and T. M. Tan, “Design and implementation of chatbot framework for network security cameras,” in Proceedings of 2019 International Conference on System Science and Engineering, ICSSE 2019, 2019, doi: 10.1109/ICSSE.2019.8823516.

[19] T. Parthornratt, D. Kitsawat, P. Putthapipat, and P. Koronjaruwat, “A Smart Home Automation Via Facebook Chatbot and Raspberry Pi,” in 2018 2nd International Conference on Engineering Innovation, ICEI 2018, 2018, doi: 10.1109/ICEI18.2018.8448761.

[20] F. Clarizia, F. Colace, M. Lombardi, F. Pascale, and D. Santaniello, “Chatbot: An education support system for student,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, doi: 10.1007/978-3-030-01689-0_23.

[21] A. M. Rahman, A. Al Mamun, and A. Islam, “Programming challenges of chatbot: Current and future prospective,” in 5th IEEE Region 10 Humanitarian Technology Conference 2017, R10-HTC 2017, 2018, doi: 10.1109/R10-HTC.2017.8288910.

[22] K. Al Jallad, M. Aljnidi, and M. S. Desouki, “Big data analysis and distributed deep learning for next-generation intrusion detection system optimization,” J. Big Data, 2019, doi: 10.1186/s40537-019-0248-6.

[23] K. Gondaliya, S. Butakov, and P. Zavarsky, “SLA as a mechanism to manage risks related to chatbot services.,” in Proceedings - 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, IDS 2020, 2020, doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00050.

[24] K. Patil and M. S. Kulkarni, “Artificial intelligence in financial services: Customer chatbot advisor adoption,” Int. J. Innov. Technol. Explor. Eng., 2019, doi: 10.35940/ijitee.A4928.119119.

[25] V. H. Perera, A. N. Senarathne, and L. Rupasinghe, “Intelligent SOC Chatbot for Security Operation Center,” in 2019 International Conference on Advancements in Computing (ICAC), 2019, pp. 340–345, doi: 10.1109/ICAC49085.2019.9103388.

[26] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends,” Proceedings of the IEEE. 2016, doi: 10.1109/JPROC.2016.2558521.

[27] M. Asija, “MAC Address,” IRA-International J. Technol. Eng. (ISSN 2455-4480), 2016, doi: 10.21013/jte.v3.n1.p5.

[28] P. Rengaraju, S. S. Kumar, and C. H. Lung, “Investigation of security and QoS on SDN firewall using MAC filtering,” in 2017 International Conference on Computer Communication and Informatics, ICCCI 2017, 2017, doi: 10.1109/ICCCI.2017.8117772.

[29] R. Ashri, “Chatbots have an identity problem. It’s time we got things straight,” 25 June 2018, 2018. [Online]. Available: https://hackernoon.com/chatbotshave-an-identity-problem-its-time-we-got-things-straightfd0d3ac3fbb1.

[30] I. Communications, “Chatbot Security – What You Need To Know.” [Online]. Available: https://inform-comms.com/chatbot-security-what-you-need-to-know/. [Accessed: 17-Jul-2020].

[31] A. Schlesinger, K. P. O’Hara, and A. S. Taylor, “Let’s talk about race: Identity, chatbots, and AI,” in Conference on Human Factors in Computing Systems - Proceedings, 2018, doi: 10.1145/3173574.3173889.

[32] M. Tsvetkova, R. García-Gavilanes, L. Floridi, and T. Yasseri, “Even good bots fight: The case of Wikipedia,” PLoS One, 2017, doi: 10.1371/journal.pone.0171774.

[33] ESparkBiz, “What To Do When AI Chatbots Get It Wrong?,” 11 February 2019, 2019. [Online]. Available: https://hackernoon.com/what-to-do-when-ai-chatbots-get-it-wrong-9c343be876c2.

[34] M. Nuruzzaman and O. K. Hussain, “A Survey on Chatbot Implementation in Customer Service Industry through Deep Neural Networks,” in Proceedings - 2018 IEEE 15th International Conference on e-Business Engineering, ICEBE 2018, 2018, doi: 10.1109/ICEBE.2018.00019.

[35] KaylaMatthews, “Your Chatbot Could Be Vulnerable to Cybercriminals,” 18 Sep 2018, 2018. [Online]. Available: https://chatbotslife.com/your-chatbot-could-be-vulnerable-to- cybercriminals-288e9b47654d.

[36] N. R. and M. Benton and Abstract:, “Evaluating Quality of Chatbots and Intelligent Conversational Agents Nicole,” Int. J. PharmTech Res., 2015, doi: 10.1109/GSIS.2013.6714845.

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

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

[39] 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,” in Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, 2017, doi: 10.1109/I-SMAC.2017.8058261.

[40] M. Baker, “What’s The Risk? 3 Things To Know About Chatbots & Cybersecurity,” 19 September 2016, 2016. [Online]. Available: https://www.darkreading.com/vulnerabilities--

threats/whats-the-risk- 3-things-to-know-about-chatbots-andcybersecurity/a/d-id/1326912.

[41] L. Hidayatin and F. Rahutomo, “Query Expansion Evaluation for Chatbot Application,” in Proceedings of ICAITI 2018 - 1st International Conference on Applied Information Technology and Innovation: Toward A New Paradigm for the Design of Assistive Technology in Smart Home Care, 2018, doi: 10.1109/ICAITI.2018.8686762.