Proceedings of the Sixth International Conference on Intelligent Computing and Control Systems (ICICCS 2022)
IEEE Xplore Part Number: CFP22K74-ART; ISBN: 978-1-6654-1035-9

Theoretical Evaluation of Securing Modules for Educational Chatbot

Milind H Shah
Research Scholar
Computer Engineering (Cyber Security)
GTU GSET, Chandkheda
Ahmedabad, Gujarat, India
milindshahcomputer@gmail.com

Mahesh Panchal
Assistant Professor
Computer Engineering (Cyber Security)
GTU GSET, Chandkheda
Ahmedabad, Gujarat, India
ap.ca.mhp@gtu.edu.in

2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS) | 978-1-6654-1035-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICICCS53718.2022.9788120

***Abstract* - A "chatbot" is a computer programme that interacts with and processes human conversations while also enabling humans to interact with and communicate with digital devices. It is also described as one of the most advanced and promising expressions of interactions between humans and machines. Its main task is to help students by providing answers to their questions. Existing chatbots are not entirely secure and can create open passages for cyber criminals or hackers to access the data flowing through the chatbot interface. So the chatbot will be made secure using the techniques of authentication (session) timeout and encryption. "Encryption is a method of secure communication that prevents others from accessing data while it is being transferred from one end system to another. The data is encrypted on the sender's system, so only the intended recipient can decrypt it. " Authentication (session) timeout restricts a time limit on how long an authenticated user can stay "logged in," so this prevents cyber criminals from having enough time to predict their way into somebody's secured account. This review addresses the various methods and techniques that assist in protecting the student's information from hackers and making the conversations secure for both the educational institute and the students.**

Keywords— Artificial Intelligence, Machine Learning, Deep Learning, Natural Language Processing, Chatbot, Dataset, Response, and Query

I. INTRODUCTION

Customer satisfaction is critical to a company's ability to generate income, profits, and revenues. It is frequently the most resource-intensive section within a company, overwhelming billions of dollars per year to change customers' overall perception.

To ensure that customers are satisfied with their purchase, employees spend a significant amount of time answering questions via phone or messaging apps. There are two flaws in the traditional customer service model: First, staff frequently receive repetitive questions from a wide range of customers, which machines can answer cost-effectively. Second, providing 24-hour services is difficult, especially for most non-global businesses.

According to Chatbots Magazine, businesses are willing to use chatbots because they understand that their customers expect quick responses. When a prospective customer contacts a business, they expect a prompt response. Customers will frequently move on if they do not receive a prompt response, potentially resulting in lost sales opportunities. The use of chatbots has provided significant benefits to the customer service department. Because chatbots handle a large amount of sensitive information, there are some serious security concerns. Using a chatbot to manage sensitive data causes serious security risks for any business.

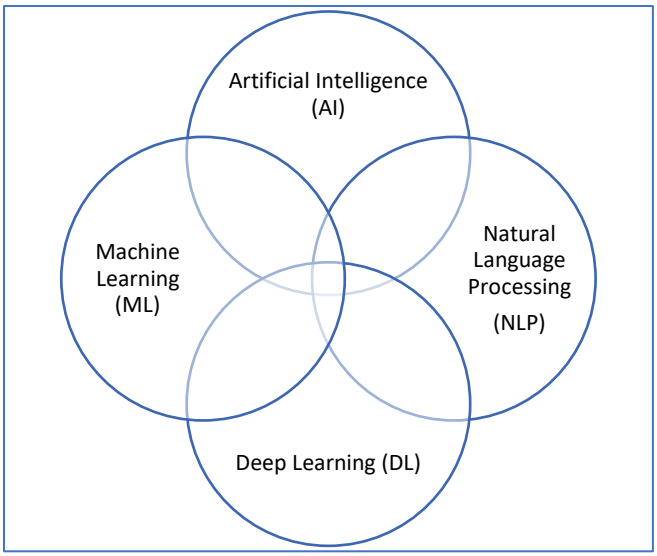

Fig 1. Relationship between AI, ML, DL & NLP

Artificial Intelligence (AI) is rapidly gaining popularity in education. The chatbot system is one of the most frequently used AI tools to support teaching and learning activities. Chatbots are viewed as a potentially beneficial technology for assisting students in educational settings. Chatbot technology is a critical component of improving and promoting a more personalized learning experience in education. Chatbots are informal or communicating agents that interact with users in real time. "Chatbots are increasingly being used to improve student interaction in today's technical world, where communication and a variety of other activities are greatly reliant on online platforms". Due to the fact that the majority of university students own a smartphone, they are avid users of web applications [1].

Recent security issues with chatbots are that while building educational chatbot they must ensure privacy and security. Because it is important for educational institutions such as colleges and schools, where chatbot captures students' data or information.

The purpose of the chatbot is to provide user support, catering to a large number of target audiences at the same time, ensuring the security of user data, and earning the confidence of users.

There are different types of chatbots used in educational institutions or organizations that explain the unique aspects of chatbot implementation in education. University of Murcia in Spain uses Lola to reduce the volume of student enquiries during enrollment times, which reduces the overburden and Dina serves the same purpose as the WhatsApp chatbot for the admissions office of Dian Nuswantoro Semarang University in Indonesia, according to the university. Outside the admissions and registration procedures, CourseQ, CEUBot, and Differ are three additional examples of how chatbots may be used as helpers in the many other services that universities provide besides admissions and registration. LTKABot is intended for administrative activities, as well as to boost manual administration and support for relevant courses, and it is built on the ChatOps paradigm, which has the goal of automating education. Answering frequently asked questions about university communities, academic requirements from visitors, and other services is the purpose of the FAQs Chatbot. LibBot is a chatbot that provides information about library services and may be used in other libraries outside of the academic context. UCM3 Library Chatbot is a chatbot designed for libraries that requires particular computer science skills. It combines a mobile-friendly design with advances in usability to provide a better user experience. All of these chatbots fall under the category of service-oriented chatbots, which includes the majority of them [27].

To the best of our knowledge, the current research gap / problem is security issues relating to chatbots, which means secure chatbot have not been discussed or implemented. Because, like any other technology, chatbots do not come without drawbacks. Chatbots, even though they seem like something new, are built on technology that already exists and they are often incorporated into online websites as well as applications. As a result, they depend on the HTTP(S) protocol and other currently available communication protocols. If a chatbot fails to perform this function, data breaches may occur, compromising the user's privacy and possibly resulting in financial losses. In light of these considerations, it is quite probable that chatbots will become a target for attackers, where known vulnerabilities and assaults, such as cross-site scripting (XSS) and SQL injections, will be exploited by malicious actors. Because of this, while designing chatbots, it is unavoidable to address security concerns [26].

This review paper consists of sections. First Section I INTRODUCTION and the Second Section II is CHATBOT SECURITY RISKS. Third Section III is Related Work, Fourth Section IV is METHODOLOGY, and Fifth Section is DIFFERENTIAL ANALYSIS, Sixth Section is TENTATIVE PLANNING and final is CONCLUSION & FUTURE WORK.

II. CHATBOT SECURITY RISKS

Chatbot security risks can also be further broken down into two categories:

A. *Threats*

Threats are often characterized as several ways in which a system may be hacked. Malware and DDoS attacks are examples of one-time threats. Business-specific targeted attacks can lock you out of your system and hold you prisoner for ransom. Spoofing, tampering, repudiation, information disclosure, denial of service, and other incidents are examples of threats.

B. *Vulnerabilities*

Vulnerabilities are defined as a method by which a system is compromised and cannot be correctly and timely identified and resolved. When a system is not well maintained, has insufficient coding, is unprotected, or is prone to human error, it becomes vulnerable and susceptible to attacks. The most effective method of addressing potential vulnerability issues is to integrate SDL (Software Development Lifecycle) practices into development and deployment activities.

To ensure the security of chatbots, the bot creators must ensure that all security processes are in place and are accountable for restoring the architecture. Data flowing through the chatbot system should be encrypted both in transit and at rest.

III. RELATED WORK

In [2] Eleni Adamopoulou and et al, the objective of the research was to organize critical information such as the process of creating a chatbot, training a chatbot, connecting a chatbot to a channel, and the conversational mode of chatbots, etc., to understand and produce natural speech, and to observe the growing use of chatbots. Each type of chatbot is defined by a simple principle; a chatbot can belong to more than one category. There are two approaches to developing a chatbot, depending on the algorithms used: pattern matching and machine learning. Because privacy and data security must be maintained, especially in authentication and payment systems that access confidential, sensitive, or financial information, directed issues such as data security must be maintained. The main finding is that it points to a new direction that researchers should take in order to create chatbots with human-like speech.

In [3] Md. Saiful Islam Bhuiyan et al, the objective of the research was to integrate chatbots with Blockchain technology in order to increase chatbot security issues, handle sensitive data and tightly manage chatbot security and privacy and choose a well-established threat model known as STRIDE, which was developed by Microsoft and captures various security threats such as identity spoofing, data damage, information disclosure, and denial of service, and so on". The current proof-of-concept does not support transactions between multiple banks; however, this feature is easily added by adding additional chaincode for different banks and changing the logic and algorithms of the Decentralized Application (dApp); the current proof-of-concept trains the chatbot using a small dataset and only a few query languages.

In [4] Kshitija Shingte et al, the objective of the research was to help the students to know about the admission process, reduce the workload of admission process department, to develop a college enquiry chatbot, and also solves the students' or parents' queries quickly. The unique features of the research were college enquiry chatbot helps the students to get the right source of information and not only our chatbot but any chatbot will provide them with an instant as well as accurate response.

In [5] Fabian Schillinger et al, the objective of the research was to provide more or better security in Online Social Networks (OSNs) and to experience more secure & private communication. The main contribution of the research was that there are several different approaches for end to end encryption to improve the privacy, such as SAFESMS, None of Your Business (NOYB), FlyByNight, Off the Record, and Signal, etc. Additionally, it enables encrypted communication between multiple users concurrently, and the most critical point was that the system is not reliant on or dependent on third-party projects, does not use any other OSNs for message exchange, but is open source and utilizes the well-known RSA and AES encryption algorithms.

In [6] Surya Roca et al, the objective of the research was to create a handy tool to remind medication and to make a chatbot that support and provides different functionalities. The main contribution of the research was to make chatbot that provides very strict security measures to protect personal user information during message exchanges in healthcare scenarios to safeguard the user's privacy.

In [7] Pavel Smutny et al, the objective of the research was to investigate educational chatbots for Facebook Messenger that could be used to aid learning, and an independent web directory was also screened for chatbots, resulting in the identification of 89 unique chatbots. Each chatbot was classified according to its language, subject, and matter, as well as the developer's platform. The research's primary contribution was that they used the analytic hierarchy process to evaluate 47 educational chatbots on the Facebook Messenger platform against the quality attributes of teaching, humanity, affect, and accessibility, and discovered that educational chatbots on the Facebook Messenger platform can perform a variety of functions, from sending personalised messages to recommending learning content. The primary objective of this study was to advise teachers on how to integrate chatbots into classroom practise and which types of chatbots to experiment with.

In [8] Chinedu Wilfred Okonkwo et al, the objective of the research was to provide a comprehensive understanding of prior research on the use of chatbots in education, including existing studies, benefits, and challenges, as well as future research areas on the implementation of chatbots in education, as revealed by the articles selected for this study. The analysis concluded that a variety of factors, including ethical, assessment, user assertiveness, observation, and maintenance concerns, may influence the adoption and use of chatbots in education, and it attempted to suggest future educational areas that could benefit from chatbot use. The primary objective of this study was to conduct a systematic review of the existing literature on chatbot applications in education in order to gain a better understanding of their current state, benefits, limitations, and future prospects.

In [9] Lap-Kei Lee et al, the objective of the research was to create a chatbot capable of instantly responding to students' questions on a variety of popular social media platforms, including Telegram, Facebook Messenger, and Line. The research's primary contribution was that allowing students to ask questions during a university course is a critical aspect of learning because it results in increased learning efficiency while also increasing the workload of faculty. The research was unique in that the chatbot can respond to questions and commands in natural language once teachers upload course-related information to an online database, the chatbot can answer questions about course materials and logistics (e.g., class schedule), and the chatbot also includes a login system that enables it to provide answers based on different student profiles.

In [10] Abbas Saliimi Lokman et al, the objective of the research is to create a universal word embedding that is unaffected by the size of the vocabulary or the language used, to create a generative model that is both flexible and accurate in terms of conversational context, and to create a universal automated evaluation model that requires no or little human assistance in order to avoid human bias. The research's primary contribution is to provide a high-level overview of contemporary chatbot design practises and implementation strategies.

In [11] Tarek AIT BAHA et al, the main objective of the research was to develop a chatbot and to propose an Encoder-Decoder framework for intent detection. Using a bidirectional transformer, encode expressions as context representations for the encoder. Use an intent classification decoder in the decoder to detect the student's intent. The main contribution of the research was the intention to bring this model to the classroom as a tool to teach students as part of our teaching intuitive, which we also intend to implement in a number of institutions, enabling us to conduct preliminary validation of the Edu chatbot's functionality and benefits in the classroom.

In [12] Fabio Clarizia et al, the objective of the research was realization of a chatbot model in the educational domain: the goal has been to design a specific architecture, model to manage communication, and provide the right answers to the student. The main contribution of the research was that a chatbot system was developed that can detect questions and, using natural language processing techniques and domain ontologies, provide answers to students. The unique features was compared to other chatbots, student says that it is more simple and effective.

In [13] Anupam Mondal et al, the objective of the research was to develop a documentary communication application, namely a chatbot, in the educational domain, with the proposed chatbot assisting in the answering of user questions. The main contribution of the research was they prepared a training data set from the scuttled data, which contains approximately 1000 unique pairs of questions and answers, in order to concentrate on developing the chatbot in the educational domain and designing the chatbot.

In [23] Martin Hasal et al, the objective of the research was that a chatbot should be designed to recreate the pattern of human interaction via computers and the chatbot should be developed in a way that is cost-effective. Authorization and authentication, end-to-end encryption, and self-destructing communications were the most significant contributions made by the study. Authorization and authentication are required in order to determine that a user has been validated and has provided valid and secure login information. End to End Encryption implies that only the persons involved in the communication can read the messages, and Self Destructed Communications means that messages containing Personally Identifiable Information (PII) are automatically wiped after a certain period of time.

In [24] Bhavika R. Ranoliya et al, the objective of the research was to develop a chatbot that responds to any query in an efficient and accurate manner based on a FAQ dataset using Artificial Intelligence Markup Language (AIML) and Latent Semantic Analysis (LSA). The research's major contribution was to help the students in accessing information such as university ratings, service availability, university culture, and updates on events taking place on campus, and other academic information.

In [25] Naveen Kumar M et al, the objective of the research was to offer an educationally based chatbot for visually impaired individuals, as well as react to educationally based questions submitted by visually impaired persons. The research's key contribution was to supply every sort of information that is included in Wikipedia, as well as user-identical content and the ability for users to design their own queries and answers.

Table 1. Existing Approach Limitations

Author Name	Publication with Year	Methods Used	Limitations
Eleni Adamopoulou and et al [2]	Elseivier, 2020	Pattern Matching Approaches and Machine Learning Approaches	Producing and understanding natural speech
Md. Saiful Islam Bhuiyan et al [7]	IEEE, 2020	Blockchain - System chaincode and Bank Chaincode algorithms	Transactions between multiple banks are not facilitated by the current PoC
Lap-Kei Lee et al [15]	IEEE, 2020	DialogFlow with Firebase database	The evaluation has a small number of participants. Despite the fact that a focus group interview was conducted, these participants provided only limited information.
Gergana Vladova et al [14]	AIS, 2019	Natural Language	Participants can provide incorrect information by asking informal questions, which can lead to incorrect development of the learning avatar

IV. METHODOLOGY

There are many methods or techniques to secure a chatbot but in this paper will discuss about few of them which is used in references.

A. ENCRYPTION / DECRYPTION ALGORITHMS

i. AES Algorithm

The National Institute of Standards and Technology approved and published the AES encryption algorithm in 2000. (NIST). The AES encryption algorithm replaces the DES and Triple DES algorithms. AES is a symmetric key algorithm used to protect premium content from unauthorized users. Because of the symmetric key algorithm, the AES algorithm uses the same key for both encryption and decryption. It is based on two standard methods for encryption and decryption, known as the substitution and permutation networks. The AES will use a plaintext block size of 128 bits. Furthermore, these 16 bytes are expressed in a 4x4 matrix, and AES operates on byte matrices [15].

ii. DES Algorithm

The most widely used encryption method is based on the National Bureau of Standards' Data Encryption Standard (DES). DES uses a 56-bit key to encrypt data in 64-bit blocks. The encryption procedure includes two permutations, known as the initial and final permutations, as well as sixteen feistel rounds. In a sequence of stages, the algorithm converts a 64 bit input into a 64-bit output. Like any other function, the encryption function requires two inputs: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits long and the key must be 56 bits long. As with any feistel cipher, decryption uses the same algorithms as encryption, except that the subkeys are applied in the reverse order. The DES algorithm is suitable for use in a wide range of applications since it is both cost-effective and efficient at the operational level. DES has already been shown to be resistant to analytical attacks such as linear and differential attacks, as well as brute-force attacks. As a result, modifying a new form of DES has the potential to provide advantages in a variety of industrial settings. Triple DES (3DES) employs the Data Encryption Standard (DES) encryption algorithm three times each data block. 3DES uses three 56-bit DES keys for encryption and decryption, comprising 168 bits. When it was realized that a 56-bit DES key was no longer sufficient to defend against attacks. 3DES was chosen to expand the key space without changing the algorithm. A key size increase of DES is achieved by performing the method three times with different keys. The first key encrypts plaintext, and the second key decrypts it. “Triple DES was intended to increase the key size of DES to guard against such attacks without creating a new block cipher algorithm” [15] [16] [17].

iii. RSA Algorithm

The RSA algorithm is commonly used in the Public Key Algorithm. RSA was described for the first time in 1977. The RSA algorithm has three steps: key generation, encryption, and decryption. RSA is a cryptographic algorithm that is based on a public-private key system. While the public key is made available to everyone in order to encrypt data, it cannot be decrypted; only the owner of the private key has the ability to decrypt it. Because it is theoretically possible but extremely difficult to generate the private key from the public key, the RSA algorithm is a popular choice for data encryption [20] [21].

iv. Signal’s Double Ratchet Algorithm

The double ratchet algorithm is a session key management algorithm. This algorithm is used to provide End to End Encryption for instant messaging or live chat. The double ratchet algorithm was designed to provide forward secrecy as well as backward secrecy for post compromise security. It also has self-healing property for this attacker can’t crack all keys if one key is available. The whole idea is that it can re-generate a key anytime it wants using symmetric

AES 256 encryption. Double ratchet algorithm combines the functionality and properties of symmetric ratchet and the Diffie Hellmann ratchet.

B. ATTACKS ON CHATBOT

Chatbots are one such technology that has grown in popularity over the years. Artificial intelligence has not only reduced people's workloads, but it has also taken complete control of AI driving cars, serving food in restaurants, and so on. However, chatbots have drawbacks, particularly in terms of security. Even though there have not been many cases of chatbot attacks, there is a possibility that these AI-enabled bots could be used by hackers to carry out various types of cyber-attacks.

1) Man in the Middle (MITM) Attack

It is a type of attack in which the attacker intrudes into a conversation between a user and a chatbot in order to eavesdrop on or manipulate the conversation. MITM attacks are designed to steal information such as login credentials, account information, and credit and debit card numbers, which can then be used for a variety of purposes, such as unauthorised fund transfers or password changes.

2) Denial of Service (DOS) Attack

A denial-of-service (DoS) attack occurs when an attacker prevents a chatbot from providing service and responding to user inquiries. This is accomplished by limiting access to servers, devices, networks, and applications. DoS attacks are carried out by a single system that gains access to the bank's servers and networks, whereas DDoS attacks are carried out by a group of systems. For malicious purposes, hackers collect all personally identifiable information (PII) and sensitive information. It is common for DoS attacks to send a large number of large requests to a chatbot in order to intentionally destroy the chatbot's pool of resources. It is possible that genuine users will no longer be able to use computer resources in the future. To prevent DoS attacks, it is recommended that security testing be included in your continuous testing pipeline.

3) Script Based Attack

Cybercriminals benefit greatly from script-based attacks. The main reason for running scripts is that they are simple to write and execute. Script-based attacks, which are stored in the computer's memory, interfere with post-conversational analysis. These malicious scripts have the ability to easily collect user information, passwords, and other sensitive data, making this extremely vulnerable.

C. PARAMETERS OF ENCRYPTION / DECRYPTION

Encryption Time – The encryption time is the amount of time it takes an encryption algorithm to generate cipher text from plain text. The throughput of an encryption scheme is calculated using encryption time. The encryption scheme's throughput is calculated by dividing the total plain text in bytes encrypted by the encryption time.

$$cycles\ per\ byte\ = \frac{cycles\ per\ second}{speed} \quad \text{[eq.1]}$$

$$Time = \frac{data\ size}{speed} \quad \text{[eq.2]}$$

The encryption time is expressed in milliseconds and is determined by the message block's size and the key's size. It has a direct impact on the performance of the encryption algorithm. To make the encryption scheme responsive and fast, each cryptographic algorithm requires a minimum encryption time.

Decryption Time - The time required to recover plaintext from cipher text is referred to as decryption time. To make a cryptographic algorithm fast and responsive, the decryption time should be measured in milliseconds, just like the encryption time.

Key Space - Key space is a set of all valid possible separate keys for a given cryptosystems. The security of a cryptosystem is relative to the size of the key space. An intercepted message with a bigger key space will be more robust to decryption attempts by attackers, since an attacker would attempt to brute force the message with all feasible key combinations if the key space is greater. For example, the key space of an encryption system might include anywhere from a small number of combinations to millions. The greater the amount of possible permutations and combinations, the more secure the encryption mechanism.

Memory Used - The size of memory is determined by the implementation of various algorithms. The amount of memory required is determined by the key size, initialization vectors, and type of operation. It is preferable to have a small memory size because it affects the system's cost.

Time & Space Complexity – An algorithm's time complexity captures how long it takes to execute as a function of input length. Hardware, operating systems, and processors, among other things, influence cryptographic time complexity. The time complexity of an algorithm is commonly expressed using asymptotic notations: Big O is denoted as O (n), Big Theta is denoted as (n), and Big Omega is denoted as Ω (n).

Throughput - Divide the total block size (Mega Byte) encrypted by the total encryption time to calculate the encryption algorithm's throughput. The algorithm's power consumption decreases as the throughput value increases. The throughput of encryption and decryption techniques is computed, however each scheme is done one at a time [18] [19]. Encryption scheme throughput is calculated as:

$$Throughput\ = \frac{average\ of\ total\ plain\ text\ in\ k\ bytes}{average\ encryption\ time}$$

Decryption scheme throughput is calculated as:

$$Throughput = \frac{average\ of\ total\ cipher\ text}{average\ decryption\ time}$$

V. TENTATIVE APPROACH

The Modified Double Ratchet algorithm's main idea is to change keys for each message. It is capable of achieving security properties such as Resilience. Forward secrecy means that if future keys are compromised, the current key will remain secret, whereas backward secrecy means that if post keys are compromised, the current key will remain secret. Fig 2 shows working of the Modified Double Ratchet algorithm and the participants' following actions:

1. Bot wants to send Initial message to N-user and then it generates a private key while N-user will generate public key.
2. Bot's output (Key) uses as input of Key Distribution Function (KDF).
3. Then Bot gets a new key for the root chain and key for the sending chain. This process will continue. And here the sending chain will also get encrypted using Paillier Cryptosystems.
4. After the sending chain is encrypted, it will generate a message key for the initial message.

5. Bot encrypts messages using the message key. And then Bot will send encrypted message to the N-User.
6. N-user receives the encrypted messages which is sent by the Bot and wants to decrypt it.
7. Then N-user launches his private key and tells Bot to send his public key.
8. Afterwards, N-user will also get same output as Bot.
9. N-user uses the Output as the input date for KDF and makes a new key for receiving chain and root chain. Notice here receiving chain will be encrypted not the original one.
10. N-User receiving chain will get decrypted using Paillier Cryptosystems and then makes a new message key.

The Paillier cryptosystem is based on the computationally difficult task of calculating the nth residue class. Once the code has been decrypted, the nature of the method allows homomorphic addition operations to get the current answer.

Paillier cryptosystem encryption algorithm Encrypt a message M where $M \in \mathbb{Z}_n$.

1. Select r as a random integer where $r \in \mathbb{Z}_n^*$
2. Calculate $c = g^m \times r^n \bmod n^2$

Paillier cryptosystem decryption algorithm

1. Decrypt a message c where $c \in \mathbb{Z}^*{}_{n^2}$
2. Calculate $m = L(c^\lambda \bmod n^2) \times u \bmod n$

11. After generating message key N-user will decrypts the message using KDF.

Save three key chains: root chain, sending chain and receiving chain.

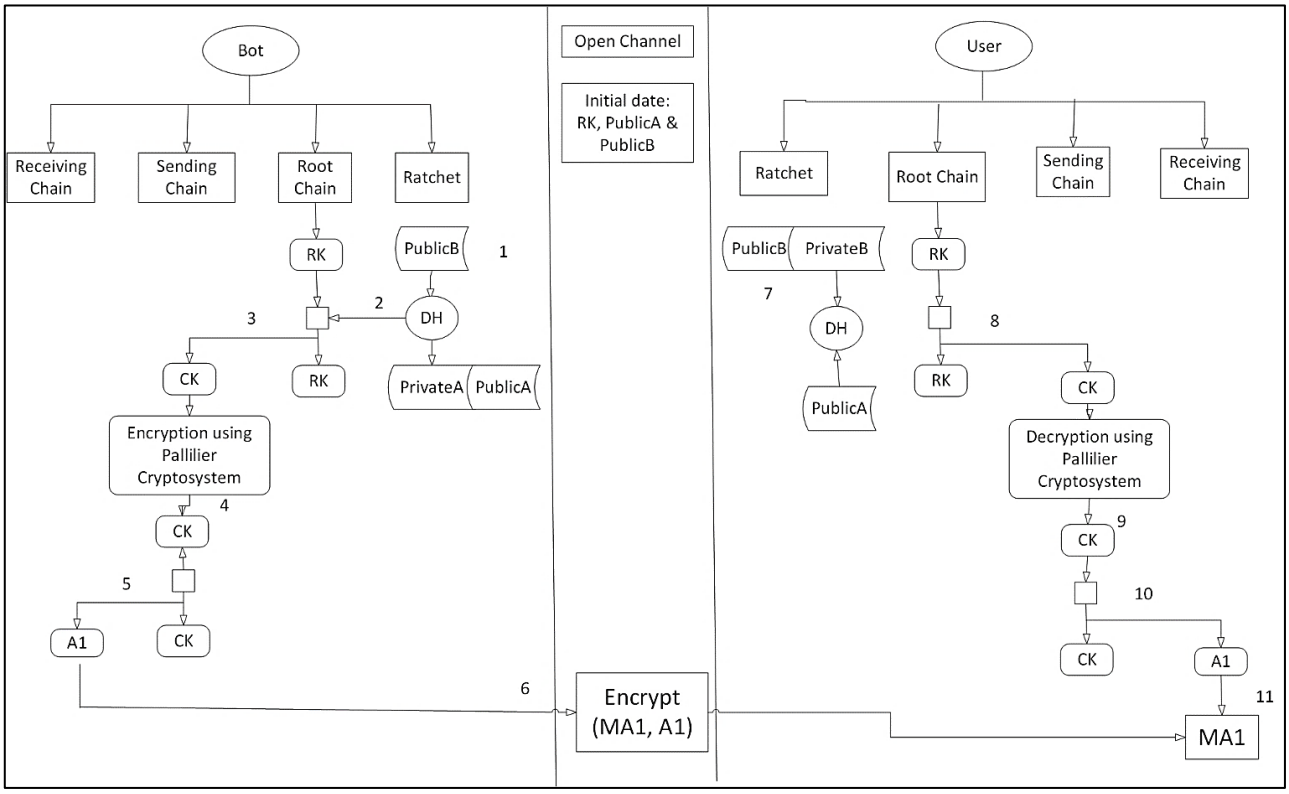

Fig 2. Modified Double Ratchet Algorithm

CONCLUSION & FUTURE WORK

End to End Encryption and Authentication (Session) Timeout plays a very significant role in securing a chatbot. This review was mainly focused on how to secure chatbots in educational institute. However, this techniques can be applied to a wide range of chatbots that are available for various sectors or enterprises, such as Healthcare, Ecommerce, Financial, Retail and many more. Chatbot developers, particularly those developing chatbots for the financial industry as well as for educational institutions, should be aware of the importance of privacy and security. When these built-in security measures are combined with basic user security precautions, chatbots provide both strong security and ease of access. This allows businesses to provide the best possible customer experience while employing the most up-to-date security measures. The objective of secure chatbot is to make a chatbot in such a way that the entire conversation will remain secure and to protect data against cyber criminals or hackers.

The future work is the message should also get encrypted two times to better increase the security. Let's take an example to better understand how to implement two times encryption. If message is sent as X, it will become Y after the first encryption then again it will become Z after the second encryption and on the server side Z will be decrypted and become Y, then Y will be decrypted and become X, and then process X generates a response.

REFERENCES

[1] C. W. Okonkwo and A. Ade-Ibijola, "Chatbots applications in education: A systematic review," *Comput. Educ. Artif. Intell.*, vol. 2, p. 100033, 2021, doi: 10.1016/j.caeai.2021.100033.

[2] E. Adamopoulou and L. Moussiades, "Chatbots: History, technology, and applications," *Mach. Learn. with Appl.*, vol. 2, no. November, p. 100006, 2020, doi: 10.1016/j.mlwa.2020.100006.

[3] M. S. I. Bhuiyan, A. Razzak, M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and S. Tarkoma, "BONIK: A blockchain empowered chatbot for financial transactions," *Proc. - 2020 IEEE 19th Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2020*, no. November, pp. 1079–1088, 2020, doi: 10.1109/TrustCom50675.2020.00143.

[4] K. Shingte, A. Chaudhari, A. Patil, A. Chaudhari, and S. Desai, "Chatbot Development for Educational Institute," *SSRN Electron. J.*, 2021, doi: 10.2139/ssrn.3861241.

[5] F. Schillinger and C. Schindelhauer, "End-to-End Encryption Schemes for Online Social Networks", *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, pp. 133-146, 2019. Available: 10.1007/978-3-030-24907-611.

[6] S. Roca, M. Hern´andez, J. Sancho, J. Garc´ıa and ´A. Alesanco, "Virtual Assistant Prototype for Managing Medication Using Messaging Platforms", *IFMBE Proceedings*, pp. 954-961, 2019. Available: 10.1007/978-3-030-31635-8116.

[7] P. Smutny and P. Schreiberova, "Chatbots for learning: A review of educational chatbots for the Facebook Messenger," *Comput. Educ.*, vol. 151, no. February, p. 103862, 2020, doi: 10.1016/j.compedu.2020.103862.

[8] C. W. Okonkwo and A. Ade-Ibijola, "Chatbots applications in education: A systematic review," *Comput. Educ. Artif. Intell.*, vol. 2, p. 100033, 2021, doi: 10.1016/j.caeai.2021.100033

[9] L. K. Lee, Y. C. Fung, Y. W. Pun, K. K. Wong, M. T. Y. Yu, and N. I. Wu, "Using a Multiplatform Chatbot as an Online Tutor in a University Course," *Proc. - 2020 Int. Symp. Educ. Technol. ISET 2020*, pp. 53–56, 2020, doi: 10.1109/ISET49818.2020.00021.

[10] A. S. Lokman and M. A. Ameedeen, "Modern chatbot systems: A technical review," *Adv. Intell. Syst. Comput.*, vol. 881, no. 3, pp. 1012–1023, 2019, doi: 10.1007/978-3-030-02683-7_75.

[11] T. A. I. T. Baha, M. E. L. Hajji, Y. Es-Saady, and H. Fadili, "Towards highly adaptive Edu-Chatbot," *Procedia Comput. Sci.*, vol. 198, no. 2018, pp. 397–403, 2021, doi: 10.1016/j.procs.2021.12.260.

[12] F. Clarizia, F. Colace, M. Lombardi, F. Pascale, and D. Santaniello, *Chatbot: An education support system for student*, vol. 11161 LNCS. Springer International Publishing, 2018.

[13] A. Mondal, M. Dey, D. Das, S. Nagpal, and K. Garda, "Chatbot: An automated conversation system for the educational domain," *2018 Int. Jt. Symp. Artif. Intell. Nat. Lang. Process. iSAI-NLP 2018 - Proc.*, 2018, doi: 10.1109/iSAI-NLP.2018.8692927.

[14] G. Vladova, J. Haase, L. S. Rüdian, and N. Pinkwart, "Educational chatbot with learning avatar for personalization," *25th Am. Conf. Inf. Syst. AMCIS 2019*, no. Weizenbaum 1966, pp. 1–5, 2019.

[15] A. Adil Yazdeen, S. R. M. Zeebaree, M. Mohammed Sadeeq, S. F. Kak, O. M. Ahmed, and R. R. Zebari, "FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review," *Qubahan Acad. J.*, vol. 1, no. 2, pp. 8–16, 2021, doi: 10.48161/qaj.v1n2a38.

[16] S. R. M. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 2, pp. 774–781, 2020, doi: 10.11591/ijeecs.v18.i2.pp774-781.

[17] R. V. Amorado, A. M. Sison, and R. P. Medina, "Enhanced Data Encryption Standard (DES) algorithm based on filtering and striding techniques," *ACM Int. Conf. Proceeding Ser.*, vol. Part F148384, pp. 252–256, 2019, doi: 10.1145/3322645.3322671.

[18] Latika, "Encryption Techniques-Study & Comparison," *IJSTE - Int. J. Sci. Technol. Eng. | Vol. 1 | Issue 11 | May 2015*, vol. 1, no. 11, pp. 299–303, 2015.

[19] Gurjeevan Singh, Ashwani Kumar Singla, and K.S. Sandha, "Through Put Analysis of Various Encryption Algorithms," *Int. J. Comput. Sci. Technol.*, vol. 2, no. 3, pp. 527–529, 2011.

[20] R. I. Emori, "Scale models of automobile collisions with breakaway obstacles - Investigation indicates that scale models can be used to show the motion of breakaway signposts and lightposts after being struck by automobiles," *Exp. Mech.*, vol. 13, no. 2, pp. 64–69, 1973, doi: 10.1007/BF02322384.

[21] Abhishek Guru, Asha Ambhaikar, "Development of "RSA" Encryption Algorithm for Secure Communication," *International Journal of Computer Sciences and Engineering*, Vol.7, Issue.6, pp.581-585, 2019.

[22] V. Patel, D. Kapadia, D. Ghevariya, and S. Pappu, "All India Grievance Redressal App," *J. Inf. Technol. Digit. World*, vol. 2, no. 2, pp. 91–99, 2020, doi: 10.36548/jitdw.2020.2.002.

[23] M. Hasal, J. Nowaková, K. Ahmed Saghair, H. Abdulla, V. Snášel, and L. Ogiela, "Chatbots: Security, privacy, data protection, and social aspects," *Concurr. Comput. Pract. Exp.*, vol. 33, no. 19, pp. 1–13, 2021, doi: 10.1002/cpe.6426.

[24] B. R. Ranoliya, N. Raghuwanshi, and S. Singh, "Chatbot for university related FAQs," *2017 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2017*, vol. 2017-Janua, pp. 1525–1530, 2017, doi: 10.1109/ICACCI.2017.8126057.

[25] M. Naveen Kumar, P. C. Linga Chandar, A. Venkatesh Prasad, and K. Sumangali, "Android based educational Chatbot for visually impaired people," *2016 IEEE Int. Conf. Comput. Intell. Comput. Res. ICCIC 2016*, pp. 0–3, 2017, doi: 10.1109/ICCIC.2016.7919664.

[26] J. Bozic and F. Wotawa, "Security testing for chatbots," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11146 LNCS, pp. 33–38, 2018, doi: 10.1007/978-3-319-99927-2_3.

[27] J. Q. Pérez, T. Daradoumis, and J. M. M. Puig, "Rediscovering the use of chatbots in education: A systematic literature review," *Comput. Appl. Eng. Educ.*, vol. 28, no. 6, pp. 1549–1565, 2020, doi: 10.1002/cae.22326.