Built-in translation on Web Messenger

U Karthikeyan¹, A Ajit Surya², S Bhargav³ and P Bhargav⁴
¹Associate Professor, ²³,4Under Graduate Students, Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai-602105,INDIA
karthikeyan.u@rajalakshmi.edu.in, ajitsurya.a.2015.cse@rajalakshmi.edu.in, bhargav.s.2015.cse@rajalakshmi.edu.in,bhargav.p.2015.cse@rajalakshmi.edu.in

Abstract. The paper aims at providing the users with a web messenger application that translates messages sent by sender to the receiver. The translation is provided by Google Translate API. This helps in having a seamless conversation experience. Any language that is supported by Google Translate can be sent and received by the users. It is planned to provide transfer of graphic files as well as other file types. Interestingly, this method of communication is the most popular form. Encryption and Decryption is provided by employing AES Algorithm function set. The encryption and decryption make it safe for communication by protecting the conversation from outside threats. In order to have a conversation between two people normally in their own preferred language, they have to rely on using Google Translate solely by copying the message text and finding the translation. This web application we have proposed combats that problem by providing simultaneous translation of text messages to the user’s preferred language. Languages that can be translated are the same as what Google Translate provides. ISO 639-1 language codes are used as language code by the sending entity to send the data to the receiving entity. Accuracy have been identified as same as what Google Translate provides, above 60%.

1. Introduction

1.1 Communication Strategy

Communication has been focused on the exchange of messages between the end users. A process has to anticipate the meanings of the messages and should be understood by the recipients. Eventually, a co-ordination is required for the activities among the components that could be performed between the sender and receiver which further depend on the active and passive mode of stages. A sender who sends the message or information with some symbolic notations which give a meaning of the entire messages like audio or text data objects that are mostly social relevance. The receiving entity who receives the message could be known to identify and understand the semantics of the message with which it has been sent with symbolic pattern on the relevant domain and thus inter process communication is being involved in the entire process.

Across the world, the small and large organizations are in need of various possible approaches to run the business in an effective way and yield a profit on the product or software with available components and data for what it has been marketed. The manufacturing cost of such component and processing would certainly be less and its serviceability where it is dependent could be continued for further operation on the design of product or program. With the advent of recent technology, business-to-communication approaches are mainly handled on the internet and communicated with telecommunication network among the customers and the business people. The web services are provided to the users where they can access the resources at any time and at any places across the network.

As communications are essentially with the internet connectivity, the people can exchange the messages based on the peer-to-peer network as relevant to the social networks. On the social networking perspective, the message are communicated in terms of chat messages, communication via
phone call, exchange of message with video application and with a string of characters with the text object to be passed between the entities. These modes of communication are prevailed in an online platform that makes a simplest form of transmission of data with a less amount of time at a faster speed through the medium of network with different locations. Moreover, the scalability is an essential challenge in the distributed environment for the exchanging process where the performance could be improved at a better rate.

The work have bring out the working scenario on providing a means of communication where the sender and receiver can communicate in their own regional/native language with the messenger application proving a translation to their preferred language from the source language. A registration with the web application is required by both the sending and receiving processes to make use of accessing the data or resources on the end systems. Also, privacy is attained by employing encryption/decryption technique with “Advanced Encryption Standard” algorithm being used for the purpose.

Language is the key and main component of communication. Language is the way to express ourselves in verbal form or in written form. Language can also be a barrier when people of different regions try to communicate. Hence the need for a translator is very much needed to enable smooth and reliable communication.

2. Related Works
Charu, Amrita and Nisheeth[1] made a study of two ridges: Firstly, the concepts of Fuzzy Logic should be known at the initial phase and it should be integrated with an intelligent agent for computation on the collected data to get a better decision. Secondly, with the current challenges it could be processed with the mostly used domain Natural Language. The techniques are involved in most of the applications such as the translation of languages, searching of a keyword in terms of query in the searching engines. Today with the latest processors with high end configurations will perform a number of tasks as such an example on translation of sentences within the computer system itself. The concepts of Fuzzy Logic have indulged in predicting the answers for the query or questions with intelligent based reasoning system. The modular designs of Fuzzy Logic are more in transparency and provide interoperability functions. The combination of techniques like Natural Language Processing and Fuzzy ideas thus acquires drastic changes on the outcome that are being executed from the gathering of scientific applications.

Dimas, Faisal and Dewi[2] The study was provided the means of ECC algorithm that were used to afford a security on transmitting a message on a smart phone applications. They adapt the mechanisms which were designed by Singh on establishing a chatting operation with an encryption process in a program that uses the Android platform which were fully set up a reliable communication. ECC, AES, RC4 is implemented in Android Messaging App. ECC algorithm is used for end-to-end encryption. They had 100% accuracy with their results. A sample of 6000 characters from the collection of datasets with a character size of 5.85 KB of each has been evaluated and performances have been improved in an aggressive manner on the two parameters time and certainty. On observation, the use of ECC Algorithm on the Android Application required an optimization technique, thus leads a preferred output.

Kushboo, Umit, Temilola and Chi [3] The author have discussed with a method in examining the embedded scripts and styles for achieving the priorities given to the type of devices as Android devices. With the run of ‘dd’ command, the image style of the given device could be captured. They have been methods focussed particularly on further development on processing with social networking application such as WhatsApp. The purpose of the review work was on searching the exact locations where the data has been placed on various applications of an Android phone. The output what it has
been attained from the distributed files such as We Chat and Viber which were then used the encryption technique. The files could be extracted from the directory path of the mobile phone. On the other side, the WeChat database file employed the decryption technique with the availability of encryption key that were accomplished through IMEI number of specified android phone. Another instant messaging application, Telegram has given a safer use of environment when compared with the other applications. It was noticed that not knowing the encryption key it was not possible for the extraction of the decrypted form of chatting files from the database.

Puneet, Grover and Laxmi[4] The author have dealt with three primary conditions for the access of any applications that were related to the chatting strategy in the security perspective. The primary security factors include Confidentiality, Integrity and Availability. The factor Confidentiality impact on the category of messages that can be exchanged only with the authenticated people. Integrity encompasses the transferred messages can be corrected exclusively by the people who have given authentication. Availability has shown the interoperations on the messages to the authenticated people at a certain time. It should be noted the security forms on the type of application what it has being selected as in terms of Instant Messaging. The message, the type of file and Cipher keys that can be exchanged between the entity programs should be encrypted that leads to security enhancement. Over the advancement of the mobile application platform, each stage have to provide a good mark on the type of application. On the developer’s aspects, it is in need of a model to test driven the applications based on customized security principles. The paper work emphasized on the latest security advancements used in the Instant Messaging application and about the improvement on performance when used with these type of applications on end devices.

Chandrasekhar and Jogalekar[5] study the web chat applications with its performance measurement parameters. The internet has been used by more number of people across the world on a large scale and an average person consume the internet facilities are nearly 12:11 minutes on each day. The services as by means of reply should be provided to the user with the powerful tools needed for processing on the availability of data with certain practices needed to deliver. As the client has to wait for a reply from the server, the web related utilizations are more common. With the application layer, the e-mail messaging system is another determined two way communication across the network. The paper have discussed the e-mail system with a large number of servers that can be operated on different machines through the network. The exclusively used protocol on e-mail messaging system is Simple Mail Transfer Protocol where agent is to communicate with the sender and receiver on the exchange of messages on the server. The other server which would be focused on Internet Message Access Protocol server which contains the repository of messages relevant to the mail program. The application Instant messaging roll out the transmit of chat information among the end users over a communication medium. Certain factors have been put forth on the paper which was increase of users on accessing the same resources by virtue of scalability, the delay occurred for the entire transmission of chat data, leakage of private data from the memory of the system. A research survey have been taken in a chat which was on a live pattern on different parts and further analyzed with the prediction of some issues that have been identified and required to be solved The supportability in online platform would be catered to the customers by the small and large enterprises that give the rise on performance basis and consumes less amount of time when work out on the online mode.

SaifAbdulwahed[6] says that web-based translation such as Google Translate has enabled communication across language barriers. The aim of this is to identify, describe and classify types of errors produced when translating authentic texts from Arabic into English. Google Translate refers to online system of Machine Translation that translates texts from one source language to its equivalent in the Target Language. The methodology and algorithms used are Google Translate using Black Box approach. This method says that the system gets more intelligent as it gets older i.e. improvement by
Syntactic and grammatical errors can be viewed which shows that there is still some progress required to fully replace human translators.

Katriel, Cramers, Luke, Jon and Kevin [7] provide a entirely synchronous hierarchical tree like structure GKE protocol that hit the latest security means called ART. They provide game like structure on the security design which was based on computation for the build of protocol on various stages to set the different data. It has been provided a validation of approach on the Java implementation of ART’s essential algorithms that have been employed, thus improve the overall design. Security properties called PCS have been used in the work. It was observed with a new design called ART has been employed. Their standard operations could be performed from the type of algorithm used, enclosed in the file ART.java whereas the remaining files were generally equip the necessary container and service styles. With the cryptography technology, the papers have used the Diffie-hellman security mechanisms they used a Java run of Curve 25519. The use of the techniques like Encryption and Decryption on the transfer of message includes the Java’s native AES-GCM. Their resulting (ART) design incorporate the utilization of messages exchanged in a group with an acknowledgement of delivery data as message on the latest end-to-end protocols used across the communication network.

Heather Kelly [8] makes a study on the SMS and its growth throughout the years. About six billion SMS data are exchanged on each day in the country United States, As per the record from Forrester Research and it has been estimated that over 2.2 trillion messages were exchanged in a year. On further estimation about the transfer of text messages from Portio Research, around 8.6 trillion of text data types of messages were transported on each year. It is perhaps 190 characters were used for the messages that were being directed across the underlying network communication. The latest communication on the way of text data type message were at the point the data can be transported i.e., pervasive.

3. Experimentation and Results

The proposed system is a web application that has the feature of translating the text messages from one language to another. The sender may communicate in a language which may not be known or understood by the receiver or vice versa. Hence the project is developed using a translator so that the user can send text messages in their preferred language while the receiver can receive and view the messages in their preferred language, thereby ensuring ease of communication. The user registers with the application using their Email ID and then proceeds to login. After logging in, the user can send messages to the receiver using their Email ID. While send the text message of desired language, a language code has to be entered to provide translation to the receiver. The user can log out after their messaging session.

3.1 AES Algorithm

The widely used encryption algorithm on the security concerns of data transportation in the cryptography is Advanced Encryption Standard (AES). The algorithm AES has a better performance on the encrypt part of message transmission than other standard say Data Encryption Standard. A change over for DES encryption standard was required since the encryption key capacity was limited. With the rise in power computation, it was spotted suspect opposed to various types of attacks in accordance with the key search. DES algorithm can be used for these types of attacks but it was in very slow process.
3.2 AES Analysis
On the current scenario of the security communication with respect to cryptography, AES is mostly accepted standard which further stayed with the components of hardware and software. It is then evidenced that there would not any cryptanalytic attack against the standard of Data Encryption Standard. Eventually Advanced Encryption Standard has implanted features of resilience of length in view of key and made a good performance on search in relate with key.

3.3 Modules
3.3.1 User Sign up/Sign in
It makes an allow of a user to login with web application using credentials such as email and password. The user also creates a unique ID which will be used for the purpose of message to be typed on the text space. The inputs for the given module are User ID and Password. The User ID and password are thus entered in the respective fields and it should be matching with what it would available in the database for further authentication and approval.

Figure 2 Sign In Pattern

Figure 3 After Sign Up Pattern

3.3.2. Sending Message
The module have allowed on sending a message from one user to another user. The inputs which would be given in the module are text message, recipients or receiver’s email and preferred translation language code. Eventually, the text message are exchanged from the server program to the client program as user and then transported to the recipient.

Figure 4 Sending Message Pattern
3.3.3. Receiving Message
The module has shown that the message that has been exchanged by different users is being received by the receivers in their preferred language based on the language translation. The output of the module has been specified as a translated text message (language) pattern.

![Figure 5 Receiving Message Pattern](image)

3.3.4. Encryption
The message is being protected with encryption technique which encompasses the original message. The text that has been sent by the user would be the input of the module. Encryption algorithms could encrypt the message using a private key which could be made decrypted by the receiver side client. The type of encryption algorithm that have used on this module would be AES.

![Figure 6 Block Diagram for a message which is being encrypted from sender to receiver](image)  

3.3.5. Decryption
The module have shown that the receiver would received the original message as a plain text message based on decryption techniques. The input of the module has been identified as an encrypted message. The encrypted message thus make a decryption using AES Algorithm. The decrypted message which made conversion from cipher text to plain text, would be an output.

![Figure 7 Block Diagram for a message which is being decrypted from sender to receiver](image)

4. Conclusion
The paper provides a platform for communication with people in a language that the users prefer. Data privacy is provided by employing encryption and decryption functions of AES algorithm. It mainly focuses on managing time efficiently and providing better service to the users. Any software is built for end user satisfaction; our system focuses in achieving this goal.

It is not feasible to design a computing system that forms the demands of the end users. The end users fundamentals are in ad-hoc pattern with respect to the computing system that is being utilized for various applications. The enhanced future work of this paper are enlighten with the following factors
namely upgrade versions of the built in systems that are to be designed and should be suited to the surrounding platform such as the use of intelligent bot which decipher the conversional talk or messages, enhancement features of security related issues and security improvisation with the share of data in terms of files and graphical data objects.

References
[1] CharuGuptaa, AmitaJainb 2018, Proc. ICCIDS Vol. 132, 1375
[2] Dimas Natanaela, Faisala, DewiSuryanib 2018, Proc. 3rd International Conference on Computer Science and Computational Intelligence Vol. 135, 283
[3] KhushbooRathi, UmitKarabiyik, TemilolaAderibigbe, Hongmei Chi 2018, Proc. 6th International Symposium on Digital Forensic and Security (ISDFS) 165
[4] Puneet Kumar Aggarwal, P.S. Grover, LaxmiAhuja 2018, Proc. RAETCS 91
[5] Dandane Tejas Chandrashekhar, U. A. Jogalekar 2015, International Journal of Engineering Sciences & Research Technology, Vol. 4, 300
[6] SaifAbdulWahed Jawad Alabaeeji 2018, Sino-Arabian Cultural & Economic Association
[7] Katriel Cohn-Gordon,CasCremers,Luke Garratt, Jon Millican,Kevin Milner 2018, Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS) 1802
[8] https://edition.cnn.com/2012/12/03/tech/mobile/sms-text-message-20/index.html
[9] Soheila Omer AL Faroog Mohammed Koko, Dr.Amin Babiker A/Nabi Mustafa 2015, IOSR Journal of Computer Engineering (IOSR-JCE) Vol.17, 62
[10] Milam Aiken 2019, Studies in Linguistics and Literature(SLL) Vol.3, 253
[11] Margaretha Ohyver, Jurike V Moniaga, Iwa Sungkawa, Bonifasius Edwin Subagyo, Ian Argus Chandra 2019, Proc. (ICCSCI) Vol.157, 396