A Chabot Supported Secured Portal for Affordable Artificial Limbs

N. Krishna Chythanya[1*], *D.* Tanusha[1], *Y. Hema* Rishitha[1], *M.* Pooja[1] *and N.* Anitha[1]

[1]Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India.

Abstract. In the last few years, there has been much demand for artificial limbs. Artificial Limbs Manufacturing Corporation of India has announced that 42 million people require artificial limbs. There are 12 million people who are suffering from limb loss and 40,000 amputations are performed in a year in India. The New Indian Express has published in 2022 that, approximately 25 leg amputations are performed each day in Kerala. The demand for artificial limbs has also raised issues such as, will the products be delivered fast, are they cost efficient, and whether customized products are available. Protecting the buyer's credentials and answering to their queries is essential. So, in order to overcome these issues, this research aims to build a website which acts as an intermediate between the buyers and manufacturers. The website is a one-step solution for the buyers where they can identify different manufactures by securing their data. Buyer's privacy can be achieved by safe-guarding all the passwords using SHA-256 algorithm. The chatbot can be used as a user-friendly mode to clarify the buyer's doubts about the products. Review and rating about the products are also described to achieve customer's belief.

Keywords: Artificial Limbs, chatbot, SHA-256 Algorithm, Prosthetics

1. Introduction

As technology has progressed, there have been a lot of contributions made in the medical world. One such significant contribution is artificial limbs. Artificial limb is a device that replace a missing hand or leg. The reasons like circulation problems from atherosclerosis or diabetes, traumatic injuries including traffic accidents, military combats and birth defects are the major reasons for the people to use these artificial limbs. There have been many improvements in these artificial limbs like robotic prosthetics, which are same as normal limbs but operated with the person's thoughts. There are many artificial limbs whose cost ranges from Rs.50,000 – Rs.1,00,000 which all people cannot afford to buy. There are vendors who are providing "Jaipur foot" for free such as Bharat Vikas Parishad, etc. Jaipur foot has benefited lakhs of people. There are many organizations like Bhagwan Mahaveer Viklang Sahayata Samiti, an NGO which is trying to improve the Jaipur foot in order to help most of the common people. All these advancements are happening but still the people are not aware of these artificial limbs. This is the main reason where most of the needy fail to buy the products and decide to continue their life with missing parts.

*Corresponding author : kcn_be@rediffmail.com

2. Literature Study

The observations made in the literature study are given below with respect to each work is done.

In work [1], the technical changes made in the features of artificial limbs are mentioned. The reasons for the demand of the artificial limbs and their uses are mentioned. The causes for the amputations and their impact on the common people are focused. The researchers have collected the information from various hospitals and gathered the information about the reasons, that people are facing while using these artificial limbs. The conclusion of this work is to provide people with comfortable, efficient, and budget friendly artificial limbs than the earlier versions. The people who are having lower limb amputations will struggle high with many issues compared to other people [2]. This research mainly dealt with the issues when the people with lower limb amputations fail to properly communicate with prosthetists. The aim of this work was to increase the communication between the amputated patients and prosthetists by providing clear prescriptions to the patients. More prosthetics options must be provided by the doctor which avoids the patients to search for the products.

To facilitate users with easy interaction, a chatbot is always helpful hence different works on building chatbots have been explored. The major focus of the work [3] was to implement various types of chatbots and to identify their problems while deploying. The chatbots mentioned in this work are rule-based chatbots, self-learning chatbots. The chatbot frameworks and platforms are clearly mentioned. The drawback of rule-based chatbots is, it only deals with straight forward questions but not the complex crucial questions and self-learning chatbots must be trained more to give relevant answers. Most of the times this chatbots are giving irrelevant answers, which is causing trouble to the users. Though, rule-based chatbots are having certain drawbacks, most of the businesses and industries are using rule-based chatbots. The result of this work was to create a voice-based chatbot which can be efficiently used in websites. Influence of the rating system on the users in the website is mentioned in [4]. The types of rating systems along with their impact on the website is focused. The evaluation of rating system is done based on their advantages. five-star, binary-visual and binary-textual rating systems are mentioned. This work says that, five-star rating is the efficient rating that can be used in the websites. five-star rating makes the users to provide the rating easily than other rating systems. Using five-star rating, the product evaluation can be done easily. Keeping the advantages in view this work is considered to implement five-star rating system. When the data is being shared on to websites, the security measures are required to safe guard the data. The SHA-256 algorithm is used to maintain security for the private data. This algorithm can be used for saving the data from the third-parties. Unlike, other algorithms that are used for security, the SHA-256 algorithm cannot be broken. That is the passwords that are saved in the intermediate form make the hackers impossible to crack them. The most important feature of SHA-256 algorithm is that, the hash values that are stored cannot be used to form the original message. The SHA-256 algorithm can be used for password verification, to identify the integrity of the data that is transferred. The SHA-256 algorithm is used in [5], to secure important details such as username, credentials, messages, pin number etc. Since the data can be stolen from the server node, the data that is being received to the server from the client node is saved using the SHA-256 algorithm.

3. Proposed Idea

The proposed idea is to develop a website which provides information about affordable artificial limbs. This website shall provide all the categories of artificial limbs related to

hands and legs. The manufacturer shall communicate with the admin for updating the products in the website. The user can search for categories of artificial limbs. Once the order is placed the manufacturer shall update the order status. The buyer shall upload the doctor's prescription before placing the order. This website shall provide both Cash on Delivery and online payment options. A chatbot makes a website more efficient and increases the interest for users to buy the products. So, including chatbot about artificial limbs will make the website handy for the users. This website shall also provide user-friendly modes such as review and rating of the products, feedback about the website which helps the buyer to buy the products confidently. This website ensures the buyers and manufacturers security by encrypting the login passwords through SHA-256 algorithm which converts the passwords into hash code.

4. System Architecture

The website has the information about products of artificial limbs. When the buyer and manufacturer logins into the website, their private information like password is secured using SHA-256 algorithm. Once the data is encrypted, it cannot be decrypted until the hash function is known to the attacker.

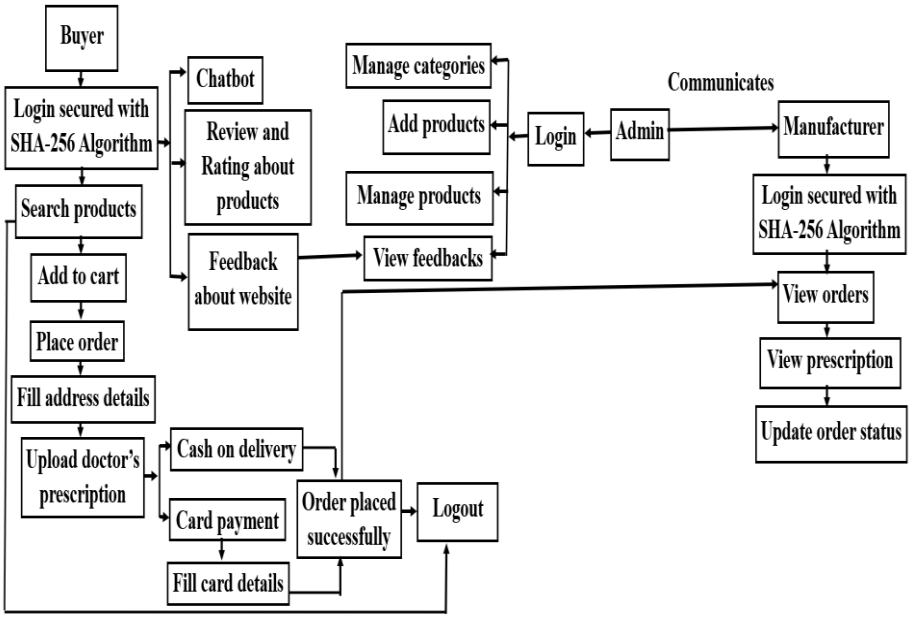

Fig. 1. System Architecture.

The admin needs to communicate with the manufacturer to identify the different types of artificial limbs that they are providing as shown in figure 1 . The admin is responsible for managing the categories where we need to add the types of limbs we are providing and add, manage products where the admin uploads and updates about the product details that the manufacturer is providing.

The manufacturer logins into the website to identify the orders that are being placed by the buyer. Here, the manufacturer is responsible to view the prescription that is uploaded by the buyer. He also needs to update the order status which can be seen by the buyer. The buyer can either login or can register into the website to search for the desired product(s). Once the required product is identified, the buyer can add the product to the cart and place order. The buyer needs to fill the details about address, then the buyer needs to upload the

doctor's prescription. The website provides payment options such as Cash on Delivery and Card Payment. Once the payment mode is selected then the order will be placed successfully.

5. Implementation

5.1 SHA-256 Algorithm

Passwords are created to add security, but now-a-days many attacks are happening on these passwords. Generally, people use easy-to-remember passwords which are easy for the hackers to steal them and misuse other's account. So, in order to increase the password security, we use SHA-256 algorithm as shown in figure 2.

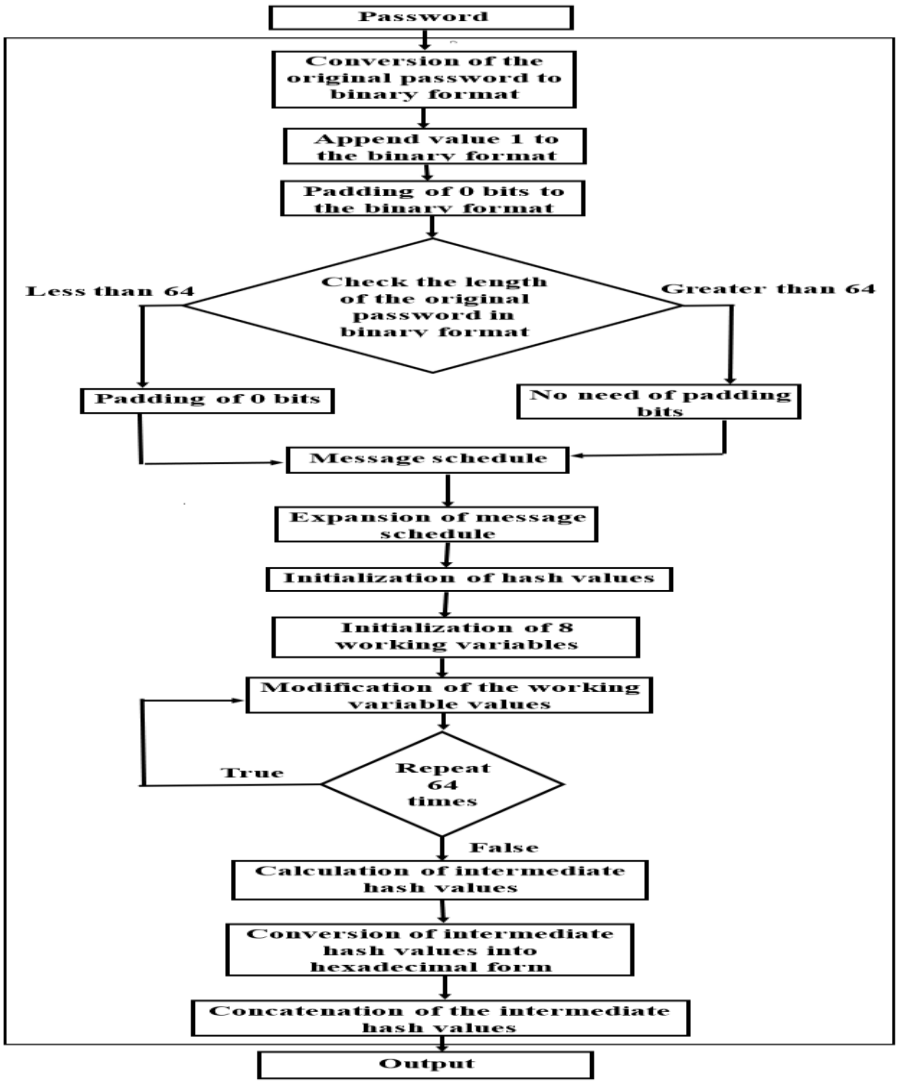

Fig. 2. Block diagram of SHA Algorithm

5.1.1 Algorithm

Step 1: Start
Step 2: The password entered by the user is converted into the binary format.
Step 3: To the binary format the number 1 is appended.
Step 4: To the binary format padding of 0 bits is done until (448 bits-length of binary message+1).
Step 5: Check the length of original password in binary format.
Step 6: IF Length of the original password in binary format
< 64
Padding of 0 bits
ELSE
No need of padding bits
Step 7: After Step 6, it results into a message schedule.
Step 8: The message schedule is divided into sixteen 32-bit words
Step 9: The expansion of the message schedule is calculated.

$$P_q = \begin{cases} A_q^i & 0 \le q \le 15 \\ \sigma_1^{256}(P_{q-2}) + P_{q-7} + \sigma_0^{256}(P_{q-15}) + P_{q-16} & 16 \le q \le 63 \end{cases} \quad (1)$$

$A_q^i = 32 - bit\ word\ from\ the\ 512 - bit\ message\ schedul$e
$P_q = 32 - bit\ word\ that\ is\ been\ created\ after\ using\ (1)$
$\sigma_0^{256}(x) = ROTR^7(x)\ XOR\ ROTR^{18}(x)\ XOR\ SHR^3(x)$
$\sigma_1^{256}(x) = ROTR^{17}(x)\ XOR\ ROTR^{19}(x)\ XOR\ SHR^{10}(x)$

Step 10: After the expansion of the message schedule, initialization of hash values is computed as follows.

$A_0^0 = 6a09e667$
$A_1^0 = bb67ae85$
$A_2^0 = 3c6ef372$
$A_3^0 = a54ff53a$
$A_4^0 = 510e527f$
$A_5^0 = 9b05688c$
$A_6^0 = 1f83d9ab$
$A_7^0 = 5beocd19$

Step 11: Initialization of 8 working variables is computed.

$s = A_0^{i-1}$
u= A_1^{i-1}
$j = A_2^{i-1}$
$l = A_3^{i-1}$
m = A_4^{i-1}
$n = A_5^{i-1}$
$o = A_6^{i-1}$
$r = A_7^{i-1}$

Step 12: Modification of the working variables takes place until 64 times.
For q=0 to 63:

{

$$T_1 = r + \sum_{r_1}^{256}(m) + ch(m,n,o) + K_q^{256} + P_q$$

$$T_2 = \sum_{0}^{256}(s) + Maj(s,u,j)$$

r=o

o=n
n=m
m=l+T_1
l=j
j=u
u=s
s=$T_1 + T_2$

}
Where:
$T_1 = temporary\ word\ 1$
$T_2 = temporary\ word\ 2$
s-r = working variables
ch (m, n, o) =choice function on m, n, o
$k_q^{256} = constants$
$P_q = words\ in\ message\ schedule$
Maj (s, u, j) =majority function s, u, j
Step 13: Computation of intermediate hash values is calculated as-
Intermediate hash values ← (Initial hash values + Modified values of working variables)
Step 14: Convert the intermediate hash values into hexa-decimal form and concatenate them.
Step 15: Stop
Disadvantages

a. SHA-256 algorithm is not supported by some of the older operating systems.

b. SHA-256 algorithm deployment is difficulting some environments.

c. Only some servers like java based servers, apache servers support this SHA-256 algorithm.

5.2 Chatbot

Chatbots are generally used to communicate with the users to solve their queries. In this research, the chatbot is designed in order to solve the general queries of the buyer regarding artificial limbs by using the technique of string comparison.

The different kinds of chatbots are Button-based chatbots, command-based chatbot, Voice bots, AI chatbot etc. The chatbot developed in the website is a command based chatbot, as it compares the string and give backs the reply. The mechanism behind the string comparison is, the chatbot is trained in beforehand with some questions and their corresponding replies. When the buyer asks a query, the chatbot compares the question asked to the questions in the database using the similarity function. The question that is more like that of the question asked by the buyer will have more frequency. The reply for the question having more frequency is given as an answer to the buyer. The chatbot used in the website will only solve the queries about artificial limbs. The chatbot used in the website is trained with 40 questions including permutations. Multiple combinations of the questions are taken and trained to the chatbot.

5.3 Rating

The rating system helps the customer to buy the products confidently. It is a group of various customer's opinions placed together which are used to judge the product. The rating that is already given helps the buyer to buy the products as their rating is displayed during the product selection. The rating system that is used in the website is star rating. The star rating system is designed by calculating the individual average of each field and the overall average is calculated out of five. Here, each field describes about the features of the product.

5.4 Review

Reviews generally increase the growth of website. Reviews change the decisions of customers while buying the products. Reviews generally build trust in users as they can confidently buy the products by learning about others opinion. It is one of the major growth factors of the website. This project provides a review option for the buyers to write their opinion about the product.

5.5 Feedback

Feedbacks help in the overall development of the website. It helps the admins to understand the problems in the user perspective. The admins can get more information in order to develop and update the website. Feedbacks create a good impression as the customers opinion is being considered. This website contains feedback with various questions that helps in the growth of website and encourage more customers to involve in the website.

6. Results

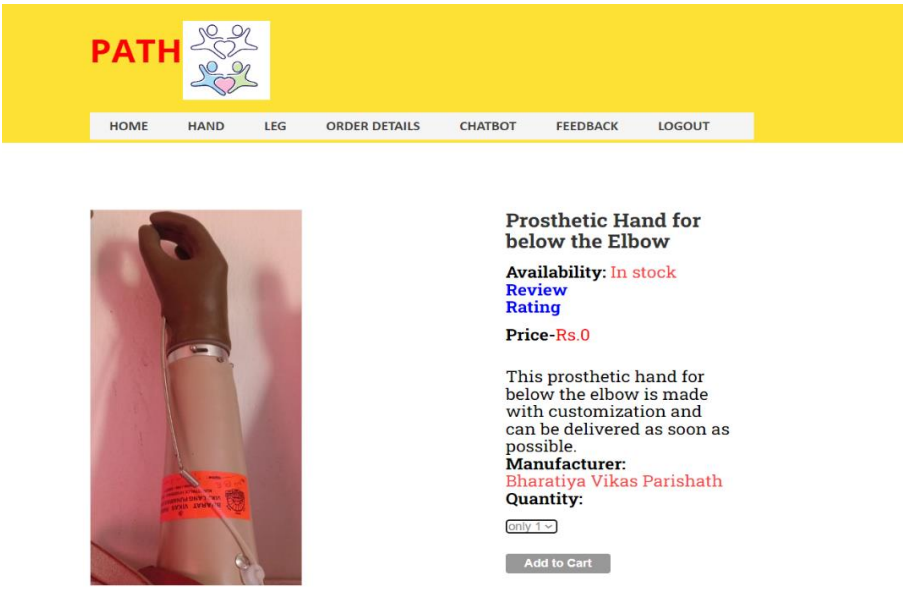

Fig. 3. Searching of Products by buyer

The buyer needs to login or register into the website. The buyer can search for required products according to the categories and sub-categories available as shown in figure 3. Once the product is identified, then it should be added to the cart. The buyer should also fill the shipping details.

Fig. 4. Uploading of doctor's prescription by buyer

Since customized products are available through the website, figure 4 shows that the buyer needs to upload the doctor's prescription. This can make the manufacturer to know more about the problem, that the buyer is facing. The buyer needs to select the mode of payment to place the order successfully.

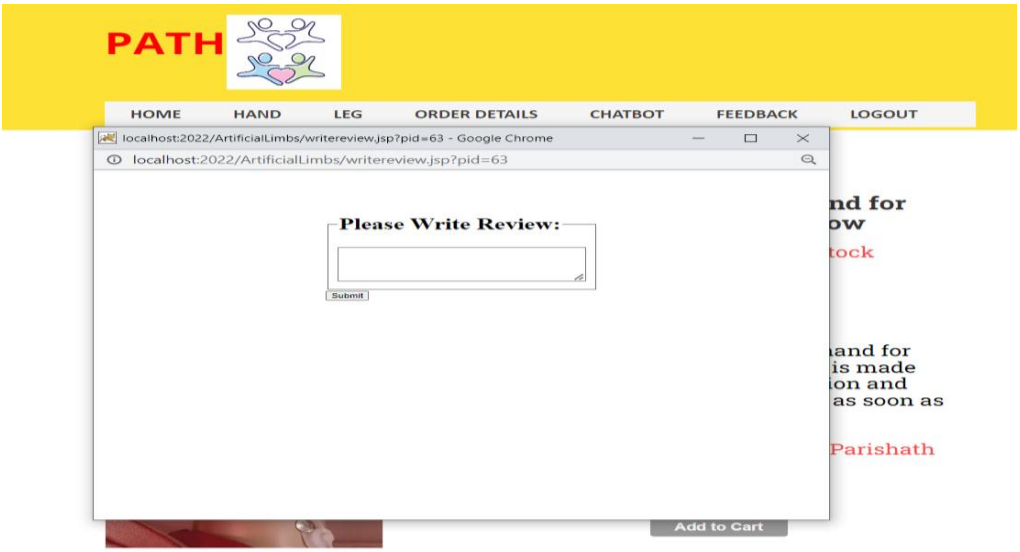

Fig. 5. Review of the Product by buyer

The buyer can add review to the product as shown in figure 5. Adding review helps in better understanding and can increase the confidence of a buyer to purchase the product.

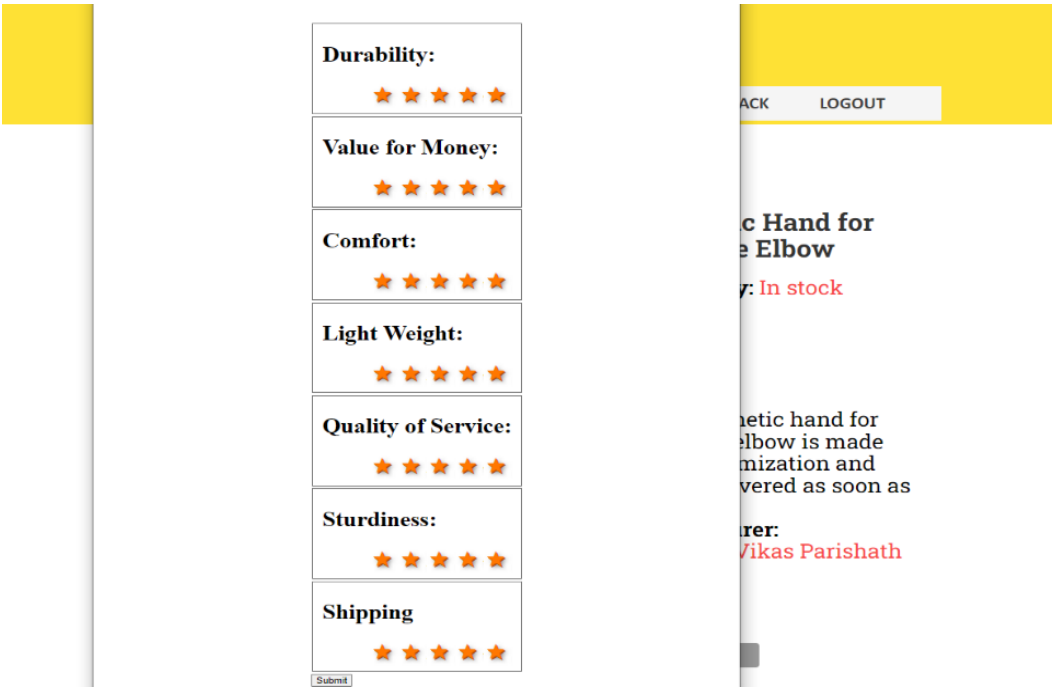

Fig. 6. Rating of the Product by buyer

In figure 6, rating the products is done by the buyer, which makes the next buyer to understand the quality of product. Different features of the products are rated, which can help the manufacturer to improve the quality of product.

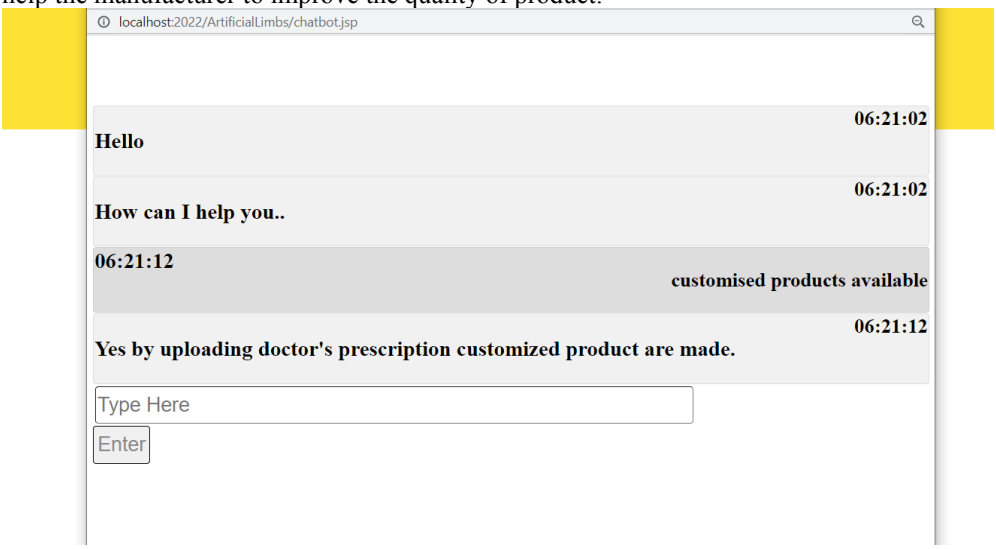

Fig. 7. Chatbot for buyer queries

A chatbot is present in the website which will clarify all the queries about the products. The chatbot shown in figure 7, is responsible in clarifying the doubts regarding the artificial limbs only.

7. Conclusion

Every research completion should satisfy some goals and should also be useful to people. This research is useful to the common people who need artificial limbs. The project fetches income to the manufacturers involved in the website. People can conveniently order the products and clarify their doubts using the chatbot. The prices are in affordable ranges. The website is a one-step solution to buy artificial limbs and all the categories of artificial limbs are available in the website. The website provides the security mechanism for passwords using SHA-256 algorithm. It provides the review, rating, and feedback mechanism to the users. This research can be extended by implementing SMS order notifications about the order status to the user. It can also use advanced speech-to-text chatbot.

References

1. Marks, J. Linda , and John W. Michael, Artificial limbs, Bmj 323, no. 7315: 732-735(2001)
2. Murray, D. Craig , Don't you talk to your prosthetist? Communicational problems in the prescription of artificial limbs, *Disability and rehabilitation* 35, no. 6: 513-521(2013)
3. A. Thorat , Sandeep, and Vishakha Jadhav, A review on implementation issues of rule-based chatbot systems, in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*(2020)
4. Chen, Chi-Wen, Five-star or thumbs-up? The influence of rating system types on user's perceptions of information quality, cognitive effort, enjoyment and continuance intention, *Internet Research* 27, no. 478-494(2017)
5. Teju, V. N. NagaSai Krishna, and K. V. Deepesh Reddy, Authentication process in smart card using Sha-256, *Journal of Computational and Theoretical Nanoscience* 17, no. 5: 2379-2382(2020)