INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Group messaging solution

Gaurav Gupta
gauravgupta078619@gmail.com
Thakur College of Engineering and Technology,
Mumbai, Maharashtra

Nikisha Mukund Mistry
nikishamistry25@gmail.com
Thakur College of Engineering and Technology,
Mumbai, Maharashtra

Abhijit Kushwaha
abhijitkushwaha98@gmail.com
Thakur College of Engineering and Technology,
Mumbai, Maharashtra

Dr. Zahir Aalam
zahiraalam@gmail.com
Thakur College of Engineering and Technology,
Mumbai, Maharashtra

ABSTRACT

In every organization, in order to work collaboratively, we need people who come up together and communicate so that they can express their ideas and share best thoughts and have good teamwork. In organizations, employees working on the same project may be residing in different places of the world to communicate, they need channels which can hold their confidential messages and also protect the messages from networking security threats. Currently, we have a number of messaging applications like Slack, Gmail, WhatsApp, etc. Prominently organizations use Gmail for emailing or their own mail sending services for communication. But for mail reception, we have a condition that mail receptor should know who has sent him mail. But there can be a condition in which someone might spoof, pretending to be someone. For organizations which to segregate authorities as senior and junior and communicate among each other, this kind of platform could be vulnerable. In current systems, hackers could even attach viruses and other malware to emails. If you want to send messages, you have to manually add the desired recipients. The project implements an application which would provide a way for communicating amongst teams and senior members of the team without hesitating and by implementing this project, members will also be able to put forward their views and points easily in front of the whole group members and senior authorities. Also, this project will make the communication effective which will, in turn, benefit the team and their work. Also, threat agents won't be able to send malicious files as this will be the only message based and hence more secure. Also, it will have a news feed section where the latest news about the company will occur which will keep everyone informed about the current scenario and everyone will be on the same page. The project also aims to identify confidential message sent using this messenger so that the confidentiality remains intact and admin can manage and see which user is using the confidential words also by implementing this, spam and rumor detection can also be implemented.

Keywords— *Security, Communication, Messaging, Group messaging solution*

1. INTRODUCTION

In every organization, in order to work collaboratively, we need people who come up together and communicate so that they can express their ideas and share best thoughts and have good teamwork. In organizations, employees working on the same project may be residing in different places of the world to communicate, they need channels which can hold their confidential messages and also protect the messages from networking security threats.

Currently, we have a number of messaging applications like Slack, Gmail, WhatsApp, etc. Prominently organizations use Gmail for emailing or their own mail sending services for communication. But for mail reception, we have a condition that mail receptor should know who has sent him mail. But there can be a condition in which someone might spoof, pretending to be someone. For organizations which to segregate authorities as senior and junior and communicate among each other, this kind of platform could be vulnerable. In current systems, hackers could even attach viruses and other malware to emails. If you want to send messages, you have to manually add the desired recipients.

The project implements an application which would provide a way for communicating amongst teams and senior members of the team without hesitating and by implementing this project, members will also be able to put forward their views and points easily in front of the whole group members and senior authorities. Also, this project will make the communication effective which will, in turn, benefit the team and their work. Also, threat agents won't be able to send malicious files as this will be the only message based and hence more secure. Also, it will have a news feed section where the latest news about the company will occur which will keep everyone informed about the current scenario and everyone will be on the same page.

The project also aims to identify confidential message sent using this messenger so that the confidentiality remains intact and admin can manage and see which user is using the confidential words also by implementing this, spam and rumour detection can also be implemented.

2. PROPOSED SYSTEM

The proposed system will have all the features we have now thought about such as spam and confidential message detection, no advertisements, affordable, a news feed, read aloud messages. Hence this project is meant to construct an application which will ease in communicating amongst themselves and also avoids distractions caused due to advertisements and other spam emails with also a feature to detect confidential or spam or rumor messages in the organization amongst themselves. Also, it will have a news feed section which will be operated by the organization itself.

3. METHODOLOGY

We have used agile methodology for making of this project. In Agile, companies keep iterating the project and testing it during the software development life cycle. So, this would help us do a lot of tasks simultaneously and develop an application exactly the way the client wants and assure security.

4. THEORY

As mentioned earlier we now understand how important communication for an organization is. So here we have come up with an application that is developed using Node.js.

The application intends to send and receive messages seamlessly with absolutely no delay and chaos. Network security is extremely important for the project. The network will only accept encrypted messages to pass through the network. An unencrypted message can be easily read by any sniffer. This is a kind of passive security attack because receptor of the message or the sender will never come to know that the message that belonged to him has reached him after someone reading it. The application has to also ensure that the attachments do not include malware. All this is taken into account while developing the application. After the completion of the application in the testing phase, we have tested the application against several possible security attacks and the application withstood most of them.

The data is stored locally in the application by using the MySQL/Mongo dB database. End-to-End security that let safely exchange private information with each other without worrying about data. In addition to the protection of storage, it has lots of modern features such as encryption support. The tools and techniques used by threat actors keep changing and adapting to the conventional security techniques currently in use. Role-based DB authorizes the sender-receiver and sends the requested resources only if the user has rights to else gives an error. Using this system admin will able to get more info like complete logged details of every user including the IP address of each system. Also, this messenger will detect any confidential message before sending it and will won’t allow sending the message, instead it will alert the admin by informing them about it. It also has a news feed section which will have the current trends managed by the organization itself.

In this project application, the data will be stored periodically in a single machine. No emails required to send the mail hence easing work. Managing is must easier with dynamic Graphical User Interface (GUI). Using AES 128-bit encryption and decryption. A group or team can interact together or individually. Admin manages and assigns the roles of users. It does not have a subscription pay scheme and hence saving money and only includes a one-time fee.

5. FEASIBILITY STUDY

5.1 Executive summary

Project is related to Group Messaging Solution. It is similar to WhatsApp but GMS will be a desktop application where the user is created by the admin and a unique certificate is generated for each user to identify his/her identity. Users will be assigned into groups i.e. into their respective departments by the admin. Each message will be encrypted by AES 256 bits and will include users certificate at the sender side and decrypted at the receiver side. An OCR technology will be introduced in this which can scan the document and convert the image into the text as it is since in GMS only text is allowed because of safety from Trojans, keyloggers, viruses, steganography etc.

5.1.1 The project maintains two levels of users:

- Administrator Level
- Departmental Level

5.1.2 Main facilities available in this project are:

- Maintaining hierarchy between users.
- Maintaining logs of chat in the server.
- Providing secure communication between end users.
- Providing socket id to each user to maintain their identity.
- Maintaining backup of data as per user requirements (between mentioned dates).
- The administrator can only assign users and provide them with their identity.
- News feed
- Confidential, spam and rumor Message detection and alerting to admin.
- Text to speech conversion of message.

5.2 Problem definition

- The system should be secure.
- The system should be able to handle multiple requests at the same time.
- The system should take automatic backup periodically.
- The system should have a responsive UI/UX.
- The system should provide role-based access control to monitor ongoing current traffic in the system.
- The system should be able to detect and stop before sending any confidential or spam messages.

5.3 Assumptions used in the study

Every user should be comfortable with working on a computer.

5.4 Audience impacted

It is designed for industry, startup organizations, and educational institutions.

5.5 Financial obligation

The financial and the economic questions during the preliminary investigation are verified to estimate the following:

- The cost to conduct a full system investigation.
- The cost of hardware and software for the class of application being considered.
- The benefits in the form of reduced cost.

5.6 Recommended action

- Time evaluation is the most important consideration in the development of the project.

- The time schedule required for the developer of this project is very important since more development time effect machine time, cost and cause a delay in the development of other systems.

5.7 Technical feasibility

As already many chatting applications are available but when it comes to security GMS is more secure than any other application.

5.8 Economic feasibility

As GMS is organization specific it will only cost for the database server to keep backup.

5.9 Socio-cultural feasibility

As GMS is all about group communication there will be complete transparency between everyone.

6. RESEARCH/TECHNICAL/PROJECT WORK

The different applications existing in the market today have a lot of features. They are all very easy to use. They are affordable facilities for usage by the common man. All the features that the developers claim are indeed worth using. But they cannot be used by business organizations as they have to discuss several formal issues. The applications can have several security threats. We conducted research to study what features are needed by users and which platform they use regularly for communication. The users gave a number of ideas for the development of better applications.

The survey can be depicted by the following pie chart:

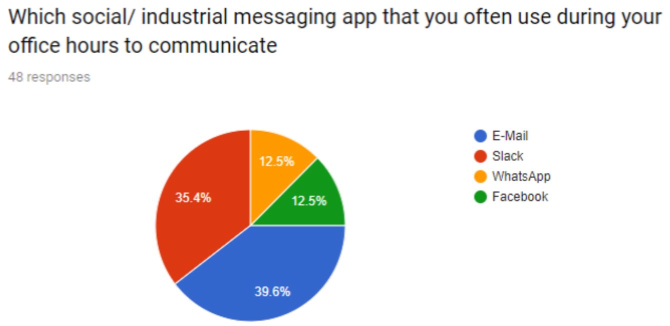


Fig. 1: Survey pie chart

The project works as follows:

- First admin registers all the legit users and saves the credentials of each user in the database.
- When the user wants to enter the system, he has to get authenticated and authorized. For this, he enters credentials.
- These credentials are checked and matched with the ones in the database.
- If the credentials match, the user gets an entry in the system else no.
- If the user enters wrong credentials, he is blocked for 5 minutes so that the brute force attack can be avoided.
- After logging in a unique ID is generated known as socket ID and it is assigned to each user for concurrency control.
- The user sends messages by selecting a user from the chat list and these messages in the database and all of them are sent in first out the way.
- Before sending the message, it will check if the message contains any confidential terms if yes then the message won't be sent and instead admin will get notified. If no then the message will be sent.

Below show flowchart describes the flow of the application.

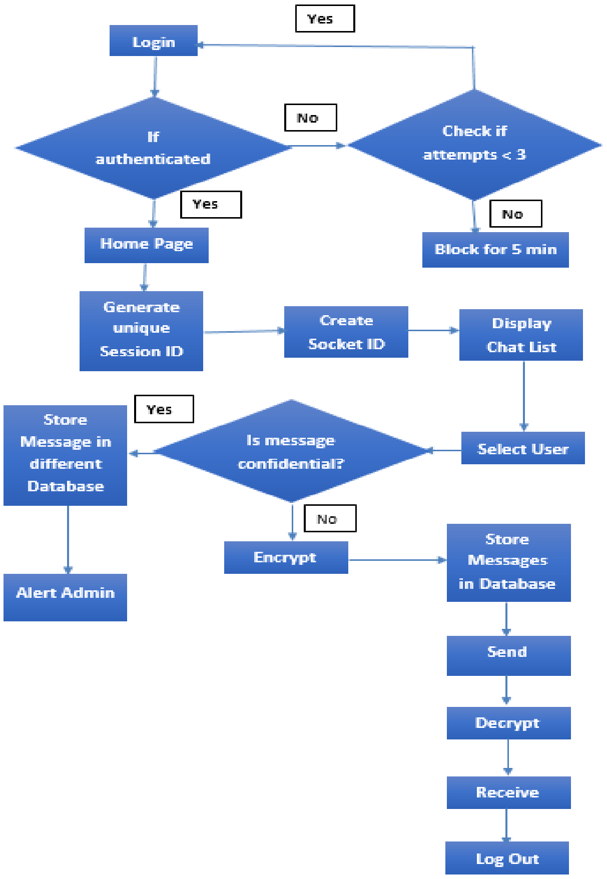
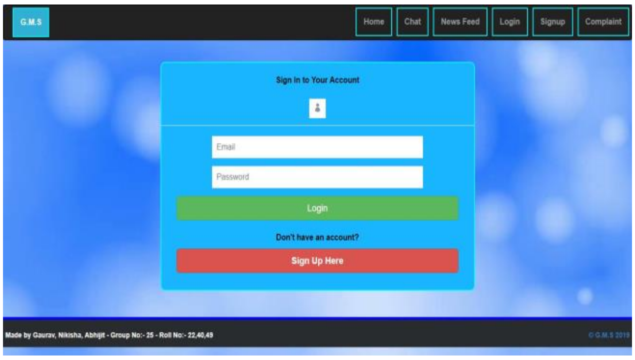


Fig. 2: Flowchart

Following are the screenshots of UI which is kept very simple and lightweight to increase the speed so that it can be even accessed by the 2G network. Register option will only be available to the admin. And after user login, he will have the access to chat list where he can select the group for communication or individual accordingly.



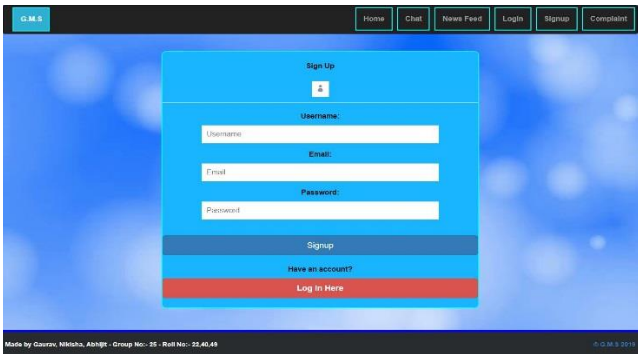
Sign In to Your Account

Don't have an account?

Made by Gaurav, Nikisha, Abhijit - Group No:- 25 - Roll No:- 22,40,49

Fig. 3: Login UI

The above screenshot describes the login page of GMS.



Sign Up

Username:

Email:

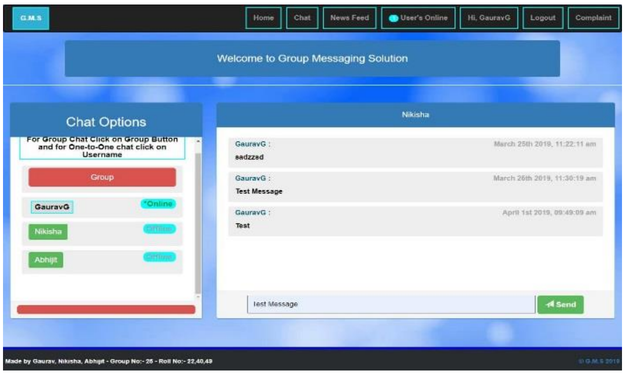
Password:

Have an account?

Made by Gaurav, Nikisha, Abhijit - Group No:- 25 - Roll No:- 22,40,49

Fig. 4: Signup UI

The above screenshot describes the signup page of GMS



For Group Chat Click on Group Button and for One-to-One chat click on Username

GauravG : March 25th 2019, 11:22:11 am
sadzzsd

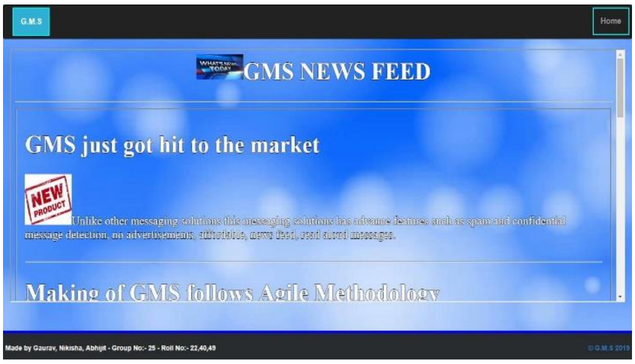
GauravG : March 25th 2019, 11:30:19 am
Test Message

GauravG : April 1st 2019, 09:49:09 am
Test

Test Message

Fig. 5: Message sending window

The above screenshot describes the Messages sending window page of GMS


G.M.S
Home
WHAT'S NEWS TODAY
NEW PRODUCT
Made by Gaurav, Nikisha, Abhijit - Group No:- 25 - Roll No:- 22,40,49
© G.M.S 2019

GMS NEWS FEED

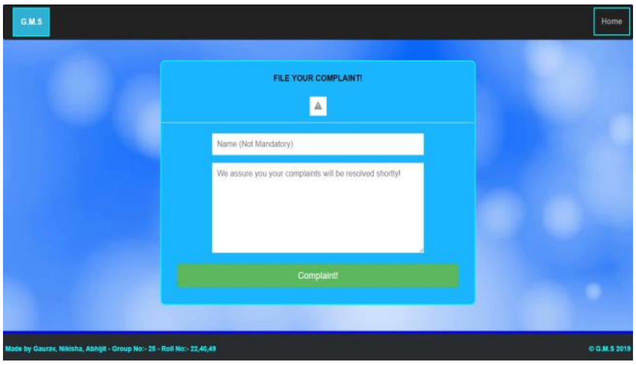
GMS just got hit to the market

Unlike other messaging solutions this messaging solutions has advance features such as spam and confidential message detection, no advertisements, affordable, news feed, read aloud messages.

Making of GMS follows Agile Methodology

Fig. 6: News feed page

The above screenshot describes the News Feed page of GMS


G.M.S
Home
Complaint!
Made by Gaurav, Nikisha, Abhijit - Group No:- 25 - Roll No:- 22,40,49
© G.M.S 2019

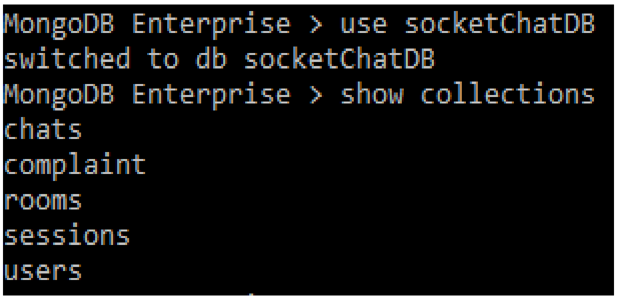
FILE YOUR COMPLAINT!

Name (Not Mandatory)

We assure you your complaints will be resolved shortly!

Fig. 7: Complaint page

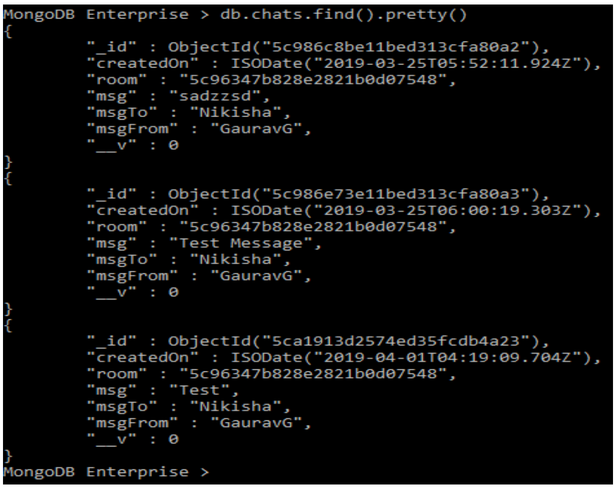
The above screenshot describes the complaint page of GMS Following is the schema of the database used in this project which consists of user table which keeps the record of the user such as username, password, socket-id, online time and another table defines the route of the message and the message. In future scope, we can apply AI and deep learning to identify spam messages or confidential messages which are not supposed to be communicated.



```
MongoDB Enterprise > use socketChatDB
switched to db socketChatDB
MongoDB Enterprise > show collections
chats
complaint
rooms
sessions
users
```

Fig. 8: Collections

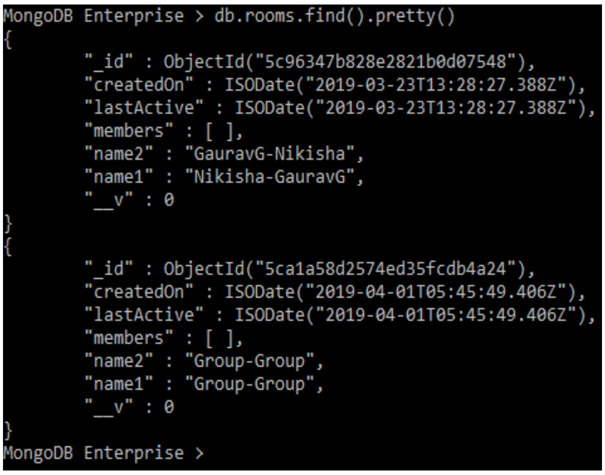
The above screenshot shows the collections part of mongo dB used in GMS where all the collections are stored in database socket ChatDB



```
MongoDB Enterprise > db.chats.find().pretty()
{
        "_id" : ObjectId("5c986c8be11bed313cfa80a2"),
        "createdOn" : ISODate("2019-03-25T05:52:11.924Z"),
        "room" : "5c96347b828e2821b0d07548",
        "msg" : "sadzzsd",
        "msgTo" : "Nikisha",
        "msgFrom" : "GauravG",
        "__v" : 0
}
{
        "_id" : ObjectId("5c986e73e11bed313cfa80a3"),
        "createdOn" : ISODate("2019-03-25T06:00:19.303Z"),
        "room" : "5c96347b828e2821b0d07548",
        "msg" : "Test Message",
        "msgTo" : "Nikisha",
        "msgFrom" : "GauravG",
        "__v" : 0
}
{
        "_id" : ObjectId("5ca1913d2574ed35fcdb4a23"),
        "createdOn" : ISODate("2019-04-01T04:19:09.704Z"),
        "room" : "5c96347b828e2821b0d07548",
        "msg" : "Test",
        "msgTo" : "Nikisha",
        "msgFrom" : "GauravG",
        "__v" : 0
}
MongoDB Enterprise >
```

Fig. 9: Chats

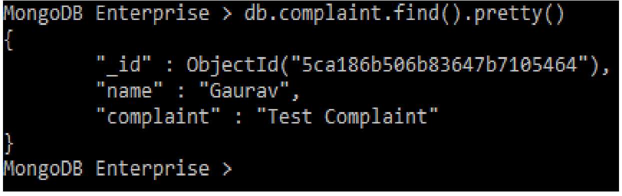
The above screenshot shows the chat collection of mongo dB used in GMS where all and from messages are stored.



```
MongoDB Enterprise > db.rooms.find().pretty()
{
        "_id" : ObjectId("5c96347b828e2821b0d07548"),
        "createdOn" : ISODate("2019-03-23T13:28:27.388Z"),
        "lastActive" : ISODate("2019-03-23T13:28:27.388Z"),
        "members" : [ ],
        "name2" : "GauravG-Nikisha",
        "name1" : "Nikisha-GauravG",
        "__v" : 0
}
{
        "_id" : ObjectId("5ca1a58d2574ed35fcdb4a24"),
        "createdOn" : ISODate("2019-04-01T05:45:49.406Z"),
        "lastActive" : ISODate("2019-04-01T05:45:49.406Z"),
        "members" : [ ],
        "name2" : "Group-Group",
        "name1" : "Group-Group",
        "__v" : 0
}
MongoDB Enterprise >
```

Fig. 10: Rooms

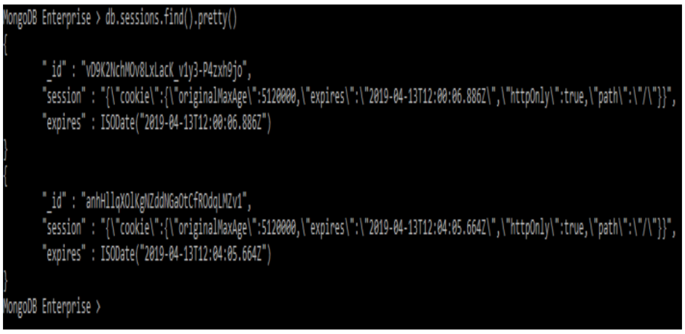
The above screenshot shows the collection of the room of mongo dB used in GMS where group's information is stored.



```
MongoDB Enterprise > db.complaint.find().pretty()
{
        "_id" : ObjectId("5ca186b506b83647b7105464"),
        "name" : "Gaurav",
        "complaint" : "Test Complaint"
}
MongoDB Enterprise >
```

Fig. 11: Complaint

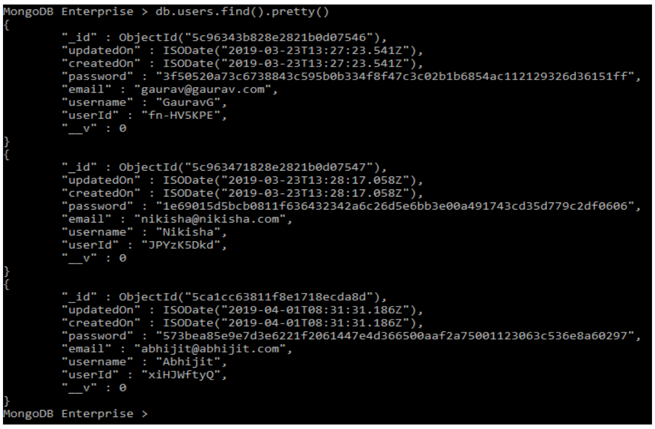
The above screenshot shows the complaint collection of mongo dB used in GMS where complaint data is stored.



```
MongoDB Enterprise > db.sessions.find().pretty()
{
        "_id" : "vD9K2NchMOv8LxLacK_v1y3-P4zxh9jo",
        "session" : "{\"cookie\":{\"originalMaxAge\":5120000,\"expires\":\"2019-04-13T12:00:06.886Z\",\"httpOnly\":true,\"path\":\"/\"}}",
        "expires" : ISODate("2019-04-13T12:00:06.886Z")
}
{
        "_id" : "anhH1lqXOlKgNZddNGaOtCfROdqLMZv1",
        "session" : "{\"cookie\":{\"originalMaxAge\":5120000,\"expires\":\"2019-04-13T12:04:05.664Z\",\"httpOnly\":true,\"path\":\"/\"}}",
        "expires" : ISODate("2019-04-13T12:04:05.664Z")
}
MongoDB Enterprise >
```

Fig. 12: Sessions

The above screenshot shows the sessions collection of mongo dB used in GMS where sessions are stored.



```
MongoDB Enterprise > db.users.find().pretty()
{
        "_id" : ObjectId("5c96343b828e2821b0d07546"),
        "updatedOn" : ISODate("2019-03-23T13:27:23.541Z"),
        "createdOn" : ISODate("2019-03-23T13:27:23.541Z"),
        "password" : "3f50520a73c6738843c595b0b334f8f47c3c02b1b6854ac112129326d36151ff",
        "email" : "gaurav@gaurav.com",
        "username" : "GauravG",
        "userId" : "fn-HV5KPE",
        "__v" : 0
}
{
        "_id" : ObjectId("5c963471828e2821b0d07547"),
        "updatedOn" : ISODate("2019-03-23T13:28:17.058Z"),
        "createdOn" : ISODate("2019-03-23T13:28:17.058Z"),
        "password" : "1e69015d5bcb0811f636432342a6c26d5e6bb3e00a491743cd35d779c2df0606",
        "email" : "nikisha@nikisha.com",
        "username" : "Nikisha",
        "userId" : "JPYzK5Dkd",
        "__v" : 0
}
{
        "_id" : ObjectId("5ca1cc63811f8e1718ecda8d"),
        "updatedOn" : ISODate("2019-04-01T08:31:31.186Z"),
        "createdOn" : ISODate("2019-04-01T08:31:31.186Z"),
        "password" : "573bea85e9e7d3e6221f2061447e4d366500aaf2a75001123063c536e8a60297",
        "email" : "abhijit@abhijit.com",
        "username" : "Abhijit",
        "userId" : "xiHJWftyQ",
        "__v" : 0
}
MongoDB Enterprise >
```

Fig. 13: Users

The above screenshot shows the users collection of mongo dB used in GMS where data of users such as username and password are stored.

After completion of this project, we performed penetration testing on this so that we can secure it from the well-known OWASP top 10 vulnerabilities that are:

- Lack of Validation
- Insecure Configuration Management
- Broken Access Control
- Broken Authentication and Session Management
- Cross Site Scripting
- Buffer Overflow
- Injection Flaws
- Improper Error Handling
- Insecure Storage
- Application Denial of Service

Also, we have done necessary steps to prevent it such as blocking the user to access the platform if wrong credentials are entered multiple times also input value is escaped and filtered to prevent XSS and other attacks.

7. RESULT AND DISCUSSION

We successfully achieved to eliminate the disadvantages of other messaging systems such as advertisements, distraction because of friends or other spam messages, fake rumours.

We managed to eliminate the subscription system and instead of paying in repetitive manner client can own this with one-time pay and can get customized according to its needs which is not provided in others.

8. CONCLUSION

Thus, by this, we conclude that the proposed system (Group Messaging Solution) transparency will be there in a hierarchy. Also, not only an industry but also other organizations where hierarchy is available. This system helps the group members to have a better communication amongst them and so that everyone can keep their idea and eliminate the research gap.

We first went for a literature survey in which we understood several research gaps. There are several systems used for messaging but they have flaws. We conducted surveys to understand the advantages and disadvantages of those applications that the users face. Advantages and disadvantages were analyzed and a feasibility study was made to understand what we can do to get a better application.

So, we tried and created an application that is customizable as per what the user needs. The user can anytime think of changes and change the system. The User interface helps the user understand the working of the system. Our work was based on agile methodology so we completed works in parts and then collaborated them. It removes annoying issues like advertisements. It also has a news feed and message detection system which will help the employees stay on the same page and eliminate the spam and rumors and also admin can keep an eye on confidential message. The application can be used all the time after paying once.

We successfully matched what was expected and we what is created.

9. FUTURE SCOPE

Through our project, we have tried to fulfil all the technological gaps that we found out through the literature surveys and surveys that we conducted. But the project has a future scope because it is an interactive project and can be advanced as per the needs and demands of the stakeholders. The following features can further be added to the project:

- Identify messages with priority.
- Sending attachments along with messages.
- Adding a dictionary.

10. ACKNOWLEDGEMENT

We would like to express deep regards and gratefulness to Principal Dr B. K. Mishra for always encouraging students to learn new technologies and implement them.

We would like to express our deep gratitude to the staff members for co-operation. Also, we would like to thank our Dean R&D Dr Kamal Shah and H.O.D Dr Rajesh Bansode for his sincere support and guidance.

We sincerely thank our guide Dr Zahir Aalam for his guidance and support for carrying out our project work. It is indeed a matter of pleasure and privilege to be able to present this project on Group Messaging Solution.

We would like to thank the non-teaching staff and friends who have helped us all the time in one way or the other. Really it is impossible to repay the debt of all the people who have directly or indirectly helped us in completing the project.

11. REFERENCES

[1] Noor Sabah, Jamal M. Kadhim and Ban N. Dhannoon, “Developing an End-to-End Secure Chat Application,” in International Journal of Computer Science and National Security, vol. 17, no. 11, November 2017.

[2] Manoj Kumar Srivastava, “Systems and methods for detecting and/or handling targeted attacks in the email channel,” US Patent No: US 9,686,308 B1, Date of Patent: June 2017.

[3] Joon S. Park, “Role-based access control to computing resources in an inter-organizational community,” US Patent No: US 9, 769,177 B2, Date of patent: September 2017.

[4] Zhen Wang, Zheofeng Ma, Shoushan Luo, Hongmin Gao, “Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network System,” in IEEE Access, March 2018.

[5] Deeksha K, P.Hemashree “Intranet Chatting System,” in International Journal of Engineering Technologies in Engineering Research, vol. 6, no. 4, April 2018.