IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secured Chatting System Using Cryptography

Muhammed Kuliya[1], Hassan Abubakar[2]

[1]Lovely Professional University, Punjab India
[2]Federal Polytechnic Bauchi, Department of Computer Science

Abstract

Chatting applications are very popular among Internet users and Smartphone's owners. Hundred millions of smartphone owners use chat applications on monthly basis. These chat applications offer the communication free of charge and majority of them are free to install which makes it very appealing for the potential customers. These chat applications offer different services and built-in features to their users while in majority of the cases, they neglect security aspects of their usages and messages. According to a report provided by Electronic Frontier Foundation (EFF) majority of these chat applications do not provide enough security for their users.

Keywords: Chat, Cryptography, Encrypt, Security

1.1 Introduction

Chatting applications have become indispensable tools in today's workforce. There are hundred millions of chatting application in the market with different operating systems and capabilities. These chatting applications have the capability of installing applications on them in order to do many tasks, such as sending text messages. Wi-Fi networks have grown dramatically for the last decade and they are almost ubiquitous in daily life. According to a report by quarter 3 of year 2014, there are 2.5 billion mobile broadband subscriptions worldwide and there are about 8.4 billion mobile broadband subscriptions in the year 2020. This growth and accessibility to an Internet connection has brought opportunities for many Instant Messaging applications to enter a new area of communication and to penetrate traditional telephony communication. Instant messaging applications are one of the most popular categories of applications among the users. (Tom, 2012).

1.2 Statement of the Problem

Malicious users are always interested to hack servers and reveal information about users in a certain system including celebrities and this happens almost every day in the introduction Internet world. Unfortunately, instant messaging applications are not an exception. There are many mobile chat applications available for users. Many of these applications claim that they are providing confidentiality, integrity and availability of user's information. However, daily hacking news prove that many developers do not consider security as the primary goal of their applications. On the other hand, governments are keen on tracking their citizens and forcing more service providers to reveal profiles of their users in the hands of their agents. Furthermore, chat applications providers misuse information of their users. For example, while many chat applications are free to use, they equip the application with built-in processes which track every single movement. There must be careful with what is going to be published on social networks. The hackers store large amounts of information about the activities we do, the places we visit, the people with whom we interact, our hobbies, the food we like, etc.

All this information can be used by an attacker to know our profile or plan and launch custom attacks such as the phishing that we mentioned in the first part of this guide. In addition, the information collected can be used even for kidnappings or extortions (Guide, 2017).

1.3 Aims and Objectives

The aim of this research is to design a secure chat application which protects user's confidentiality and privacy. The research investigates current security features of several messaging applications. The selected instant messaging applications have been investigated and a list of requirements for the design of a secure chat application was created.

The objectives are:

i- To develop a secured chatting using cryptography algorithm
ii- To implement a chatting that can encrypt text message
iii- To implement a chatting that can decrypt text message
iv- To implement a chatting that can decrypt recent text message

1.4 Scope and Limitation of the Study

In this research different chat applications have been investigated. Based on the threat model of chat applications, different requirements for a secure chat application have been enlisted and a design was also proposed. The scope of this project is to propose solutions for different security challenges of the current chat applications in the market and to design and implement a secure chat application. The main contributions of this research can be structured into the following four sub-goals:

i- Literature study and related security vulnerabilities in current chat apps

ii- To propose a secure chat application architecture

iii- A detailed design of secure chat application

iv- To implement and evaluate a demo as proof of concept (POC)

Some of the Limitations In the proposal and the design of the secure chatting system application is based on the client/server model. However, with the rise of mesh networks and built in features in operating systems such as iOS* which has the built-in ability of "multi peer connectivity", very few peer-to-peer chat applications are available in the market. Peer-to-peer (P2P) chat clients are omitted from this thesis since their architecture and infrastructure is different. Another thesis can be derived to focus only on such peer-to-peer chat applications and investigation of their security vulnerability and design flaws.

1.5 Justification of the Study

Chatting system technology has taking almost all the areas of our life, and the technology development is at the speed of light. A successful development of the secured chatting system will bring about a long run solution to the problems faced by the chatting system users, among the solution this system intend to bring is; security of data is paramount factor, but the proposed system intend to bring solution to that by providing a kind of system where only authorized persons can have access to the specific data in the system. Username and password will be assigned or given upon registration so that it will prevent un-authorized person from having access to the areas where there not suppose. Basically, the proposed system will be developed in such a way that it will solve the problems faced and transformed ways of operation into the systematic method.

The system has many great benefits to the users:

i- Protects user’s confidentiality and privacy
ii- Makes chatting process easy for the users
iii- Proposed system will provide easy access and user-friendly system
iv- Easy to encrypt and decrypt the messages

2.1 Related Literature

The most basic conversation security features that a secure chat protocol can provide are confidentiality and integrity. This can be easily implemented without adversely affecting usability and adoption properties by using a central server to relay messages and securing connections from clients to the central server using a transport-layer protocol like TLS. This also allows the central server to provide presence information. Since this approach does not negatively affect usability, it is no surprise that this architecture has been adopted by some of the most popular messaging systems today (e.g., Skype, Facebook Chat, Google Hangouts)(Bonneau, Fahl, Perl, Goldberg, & Smith, n.d.). The global cost of cybercrime has now reached as much as $600 billion — about 0.8 percent of global GDP — according to a new report. More worrying than that figure may be the massive growth from 2014, when the same analysis showed the cost was only as much as $445 billion. That rapid increase is largely due to the lower cost of entry and advancements in technology such as machine learning and artificial intelligence, according to Ian Yip, the Asia Pacific chief technology officer at cyber security firm McAfee. Speaking with CNBC's "Street Signs" on Thursday, he explained how conducting criminal activity in cyberspace has gotten easier. Cybercrime is the only criminal enterprise that has "a help desk," he said, adding that would-be criminals "don't need to be technologically advanced" anymore to conduct a cyber-attack. The analysis comes as McAfee and American think tank the Center for Strategic and International Studies releases a study entitled "The Economic Impact of Cybercrime—No Slowing Down," which assesses the gravity of what Yip called a cybercrime "pandemic. Certain nation states have come to be regarded as safe havens for cybercriminals, adding that countries such as North Korea, Iran and Russia "tend to go after financial services," while "espionage activities" are more rampant in China.

The potential cost of cyber-crime to the global community is a mind-boggling $500 billion, and a data breach will cost the average company about $3.8 million. Now, that’s a lot of money. But this can easily be fixed once we get a few facts right: about 63 percent of all network intrusions and data breaches are due to compromised user credentials, so taking measures to protect your credentials should give you an added layer of protection. An attacker spends about 146 days within a network before being detected that’s quite a lot of time. Knowing this, regular measures could be taken to audit a network and ensure its security. According to data from Juniper Research, the average cost of a data breach will exceed $150 million by 2020 — and by 2019, cybercrime will cost businesses over $2 trillion — a four-fold increase from 2015. We were still gasping at the cost of $3.8 million Microsoft said a data breach costs the average company. However, data from Juniper Research shows this amount will be increased by a massive 3,947 percent to over $150 million by 2020. As your company grows, and as the Internet continues to develop at a massive pace, it might be a good idea to increase the percentage of your budget that goes towards security. Unfilled cyber security jobs are expected to reach 3.5 million by 2021 — compared to about 1 million in 2016. While this might not seem like much, it is worth paying attention to: the projected increase in the number of cyber security-related jobs is proportional to a projected increase in cybercrime, and a more than 200 percent increase means we can expect cybercrime to increase by at least that much by 2021. 90 percent of hackers cover their tracks by using encryption, Hackers are also widening up to the use of encryption techniques like VPNs, and they are now more effectively covering their tracks making it much easier to arrest them. The most effective method to combat cyber-attacks as hackers get more sophisticated is by using the right preventative methods. It’s getting more and more difficult to catch them (Mason, 2018).

The computer hackers may be tempted to break into the database of an organization to steal information or data which may be used or information about their organization to other organization that is competing with them. Such an act is disastrous to the organization concerned. This problem can be minimized by using the principle of encryption of data such that a decryption key is hidden from the lower management and by so doing, if an intruder or hacker try to break into the file of the organization, even if such is done the hacker may not understand the encryption code of information. The importance of securing data in a computer system cannot be over-emphasized, that is why the researchers feel it is necessary to address this pertinent topic because information is a weapon of an organization. As a result of this there is a need for it to be protected from unauthorized users, since it is almost inevitable for information to be kept completely safe from computer software hackers, it is necessary to prevent information once accessed by unauthorized persons. Software security is the idea of engineering software so that it continues to function correctly under malicious attack. Most technologists acknowledge this undertaking's importance, but they need some help in understanding how to tackle it.

2.2 Application Security

File transfer is very sensitive especially for instant messaging. One thing is that file transfer is executed in peer-to-peer model and therefore it should be more secure(Sasko & Chao, 2007). Application security means many different things to many different people. It has come to mean the protection of software after it's already built. Although the notion of protecting software is an important one, it's just plain easier to protect something that is defect-free than something riddled with vulnerabilities. Pondering the question, "What is the most effective way to protect software?" can help untangle software security and application security. On one hand, software security is about building secure software: designing software to be secure, making sure that software is secure and educating software developers, architects and users about how to build secure things. On the other hand, application security is about protecting software and the systems that software runs in a post facto way, after development is complete**.**

Application security follows naturally from a network-centric approach to security, by embracing standard approaches such as penetrate and patch and input filtering (trying to block malicious input) and by providing value in a reactive way. Put succinctly, application security is based primarily on finding and fixing known security problems after they've been exploited in fielded systems. Software security—the process of designing, building and testing software for security—identifies and expunges problems in the software itself. In this way, software security practitioners attempt to build software that can withstand attack proactively. Let me give you a specific example: although there is some real value in stopping buffer overflow attacks by observing HTTP traffic as it arrives over port 80, a superior approach is to fix the broken code and avoid the buffer overflow completely. The biggest threats in cybersecurity today are around the large scale proliferation of targeted attacks – from breach and email distribution of socially engineered ransomware to potentially harmful attacks on critical infrastructure like energy networks (Gedda, 2016).

2.3 Cyber Security

Good cybersecurity readiness encompasses an understanding of risks and threats to assets and information relevant to the organisation and its people, monitoring and detecting cybersecurity threats regularly, protecting critical systems and information, ensuring the organisation meets all relevant standards compliance, has incident response plans in place in the event of a breach, and clear business continuity plans to minimize any loss (Gedda, 2016). With a substantial increase in Internet access, concerns around Cyber Security are particularly prominent. This growth in concern is, of course, fuelled by the dramatic increase in online fraud and hacking. Emails have become a particularly popular delivery method for online criminals, with an incredible 1 in 131 emails containing malware.

Ransomware – the malicious software that locks personal and business computers until a ransom is paid has seen a substantial increase over the last 12 months, rising 36% globally in the last year. The average amount demanded by a ransomware attack is $1,077, an increase of 266% on the previous year. Research from Symantec suggests that 34% of people globally are willing to pay a ransom to get their data back – increasing to 64% for Americans. The FBI suggests there are more than 4,000 ransomware attacks globally every day. Identity fraud has also seen a significant rise, particularly in developed countries like the United States and the UK. In 2016, 6.15% of consumers became victims of identity fraud, with the costs associated with also increasing. In 2017, the total amount of losses due to identity fraud in the US reached $16 billion.

Fears around security are notably prevalent among businesses, many of whom are responsible for huge swathes of customer data. Looking at the associated costs, it's easy to see why businesses are so concerned. A single data breach will cost the average company $3.8 million. Juniper Research suggests that this will exceed $150 million by 2020. The impact on affected businesses is also cause for significant concern, with 60% of small companies going out of business within six months of an attack. Given the potential sums available to cyber criminals, they remain an appealing target. As with attacks against private citizens, email remains a popular delivery method for malware and phishing. Business Email Compromise (BEC) scams targeted over 400 businesses per day last year, draining $3 million over the last 3 years. 43% of cyber-attacks target small businesses. While cyber-crime is a global problem, some regions are seeing significantly higher levels of infection (cyber security, 2015). Cyber-attacks are growing in prominence every day – from influencing major elections to crippling businesses overnight, the role cyber warfare plays in our daily lives should not be underestimated. In fact, billionaire investor Warren Buffett claims that cyber threats are the biggest threat to mankind and that they are bigger than threats from nuclear weapons.

2.4 Instant Messaging

Instant messaging (IM) is a real time text based communication between two or more people connected over a network like the Internet. Instant message has become very popular, with this you can interact with people in a real time environment and you can keep the list of family and friends on your contact list and can communicate as long as the person is online. When deploying an instant messaging (IM), Presence and real-time communications platform, an enterprise or service provider must ensure that the platform addresses the needs of many users and applications, each with a unique set of challenges, as well as the organization’s strategic operations (Primer, 2017).

2.4.1 SMS based Text Messaging

Text messaging, also known as "texting", refers to the exchange of brief written messages between mobile phones over cellular networks. The messages may include images, video, and sound content (known as MMS messages). Individual messages are referred to as "text messages" or "texts". The most common application of the service is person-to-person messaging.

2.4.2 *Features of Instant Messengers*

i- Instant text messaging
ii- Video chat using Webcam
iii- Voice chat
iv- Sharing files
v- Chats and buddy list in one screen
vi- Add and manage buddies
vii- Recent chat history
viii- Send/Receive offline messages
ix- Multiple languages
x- Multi-party video chat and Video messaging
xi- Some of the chat applications do not require installation, we can directly chat by accessing the site through browser

2.4.3 *Types of Chat Rooms*

Chat can be done in public rooms, open to anyone, or private rooms where only those of the community can enter. Common chat rooms are as follows

i- Business chat room
ii- Single chat room
iii- Stranger chat room
iv- Romance chat room
v- Human interest chat room
vi- Family chat room
vii- Political chat room.
And there are many more chat rooms available in the instant messenger applications.

2.4.4 Risks and Threats on Chatting Applications

i- Security Risks

Crackers (malicious "hacker" or Blackhat hacker) have consistently used IM networks as vectors for delivering phishing attempts, "poison URLs", and virus-laden file attachments. For example, IM used to infect computers with spyware, viruses, trojans, worms

ii- Compliance risks

In addition to the malicious code threat, the use of instant messaging at work also creates a risk of non-compliance to laws and regulations governing the use of electronic communications in businesses.

iii- Inappropriate use

Organizations of all types must protect themselves from the liability of their employees' inappropriate use of IM. The informal, immediate, and ostensibly anonymous nature of instant messaging makes it a candidate for abuse in the workplace

2.5 Cryptography

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shares the decoding technique only with intended recipients to preclude access from adversaries. The cryptography literature often uses the name Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary. Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

2.5.1 Cryptanalysis

The art and science of breaking the cipher text is known as cryptanalysis. Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths. Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

2.5.2 *Security Services of Cryptography*

The primary objective of using cryptography is to provide the following four fundamental information security services. Let us now see the possible goals intended to be fulfilled by cryptography.

i- Confidentiality

Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy.

Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

ii- Data Integrity

It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

iii- Authentication

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.

Authentication service has two variants:

a- Message Authentication identifies the originator of the message without any regard router or system that has sent the message.

b-Entity Authentication is assurance that data has been received from a specific entity, say a particular website. Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

Iv-Non-repudiation

It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party. Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

2.5.3 Cryptography Primitives

Cryptography primitives are nothing but the tools and techniques in Cryptography that can be selectively used to provide a set of desired security services:

i- Encryption

ii- Hash functions

iii- Message Authentication codes (MAC)

iv- Digital Signatures

2.5.4 A *Cryptosystem*

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system**.**

The various components of a basic cryptosystem are as follows:

i- Plaintext- It is the data to be protected during transmission.

ii- Encryption Algorithm- It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.

iii- Ciphertext- It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

iv-Decryption Algorithm- It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.

v- Encryption Key- It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.

vi- Decryption Key- It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext. For a given cryptosystem, a collection of all possible decryption keys is called a key space.

viii- **Interceptor-** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

3.1 Throw Away Prototyping Methodology

Throw away prototyping or rapid prototyping refers to the creation of a model that will eventually be discarded rather than becoming part of the final deliver software. After preliminary requirement gathering is accomplished, a simple working model of the system is constructed to visually show the users what their requirements may look like, when they are implemented into finished system. It is also a rapid prototyping.

In the development of a system, tentative design is implemented, which is made possible by the use of the System Development Methodology. Under this project the author chose Throw-Away Prototyping methodology as the suitable methodology to be used when implementing pharmacy inventory management system and the reasons will be stated below. Below is the structural representation of the throw-away methodology as shown in the figure 3.1.

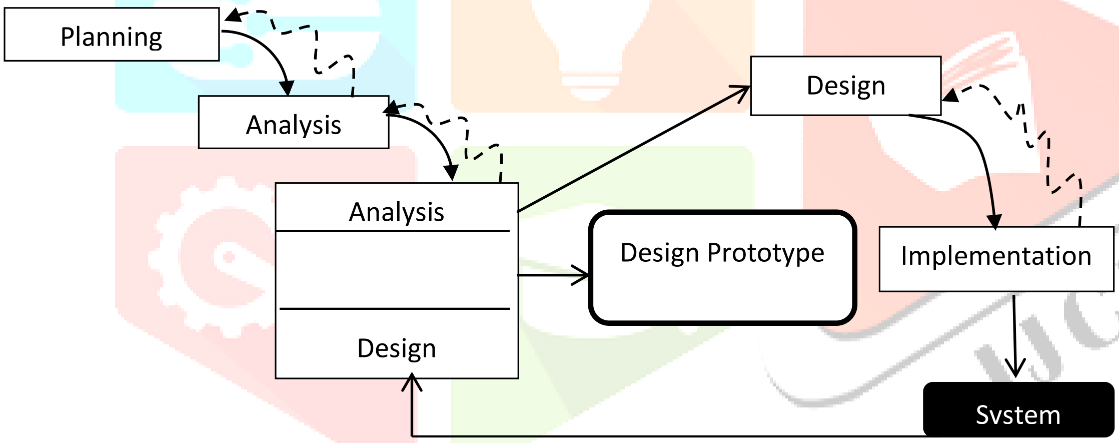


Figure 3.1: Throw-away prototyping model (Dennis, A. et al., 2010)

3.1.1 Planning

During the planning phase, we conducted some series of tasks which are listed as follows; select project topic, identify problems of the current system, defined project objectives and scope of the proposed system, conduct feasibility studies, project work plan, develop a time schedule (Gantt Chart) and prepare project proposal. The focal point of the planning phase is to understand why a system is being developed to implementation stage. This led the authors to conduct a series of investigation into the problems of current chatting system application, how they operate, improvement areas, and action to be taken in order to meet up with standard requirement specifications. The main goal of this project is to implement a secured chatting system application which will meet up with the user's specification.

3.1.2 Analysis

At this stage analysis is driven by business concerns, specifically, those of system users. Hence, there is a need for the existing chatting system and the definition of chatting requirement and priorities for a new or improved system and also for the purpose of understanding what, why, and how the system can be implemented.

3.1.3 Design

At this stage, the design architecture and data flow diagrams using Unified Modeling Language (UML) tools will be shown. Database and interface designs be created.

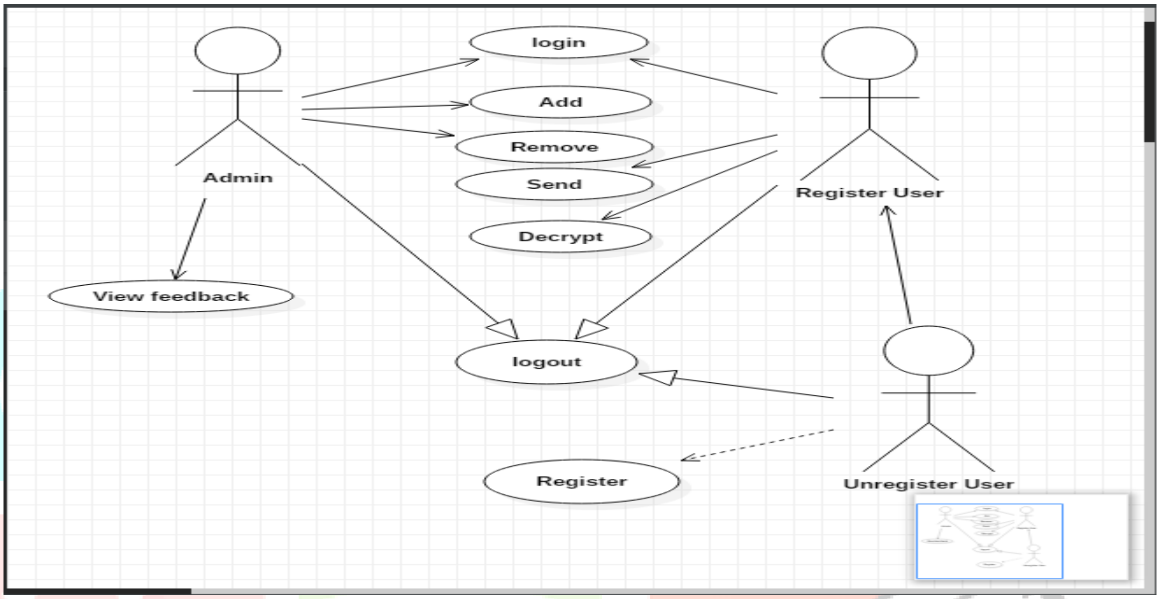
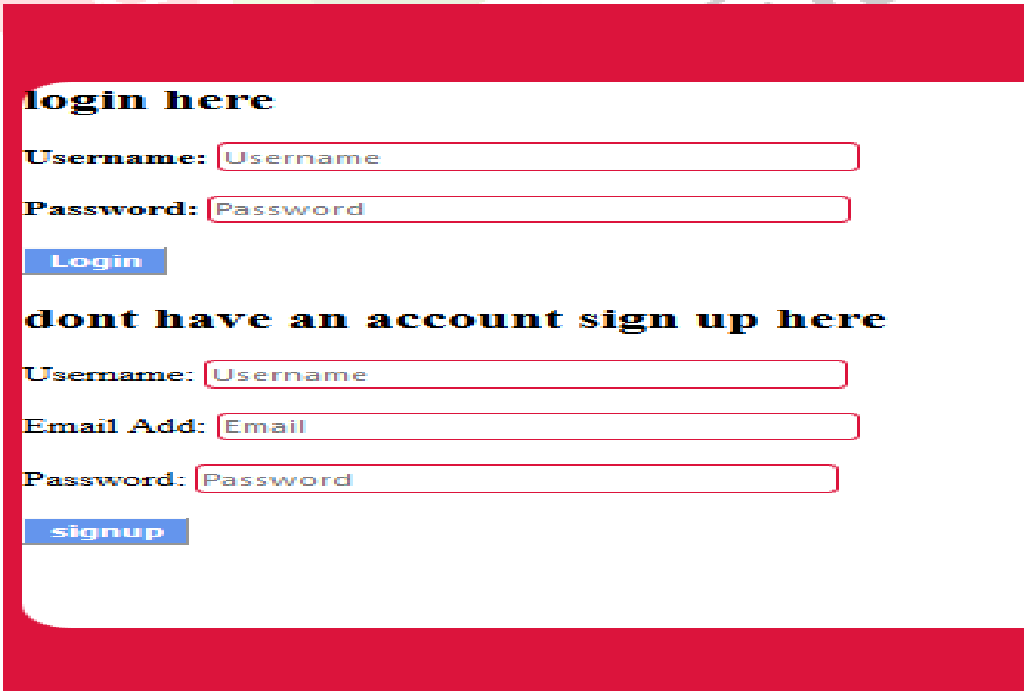


Figure 3.2: Use Case Diagram



login here

Username: Username

Password: Password

Login

dont have an account sign up here

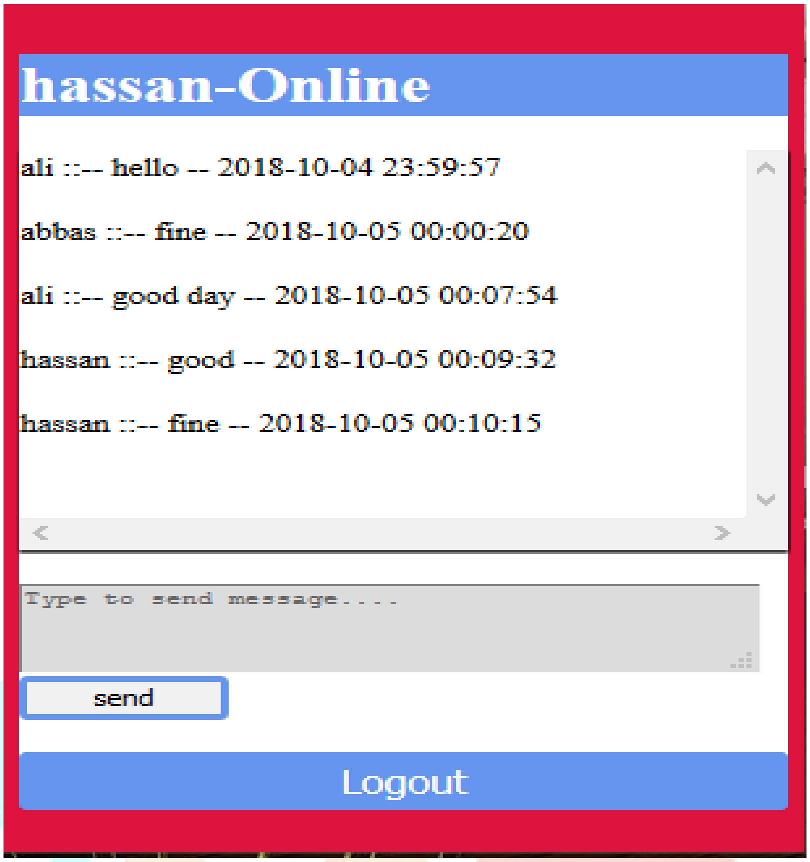
Username: Username

Email Add: Email

Password: Password

signup

Figure 3.3: Login System



hassan-Online

ali ::-- hello -- 2018-10-04 23:59:57

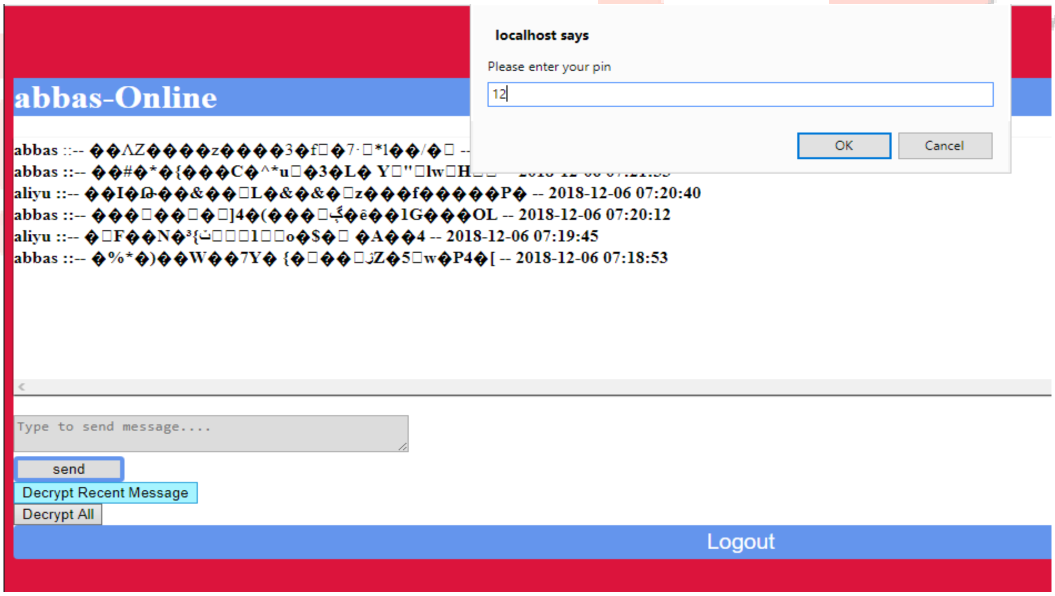
abbas ::-- fine -- 2018-10-05 00:00:20

ali ::-- good day -- 2018-10-05 00:07:54

hassan ::-- good -- 2018-10-05 00:09:32

hassan ::-- fine -- 2018-10-05 00:10:15

Figure 3.4: Chatting platform



abbas-Online

abbas ::-- ��ΛZ����z����3�f□�7·□*1��/�□ --
abbas ::-- ��#�*�{���C�^*u□�3�L� Y□"□lw□H□□ -- 2018-12-06 07:21:55
aliyu ::-- ��I�ꭥ���&���□L�&�&�□z���f�����P� -- 2018-12-06 07:20:40
abbas ::-- ���□���□�□]4�(���□ڴ�ê��1G���OL -- 2018-12-06 07:20:12
aliyu ::-- �□F��N�³{ٮ□□□1□□o�$�□ �A��4 -- 2018-12-06 07:19:45
abbas ::-- �%*�)��W��7Y� {�□���□ڗZ�5□w�P4�[-- 2018-12-06 07:18:53

localhost says

Please enter your pin

12

Figure 3.5: Encrypted Chatting Platform

3.1.4 Methods Used for the Analysis

The methods used for the research analysis are both quantitative and qualitative research methodology. Questionnaire were used to collect data on patient view perspective, interview with an experience chatting system user was carried out and observations of chatting system user performing operation were also used.

Table 3.1:

Proposed system	**Yes**	**No**
Have you been using chatting system before	100%	0%
Chatting system with security system	40%	60%
Secured system has better services	65%	35%
chatting system needs improvement	100%	0%

3.1.2 Implementation

At this stage of development, testing the system functionality with relevant test data and providing user manual for the proposed system will be put into consideration. System data and functionality testing will be conducted with validation made. Other non-functional requirements such as security and performance will be tested as well.

3.2 Chosen System Development Methodology

The chosen methodology is adopted based on its ability to supports iterative development, user involvement and flexibility. Among other reason why this methodology is selected is as follows:

i- It allows the researcher to find and solve issues in the technology world.
ii- It looks in-depth into matters that affect human behavior.
iii- It leads to new discoveries, because the deeper the researcher goes, the more problems discovered.
iv- It enables the developer to make changes at the preliminary stages of design

4.1 System *Analysis*

System analysis can be defined as the application of a disciplined logical, step-by-step approach to the identification, isolation, and clear statement of information problems of an organization. It is required of this system to construct a chatting software that will be able to convert text into enciphered codes and to also design another module that will reconvert them back to their original forms. As it was stated the principle of the theory of cryptography and crypto-analysis, each character text, A to Z lays an equipment secret representation that is assigned to it and added 1 to it. When the ciphered and deciphered program is running each character is converted to an equivalent enciphered form which is pointed out in a text file. File can serve as output of enciphered after the whole text have been typed, run and saved together with its encryption codes.

The decryption notice reconverts the enciphered codes (forms) to their original state, therefore making the software ciphered information useful to the user(s) in practice. The software is linked and converted to an executable file; hence an intruder will not read the source code. In the task or program writing and coding using the system specification, the programmer will write up programs necessary for carrying out the tasks in the system.

4.1.1 System *Requirement Specification*

A System Requirement Specification (SRS) is a structured document with the collection of information that embodies the requirement of a system. This system specification describes the function, performance and gives detail description of the system formation services and operational constraints, explaining what should be implemented. In the other side, they are all the capabilities and constraints that the new system must meet.

5.1 Summary

After a careful research and successful development of the secured chatting system, the author has come to summarize the findings by making a highlight on the important points. The author understood that the current system in operation have not been proven to have function in hundred percent, due to some factors which has been found. It is also well understood that the current system as issues of not decrypting the encrypted messages, with that is come to a conclusion that 70% of the current system is not secured. The proposed system will provide an operation in an efficient and effective method.

5.2 Conclusion

In conclusion, the integration of secured chatting system for users operations will have a great potential to reducing operational errors, poor accessibility to record information, and poor security of data entry. Almost 90% published studies and reviews according to findings did not meet the rigorous quality standard thereby resulting in poorly generalized standards across all chatting system. The author did literature review based on articles, journals and the internet to gather facts about the current chatting system. Questionnaires and interviews were also used as important resources to obtain accurate information about the prevailing situation in the problem domain. This study is proven that the integration of the chatting system will help in reducing the insecurity in chatting system. Microsoft packages such as visual studio web developer was used to develop the supporting application and online operation offer through a knowledge seeking novice programmers, which helps the author in achieving all the initial state objectives without challenges. The major problems with the current system has been analyzed and examined and a solution proposed to address the issues through proper identification and evaluation of methods, tools, and techniques used to develop solution.

5.3 Recommendation

Secured chatting System in the near future may be enhancing by adding certain other features, in the opinion of the author. Some of the recommended and perceived future improvement includes:

i. **Audio and Video:** uploading and downloading of audio and video files.

ii. **Instant Alert Feature:** sending alert massage to user when unauthorized users try to hack an account. The entire future enhancement will be achieved through advance research in literatures and necessary programming and design techniques needed to implement these features and deliver a friendly easy use graphical user interface for the users of secured chatting system.

References:

Agiledata. (2010) Data modelling 101, Available at: *http://www.agiledata.org/essays/dataModeling101.html#WhatIsDataModeling* (Retrieved 19 March 2012).

Al-Kadi, Ibrahim A. (1992). *"The origins of cryptology: The Arab contributions". Cryptologia.* ***16*** *(2): 97–126. doi:10.1080/0161-119291866801*.

Barry W. Boehm, A. (2006), *Spiral Model of Software Development and Enhancement, Computer, May 2006*, IEEE, pp.61-72.

Bonneau, J., Fahl, S., Perl, H., Goldberg, I., & Smith, M. (n.d.). SoK: Secure Messaging 1, 1–25.

Esiefa, M.B. (2005). Management Information system, page 52-72,

Francis, M. (2017), Importance of Application Security, Available at*: https://www.veracode.com* (Retrieved 24th May, 2018).

Gannon, James (2001). Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century. Washington, D.C.: Brassey's. ISBN 978-1574883671.

Grady B., Jim R., and Ivar J. (1999). Unified Modeling Language—User's Guide, Addison-Wesley, 1999.

Gedda, R. (2016). Cybersecurity -Threats Challenges Opportunities, (November).

Guide, A. B. (2017). *A beginners guide*. *Open Data Security*.

Hakim, Joy (1995). A History of US: War, Peace and all that Jazz. New York: Oxford University Press. ISBN 978-0195095142.

Internet Engineering Task Force (2000). *"Internet Security Glossary" RFC* 2828. Retrieved 26 March 2015.

Kelly, Jon (2010). *"Instant messaging: This conversation is terminated"*. BBC. Retrieved 14 March 2018.

Mason, J. (2018), Cyber-Security Statistics, Available at: *https://thebesttvpn.com*
Retrieved 22nd May, 2018.

Mason, J. (2017), Cryptography, Available at*: https://www.cnbc.com* (Retrieved 24th May, 2018).

MacAfee, G. (2018), Cost of Computer Crime, Available at*: http://www.cnbc.com* Retrieved 22nd May, 2018).

Merriam (2015) *"Cryptology (definition)". Merriam-Webster's Collegiate Dictionary* (11th ed.). *Merriam-Webster*. (Retrieved 26 March 2015).

Primer, T. (2017). *Real-time Collaboration for Enterprises and Service Providers Oracle Communications Instant Messaging Server – Technical Primer*.

Prof. A.I. Adesina. (2002) "Introduction to computer" page 180-198,

Sasko, J., & Chao, K. (2007). *Security of Instant Messengers*.

Schneier, Bruce. (2016). *"Multi-Encrypting Messengers – in: A Worldwide Survey of Encryption Products,"* (PDF). Retrieved 28 March 2017.

Schrödel, Tobias (2008). "Breaking Short Vigenère Ciphers". *Cryptologia*. **32** (4): 334–337. doi:10.1080/01611190802336097.

Tom Van Vleck. *"Instant Messaging on CTSS and Multics"*. Multicians.org. Retrieved 2012-05-11.

Walsh, L.(2003),Information Security Management, Available at: *http://infosecuritymag.techtarget.com* (Accessed 9th September, 2018).