Secured Talks

Gunavathie M A[1], G. Anitha[2], J.Joslin Iyda[3], S. Kumari[4], S. Aiswarya[5]

[1]Assistant Professor, Department of IT, Panimalar Engineering College, gunavathie.ap@gmail.com

[2,]Assistant Professor (SG Grade), Department of IT, Rajalakshmi Engineering College, anitha.g@rajalakshmi.edu.in

[3]Assistant Professor (SG Grade), Department of IT, Rajalakshmi Engineering College, josliniyda.j@gmail.com

[4]Assistant Professor, Department of IT, Panimalar Engineering College,Sudhakar.kumari@gmail.com

[5]Assistant Professor, Department of Information Technology, SriVenkateswara College of Engineering, aiswaryas@svce.ac.in

Article Info
Page Number: 655 – 664
Publication Issue:
Vol. 71 No. 3 (2022)

Article History
***Article Received:** 12 January 2022*
***Revised:** 25 February 2022*
***Accepted:** 20 April 2022*
***Publication:** 09 June 2022*

Abstract:

Current trends in mobile application development are centred on the market for mobile applications. Client-server architecture is typically used by mobile applications.A majority of security issues are found in mobile applications. Uncertain storage of data is the primary concern, affecting 76 percent of mobile applications. Secret Passwords, financial data, private information, and communication are all in danger.These oversights can cause serious results, including monetary losses for people. The proliferation of mobile devices has created other issues like cyber harassment, which appears to be on the rise.Through our work, we demonstrate how to combat cyber-harassment by preventing junk mail messages and online threats to students' well-being, schooling, and relationships with their peers.A self-destroying identity is used to enhance privacy while users interact with the app daily.Cybersecurity experts view the success of more innovative and effective malware defence mechanisms as an urgent need.Following that, speculative observations about future research directions are made regarding the attack patterns associated with emerging technologies, such as those associated with social media, cloud computing, smartphones, and critical infrastructure.

Keywords: self-destroying, privacy, communication

1. Introduction

As part of their security features, modern mobile operating systems provide a number of features.Apps have access only to files within their sandboxes, and user access controls prevent access to data. Yet, mistakes made in creating or writing code for mobile applications can cause security holes which can be exploited by attackers.In addition to probing for weaknesses in the client and server, security checks for mobile applications also include data transmission between the two.Various security mechanisms are built into mobile operating systems. Installed applications have access to only files inside their sandbox directory by default, and they can't access other files unless they edit their system files.Although developers design and write codes for mobile apps, errors can cause security gaps and be exploited by attackers.Messages are sent back and forth between clients and servers via request-response messaging. A request is sent by the client, and a response is sent back by the server.This represents inter-process communication. To communicate with computers, they need to speak the same language and follow the same rules, so the client and server know what to expect.In a communication protocol, the rules are laid out and the language is defined.Protocols between clients and servers operate at the application level. Basic communication patterns are defined by the protocol.An application programming interface (API), serving as an abstraction layer for interaction with services, may further formalize the exchange.The communication is limited to a specific format, simplifying parsing.Access is abstracted so that cross-platform data exchange is simplified. A mobile application's security must include checking for weaknesses in the client and server, as well as the transmission of dataThis paper covers all three aspects.Furthermore, we will discuss threats to users, such as those associated with mobile application server-client interactions.We conclude the paper with a detailed explanation of our methodology and data sources.

2. Literature Survey

Author explained [1] the software that protects a user from drive-by download attacks.The list contains the files that were downloaded via the URL visitation process at the backend.With a malware detection tool online, it scans the files and displays the results in an interactive SQLite database and visual presentation.These files display details about malware graphically. Researchers [2] presented a web-based framework that detects malware on Android devices.By analysing apps dynamically, the proposed framework detects Android malware.Our proposed framework was trained to spot malware fromapps by selecting features gained from implementing feature selection techniques.Social media like Google [3] and Facebook has given users lot of refreshing options to store, search and communicate. Even the users are aware of the issues in the social media, they couldn't even stop using that. The users should be made aware of the secure usage of social media. Models were developed for identifying vulnerableentitiesamid a set of entities by researchers [4] and predicting how susceptible they are. Three kinds of features were explored for prediction: linguistic, network and behavioural ones.

Researchers [5] explored the privacy and security concerns of online social networks like Myspace, Twitter, Facebook etc. They also explored the ways to mitigate the privacy and security concerns and to have secure communication in online social networks. The authors proposed a system [6] for controlling cyber harassment, such as junk mail messages and unsolicited phone calls.Using self-destructing identities, an advanced smart app has been created and evaluatedto ensure privacy in daily communications.The social media application Facebook [7] has a lot of facilities that will enable the users to communicate very easily. But the Facebook has a lot of security issues [8] which the users are even unaware of. The researchers in [9] discussed the privacy issues in the Social media network. They discussed issuesrelated to security, privacy, and accessibility in both Mobile and Web applications.

Cryptographic counting control is a new method for Self-destroying message which meets forward secrecy requirements [10].It is impossible to recover messages that have passed into the "destroyed" state, including the sender, the provider of service, and the key organization module.Authors [11] demonstratedthe effectiveness of Deep Learning algorithms in classifying eating disorder-related images in a proof-of-concept demonstration.Throughout this study, a detailed survey is employed to determine how much personal information members reveal at the period of joining social networking sites and during their subsequent interactions.We examine their types of information, their level of understanding of how their information is protected by social networking sites, and their understanding of over-sharing risks.Moreover, this study examines the shape of privacy settings and disclosure of personal information based on gender, age, education, and privacy concerns.

JavaScript malware detection and prevention that is small, low-cost, and fast enough to be implemented in the browser was proposed by researchers in [12].In order to identify syntax elements associated with malware, the researchers applied Bayesian classification to the JavaScript abstract syntax tree. Authors in [13] proposed an effort to combine three different approaches for Wikipedia vandalism detection. The approaches used for integration are Spatiotemporal metadata analysis,and features of natural language processing. They did the task of positioning and detecting new vandalism. The approaches were found to be performing well in detecting vandalism. Researchers in [14] analysed the malware in smart devices. They gave detailed analysis to detect the malware and the suspicious software. In response to an analysis of drive-by download attacks, authors[15] proposed a framework that takes into consideration possible browser state changes that may be encountered when rendering HTML documents.Frameworks like this can be used to recognize new structures that have not yet been developed and to infer the difficulties related to the use of those features in drive-by download detection

Using machine learning techniques, Authors in [16] evaluated the permissions from Android applications in order to detect malicious applications.Third-party content is integrated into social networking platforms. This allows developers to access data about users, and allows site enhancements. It poses serious privacy risks for third-party developers to gain access to the user's data.Based on the findings of researchers [17], the most popular Facebook apps could remain functional with just an anonymized social graph and placeholders for users' information.Authors studied [18] the practices and guidelines of the analysed applications and found that they generally do not follow industry standards and guidelines, nor do they comply with lawfullimitationslevied by modern data protection regulations, therefore threatening the privacy of users.Their analysis of selected mobile health applications includes both static and dynamic testing, as well as custom-made testing of functionalities of each application. According to [19], information privacy is conceptualized, associated with other constructs, and contextualized.As well as taking into account actual outcomes and privacy concerns, positivist empirical studies add the most value.

A vast public dataset of 11000 Android apps contains 123 dynamic permissions extracted by researchers [20].A number of machine learning approaches were evaluated for detecting malicious Android apps. The research [21] presented here uses dynamic studybuilt on machine learning to recognize malware on real devices.The use of machine learning algorithms to compare the effectiveness of emulator-based and device-based detection is investigated using an automatic tool to extract dynamic features from Android phones.

Authors [22] presented a software application to launch real-time communication between operators/users.It will be possible for users to communicate via text messages with another user through the internet using the Android system.Users need to connect their devices to the internet for the system to work.Based on Android, this application utilizes Firebase and is backed by Google.Applications concealing their activities should be considered suspicious by application marketplaces and users.Since activity concealing has such a nature and intent, users are put at risk as a result.In this study on [23], they focus on characterizations and detections of self-hiding techniques, such as hiding the application or removing traces.The author [24] explored security limitations in general purpose computers and mobile phones and how they relate to reconciling governance practices in use today.

3. Proposed Work

Our system allows you to communicate digitally without compromising privacy or security.Our self-destructing, screenshot-proof, and encrypted messages assure you that your private communications remain private. When a message is decrypted, its vulnerability is exposed. Our system lets you archive, print, and even forward messages.They will disappear from the user device and even from the database after that.

SVM technique discovered the malware in hybrid analysis resulting in less training effort because it discovered malware.With our malware detection systems, we eliminate the flaws of signature-based and behaviour-based detection, incorporating the hybrid analysis for effective malware detection.Using this method, you're able to detect unknown malware while minimizing false positives.Our virtual environment monitors the user's profile in social media networks and their location. The user should be able to authenticate known and unknown users according to the requests they receive.We have a system to protect privacy by sending the unknown user self-destructive messages which will be deleted once viewed. Tracking their location is also a feature in order to protect privacy.Also, we provide the ability to share the location regardless of our current location. It is shown in fig 3.1

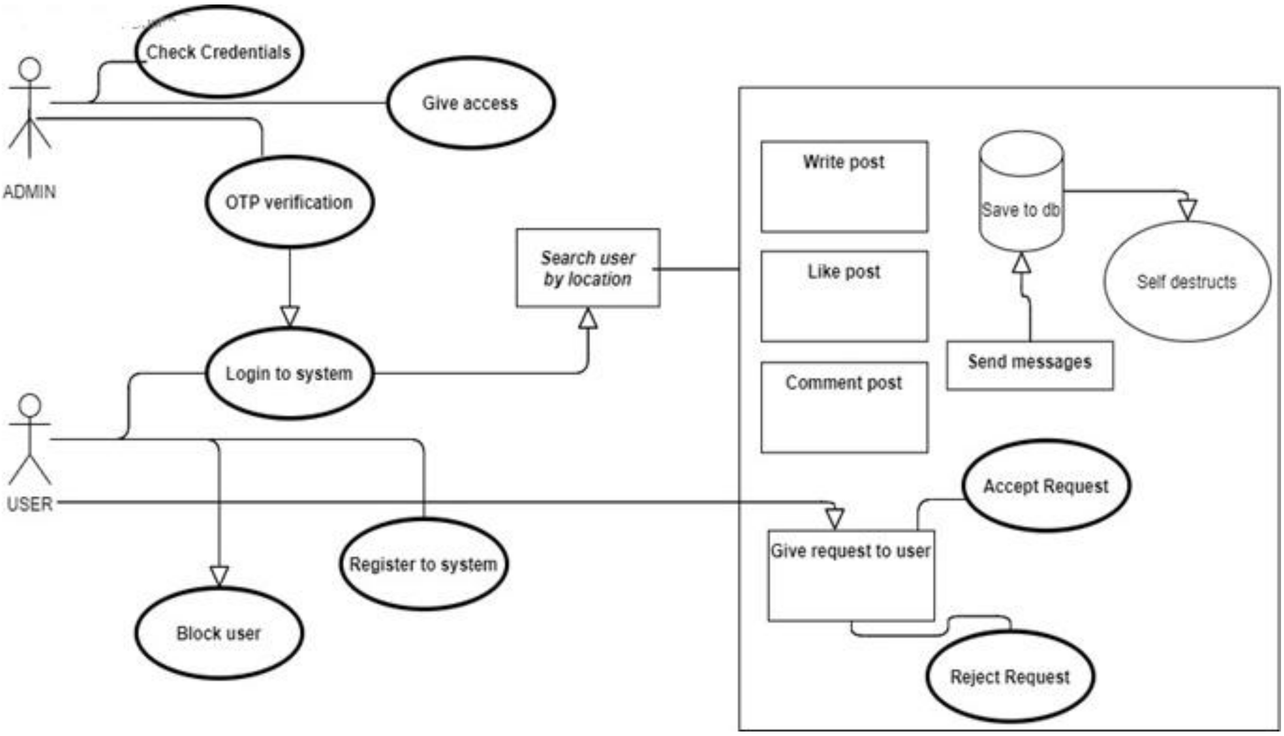


Fig.3.1 System Architecture.

LIST OF MODULES:

- Authentication
- System privacy
- Location tracking

Module 1: Authentication

Authentication occurs when the client or server verify the identity of the user. The authentication process is typically implemented by a user name and password. A server uses it to determine if the user is authorized.

Module 2: System privacy

Privacy gives people the opportunity to choose with whom they want to share their feelings and thoughts. Privacy protects information that they do not want to be shared publicly.

Module 3: Location tracking

Alocation tracking system involves physically locating and electronically recording and tracking the movements of individuals or objects.Location tracking technology is used in everyday activities such as GPS navigation, mapping digital photos, and searching for local businesses using common apps.The project will track the location within a range of 5 km and display the notification to the user.

4. Experimental Results

The proposed system has been implemented in java and the screenshots are shown below

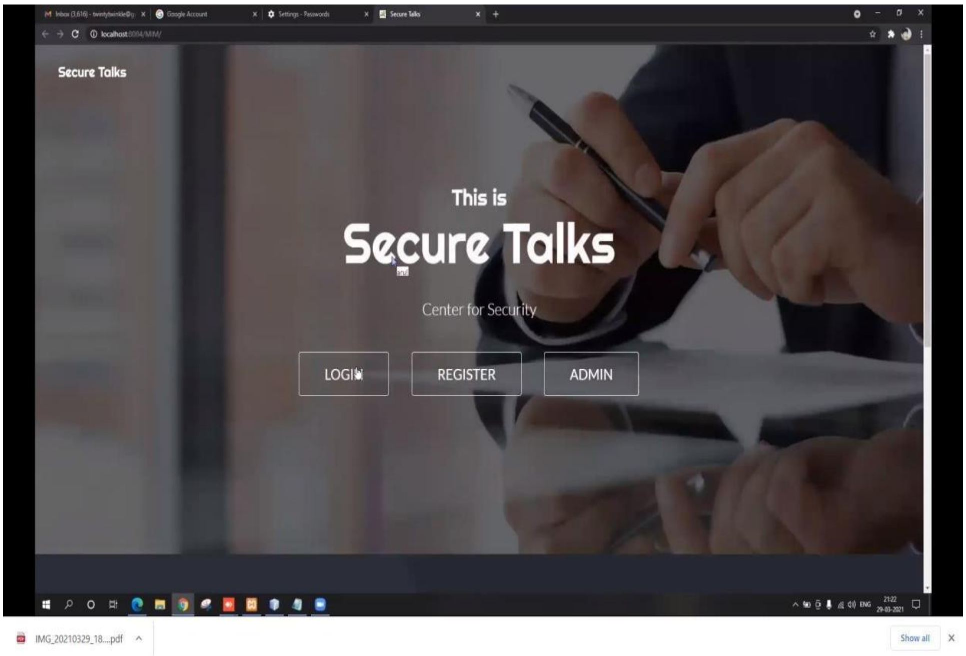
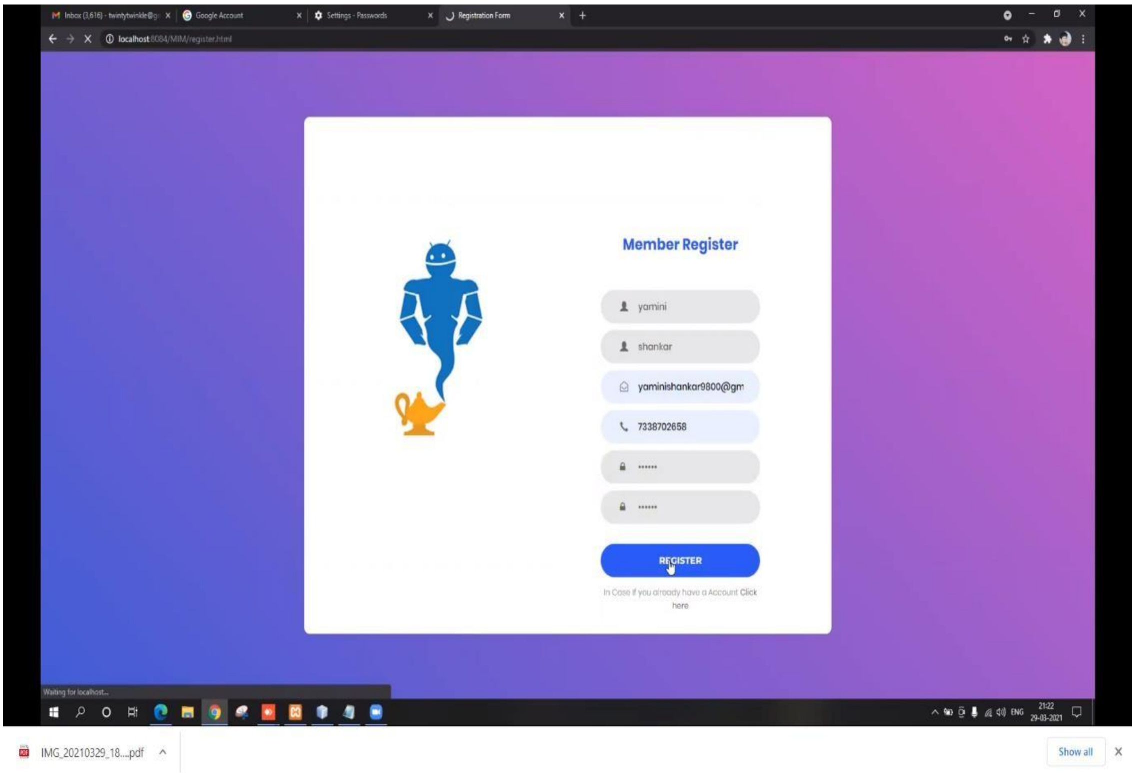


Fig 4.1 Secure Talks Home Screen

The Fig 4.1 represents the home screen of our project Secure Talks. In this screen we have three tabs, which includes Login, Register, Admin. Login tab is for the users who were already signed up. In the login tab, they need to provide only the username and the password. Register tab is for the new users who want to sign up for the first time.


Member Register

yamini

shankar

yaminishankar9800@gm

7338702658

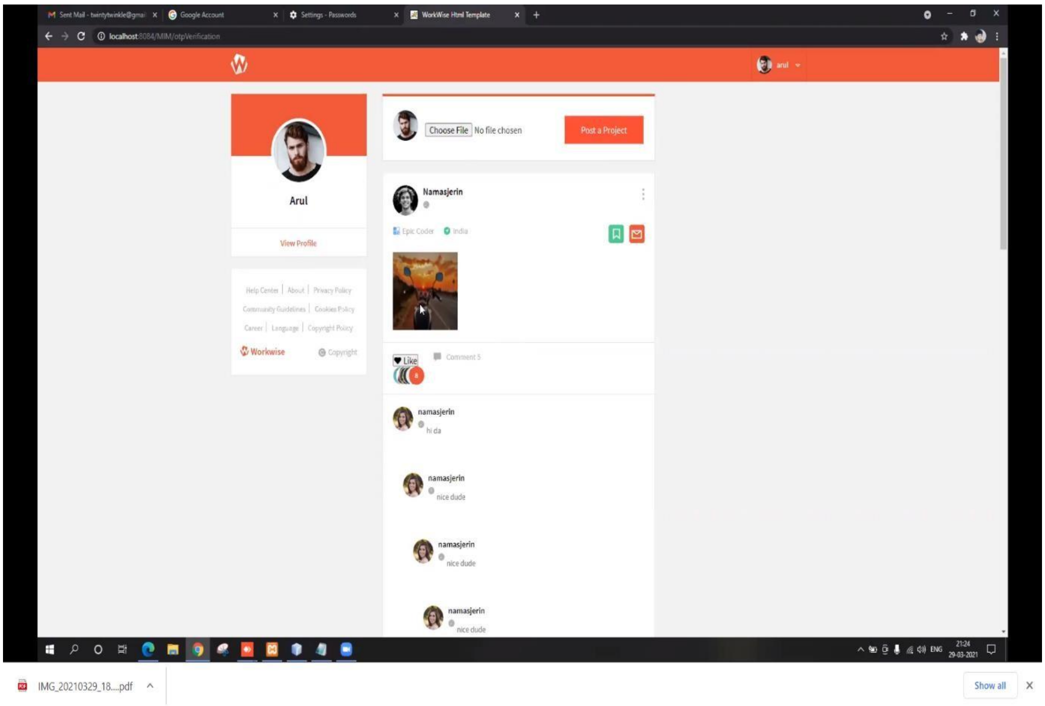
••••••

••••••

In Case if you already have a Account Click here

Fig 4.2 Secure Talks Registration Screen

The Fig 4.2 represents the registration screen of our project Secure Talks. In this screen we need to providenecessary details like name, username , password and email id to get registered.


WorkWise Html Template
localhost:8084/MIM/otpVerification
Arul
View Profile
Choose File No file chosen
Post a Project
Help Center | About | Privacy Policy
Community Guidelines | Cookies Policy
Career | Language | Copyright Policy
Workwise
Copyright
Epic Coder
India
Like
Comment 5
IMG_20210329_18....pdf
Show all

Namasjerin

namasjerin
hi da

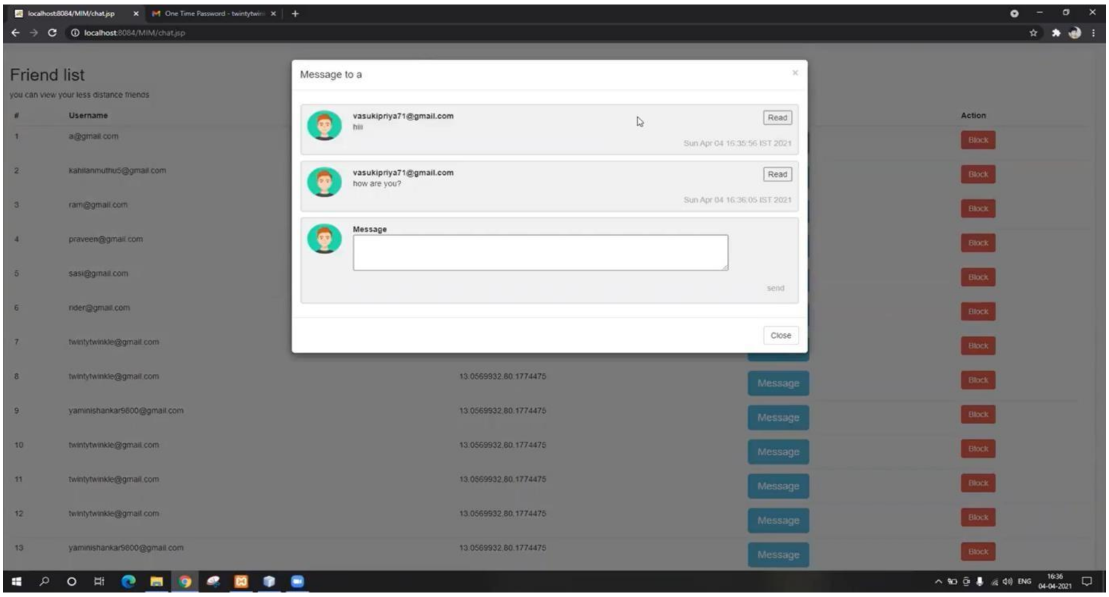
namasjerin
nice dude

namasjerin
nice dude

namasjerin
nice dude

Fig 4.3 Secure Talks User Account Screen

The Fig 4.3 represents the user interface screen of our project Secure Talks, where the users can share their post, like and comment on their friend's posts. Every user can change their profile picture on their wish.



Friend list

you can view your less distance friends

#	Username			Action
1	a@gmail.com			Block
2	kahilanmuthu5@gmail.com			Block
3	ram@gmail.com			Block
4	praveen@gmail.com			Block
5	sasi@gmail.com			Block
6	rider@gmail.com			Block
7	twintytwinkle@gmail.com			Block
8	twintytwinkle@gmail.com	13.0569932,80.1774475	Message	Block
9	yaminishankar9800@gmail.com	13.0569932,80.1774475	Message	Block
10	twintytwinkle@gmail.com	13.0569932,80.1774475	Message	Block
11	twintytwinkle@gmail.com	13.0569932,80.1774475	Message	Block
12	twintytwinkle@gmail.com	13.0569932,80.1774475	Message	Block
13	yaminishankar9800@gmail.com	13.0569932,80.1774475	Message	Block

Message to a

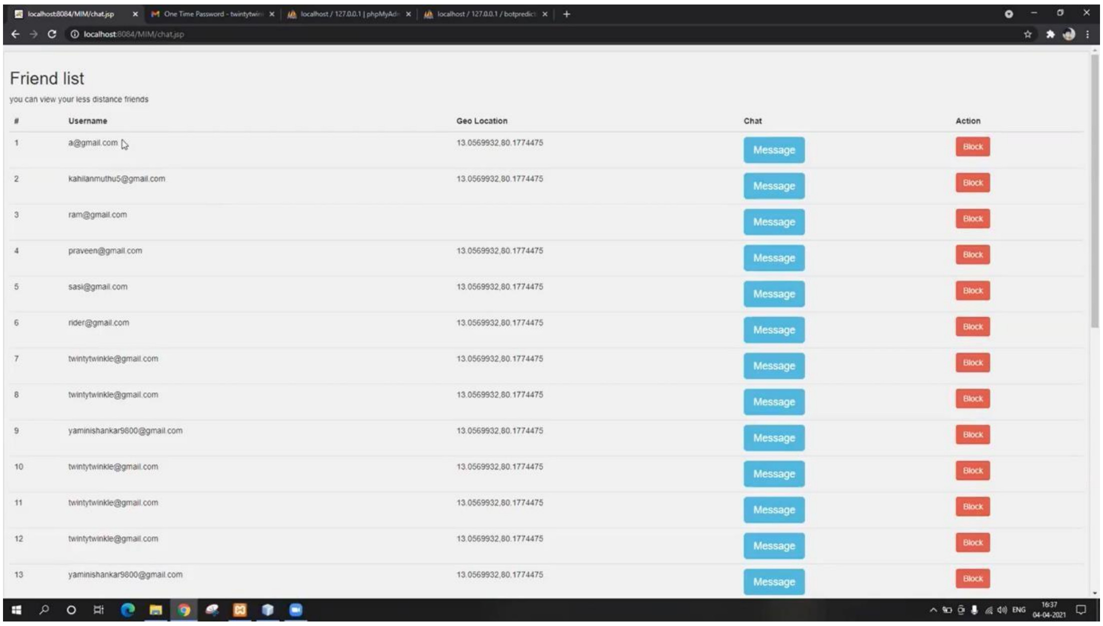
vasukipriya71@gmail.com
hiii
Read
Sun Apr 04 16:35:56 IST 2021

vasukipriya71@gmail.com
how are you?
Read
Sun Apr 04 16:36:05 IST 2021

Message

Fig 4.4 Secure Talks Messaging Interface

The Fig 4.4 represents the messaging interface of our project Secure Talks. In this screen we can send messages to our friends and we can also self-destruct the message by clicking on the Read button.



Friend list

you can view your less distance friends

#	Username	Geo Location	Chat	Action
1	a@gmail.com	13.0569932,80.1774475	Message	Block
2	kahilanmuthu5@gmail.com	13.0569932,80.1774475	Message	Block
3	ram@gmail.com		Message	Block
4	praveen@gmail.com	13.0569932,80.1774475	Message	Block
5	sasi@gmail.com	13.0569932,80.1774475	Message	Block
6	rider@gmail.com	13.0569932,80.1774475	Message	Block
7	twintytwinkle@gmail.com	13.0569932,80.1774475	Message	Block
8	twintytwinkle@gmail.com	13.0569932,80.1774475	Message	Block
9	yaminishankar9800@gmail.com	13.0569932,80.1774475	Message	Block
10	twintytwinkle@gmail.com	13.0569932,80.1774475	Message	Block
11	twintytwinkle@gmail.com	13.0569932,80.1774475	Message	Block
12	twintytwinkle@gmail.com	13.0569932,80.1774475	Message	Block
13	yaminishankar9800@gmail.com	13.0569932,80.1774475	Message	Block

localhost:8084/MIM/chat.jsp
One Time Password - twintytwin
localhost / 127.0.0.1 | phpMyAd
localhost / 127.0.0.1 / botpredict
localhost:8084/MIM/chat.jsp
ENG
16:37
04-04-2021

Fig 4.5 Secure Talks Friend List Screen

Fig 4.5 represents the Friend List screen of our project Secure Talks. In this screen we can seethe list of friends and unknown users who are within two- a kilometre radius. We can also block the users for our wish.

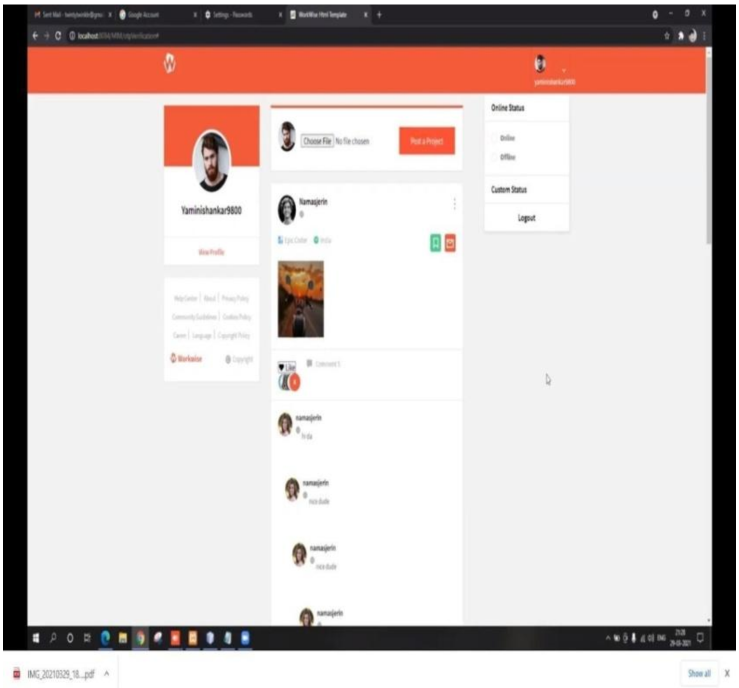


Fig 4.6 Secure Talks User Logout Screen

The Fig 4.6 represents the logout screen of our project Secure Talks. If we click Logout option, we will be re-directed to the home screen.

5. Conclusion

SMN (Social Media Networking)refers to a web concept used primarily for social collaboration and entertaining purposes. SMN is used as a value-added service by leading organizations around the world today.There are higher percentages of successful businesses that are partly based on social media or that use social media as a complement to their business. The system proposed is low-cost since all the software required is freely available, and it presents a wide range of benefits to social media users.In an experiment, 95.8% of the data was detected using static, 97.1% using dynamic, and 98.7% using hybrid methods.

6. Future Enhancements

As new tools and consumer demands emerge, digital media is becoming better and more accessible.As the project develops, it will be developed so that everyone in the world can use it with high security and better Graphical user interface.

7. References

1. Ahuja Laxmi ;SubhranilSom; Sunil Kumar Khatri, “Prevention of Drive by Download Attack (URL Malware Detector)”, Third International Conference on Inventive Systems and Control (ICISC), 2019, 10.1109/ICISC44355.2019.9036341

2. Arvind Mahindru, A L Sangal, “framework for Android malware detection using machine learning techniques”, Neural Computing and Applications, Publishedin:Springer

3. C. Dwyer, “Privacy in the age of Google and Facebook”, IEEE Technol. Soc. Mag.30 (3) (2011) 58–63.

4. C. Wagner, S. Mitter, C. Körner, M. Strohmaier, “When social bots attack: modeling susceptibility of users in online social networks” , Proceedings of the International Conference on World wide web (WWW), vol.12, 2012.

5. C. Zhang, J. Sun, X. Zhu, Y. Fang, “Privacy and security for online social networks: challenges and opportunities”, IEEE Netw. 24 (4) (2010) 13–18

6. CharalamposHoulis,ConstantinosPatsakis, Efthimios Alepis, “Smart Android Application using Self-Destructive Identities against Cyber Harassment”, International Conference on Information, Intelligence, Systems and Applications (IISA), 2019

7. E. Protalinski, 56% of employers check applicants’ Facebook, LinkedIn, Twitter, 2012, URL: http://www.zdnet.com/article/

8. E. Staff, Verisign: 1.5 m Facebook accounts for sale in web forum, 2010, URL: http://www.pcmag.com/article2/0,2817,2363004,00.asp.

9. E. Zheleva, L. Getoor, “Privacy in Social Networks: A Survey”,Social Network Data AnalyticsSpringer,pp. 277–306.

10. Yan Zhu, LiguangYang, Di Ma, “SecureSnaps: A New Forward Secrecy Cryptosystem for Self- destructing Messages in Mobile Services”, IEEE International Conference on Mobile Services, 2015

11. Samsara N. Counts, Justine-Louise Manning, Robert Pless, “Characterizing the Visual Social Media Environment of Eating Disorders”, IEEE Applied Imagery Pattern Recognition Workshop (AIPR) 2018

12. Charlie Curtsinger, Ben Livshits, Benjamin Goth Zorn, Christian Seifert,“ZOZZLE: Fast and Precise In-Browser JavaScript Malware Detection”, Proceedings of the 20th USENIX conference on SecurityAugust 2011

13. B. Thomas Adler, Luca de Alfaro, Santiago M. Mola-Velasco,Paolo Rosso, Andrew G. West, “Wikipedia Vandalism Detection: CombiningNatural Language, Metadata, and ReputationFeatures”, Proceedings of the 12th International Conference on Intelligent Text Processing andComputational Linguistics, LNCS 6609, pp. 277-288. Tokyo, Japan.

14. Guillermo Suarez-Tangil, Juan E. Tapiador, Pedro Peris-Lopez, and Arturo Ribagorda, “Evolution, Detection and Analysis of Malware for Smart Devices”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, October 2013, DOI: 10.1109/SURV.2013.101613.00077

15. Van Lam Le, Ian Welch, Xiaoying Gao, Peter Komisarczuk, “Anatomy of Drive-by Download Attack”, Proceedings of the Eleventh Australasian Information Security Conference (AISC 2013), Adelaide, Australia.

16. Borja Sanz, Igor Santos, Carlos Laorden, Xabier Ugarte-Pedrero, Pablo Garcia Bringas and Gonzalo Alvarez, “PUMA: Permission Usage to detect Malware inAndroid”. International Joint Conference CISIS’12-ICEUTE' 12-SOCO' 12, pp.289-298.

17. Adrienne Felt, David Evans, “Privacy Protection for Social networking Platform”, Workshop on Web 2.0 Security and Privacy. Oakland, CA. 22 May 2008.

18. Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, AgustiSolanas,and ConstantinosPatsakis, “Security and Privacy Analysis of Mobile HealthApplications: The Alarming State of Practice”, IEEE Access · January 2018

19. H. Jeff Smith, Tamara Dinev, Heng Xu, “Information Privacy Research:An Interdisciplinary Review”, MIS Quarterly Vol. 35 No. 4 pp. 989-1015/December 2011.

20. Arvind Mahindru, Paramvir Singh, “Dynamic Permissions based Android Malware Detection using Machine Learning Techniques”, Proceedings of the 10th Innovations in Software Engineering ConferenceFebruary 2017 Pages 202–210.

21. Mohammed K. Alzaylaee, Suleiman Y. Yerima, SakirSezer, “Emulator vs real phone: Android malware detection using machine learning”, Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics, March 2017 Pages 65–72

22. Sai Spandhana Reddy Emmadi, Sirisha Potluri,“Android based instant messaging application using firebase”, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-7 Issue-5S2, January 2019

23. Zhiyong Shan, Iulian Neamtiu, “Self-hiding behavior in Android apps: detection and characterization”,Proceedings of the 40th International Conference on Software EngineeringMay 2018 Pages 728–739.

24. N. Husted, H. Saïdi, and A. Gehani, “Smartphone Security Limitations: Conflicting Traditions,” Proc. 2011 Workshop on Governance of Technology, Information, and Policies, ACM, 2011, pp. 5-12.