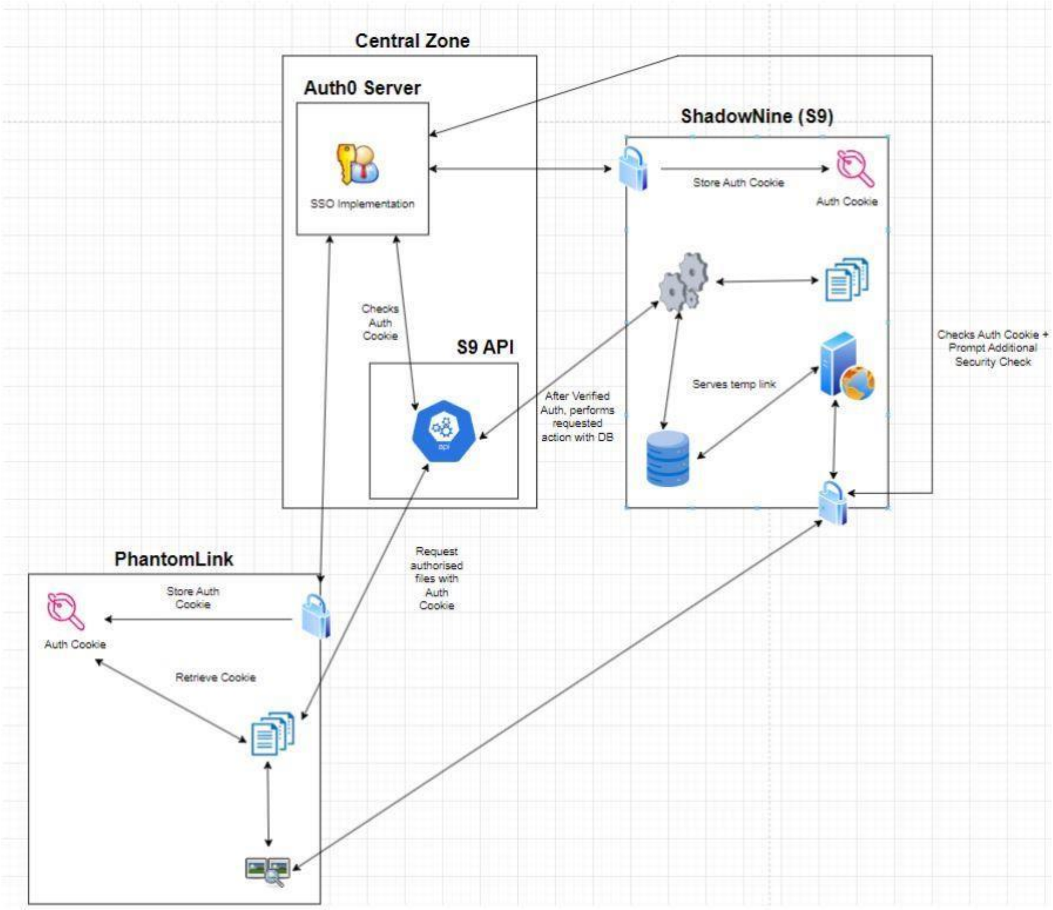
1. Project Description

Ghostnet is a secure military ecosystem consisting of a Secure Military Communications mobile application, PhantomLink and a Secure File Sharing & Management System, ShadowNine (S9). The purpose of Ghostnet is to establish a comprehensive and impenetrable secure military ecosystem that prioritizes the confidentiality, integrity, and availability of sensitive information critical to military operations. To allow file sharing in PhantomLink with users, it is done through ShadowNine where users can retrieve file links that will expire over time. Ghostnet is designed to create a clandestine network, rendering our military data and communications virtually '*invisible*' to unauthorized entities, and hence securing our data assets.

Ecosystem

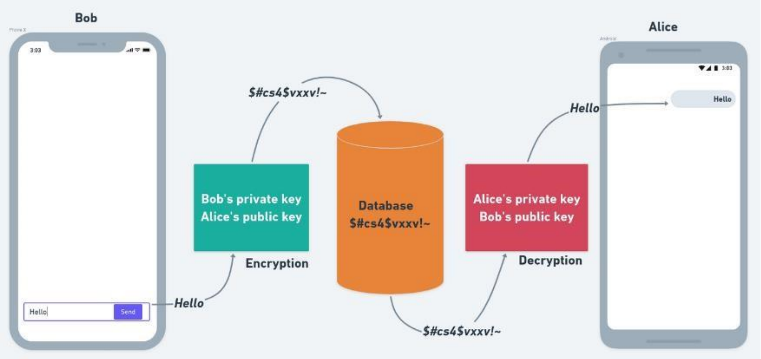
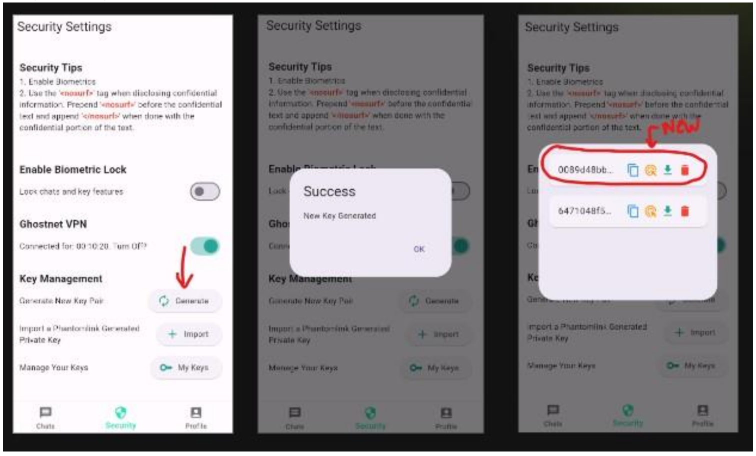
The integration of all components that form the ecosystem is through file management and sharing. The diagram below illustrates how all the components of Ghostnet interact with one another to form our file ecosystem.

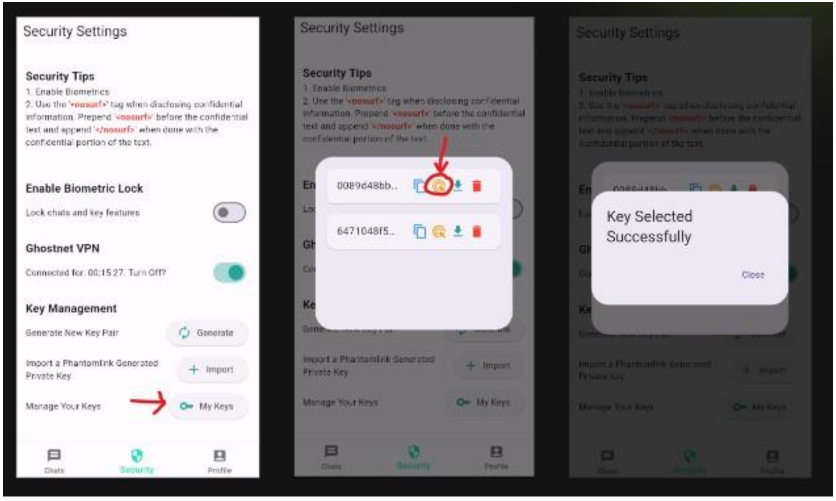
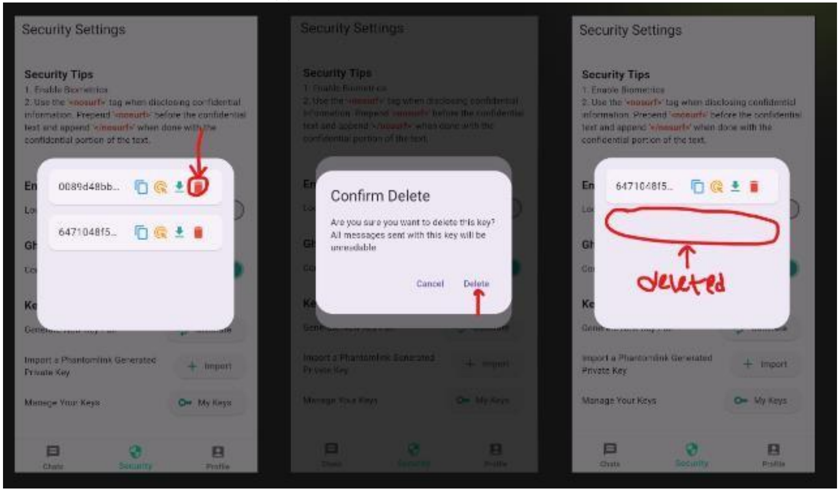


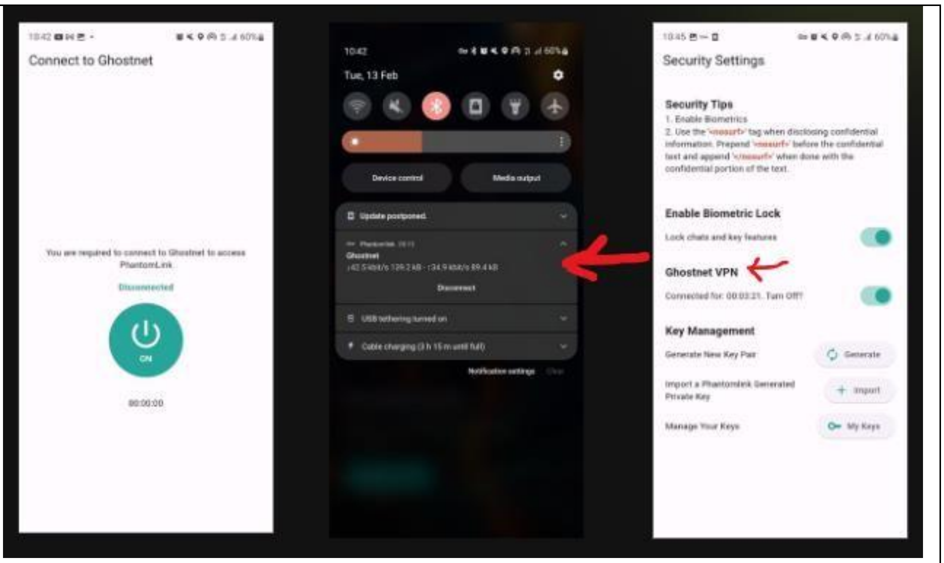
My Role

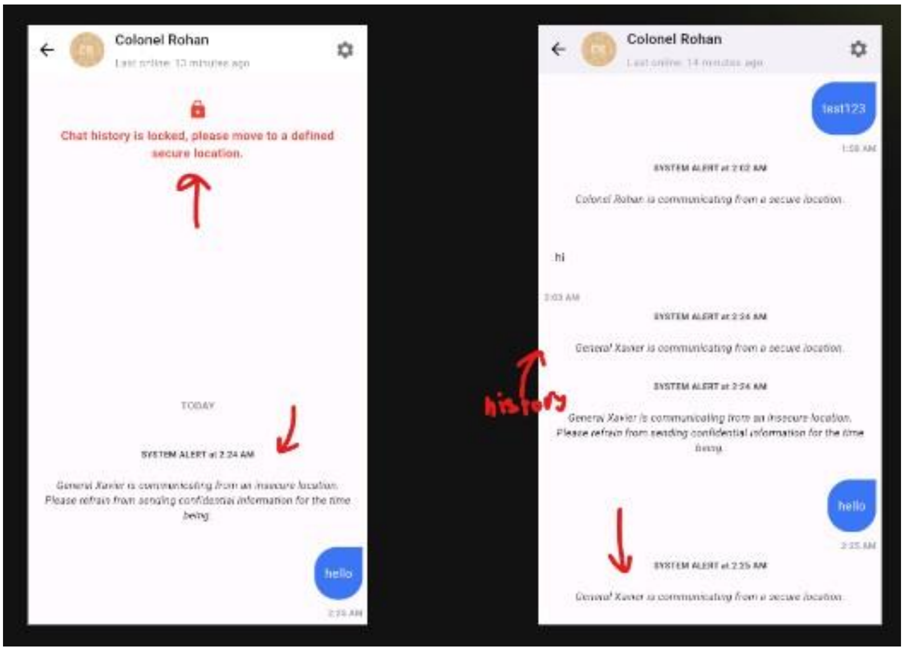
I worked primarily on PhantomLink. The idea was to build a proof-of-concept (POC) of a secure communications app that can be implemented in government organisations. PhantomLink is for the most part independent of ShadowNine. Only the file management aspect is integrated with ShadowNine.

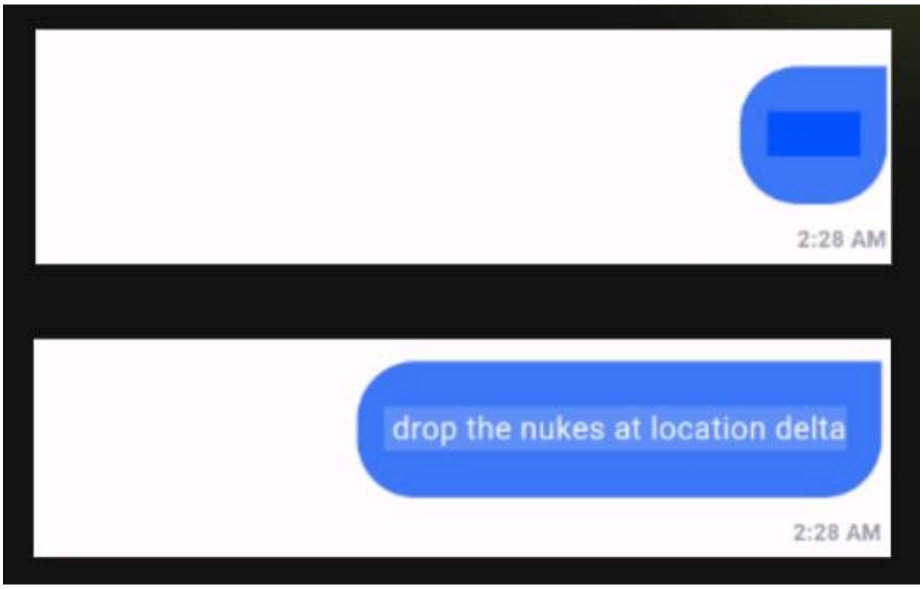
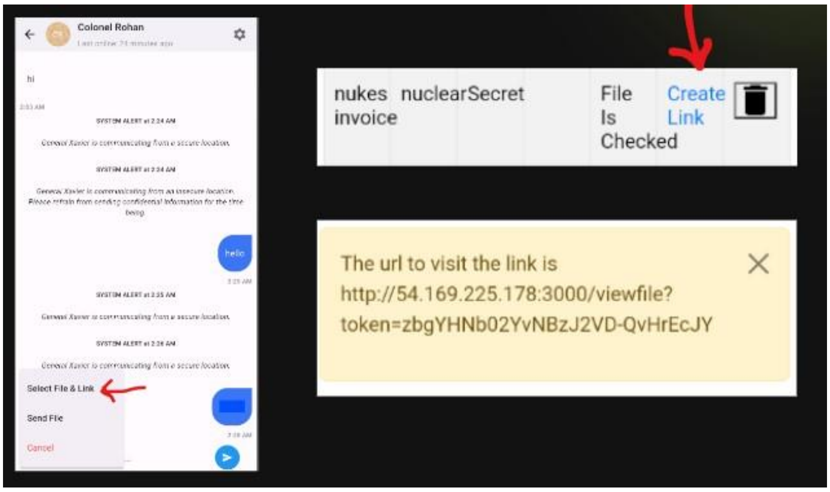
2. Individual Tasks

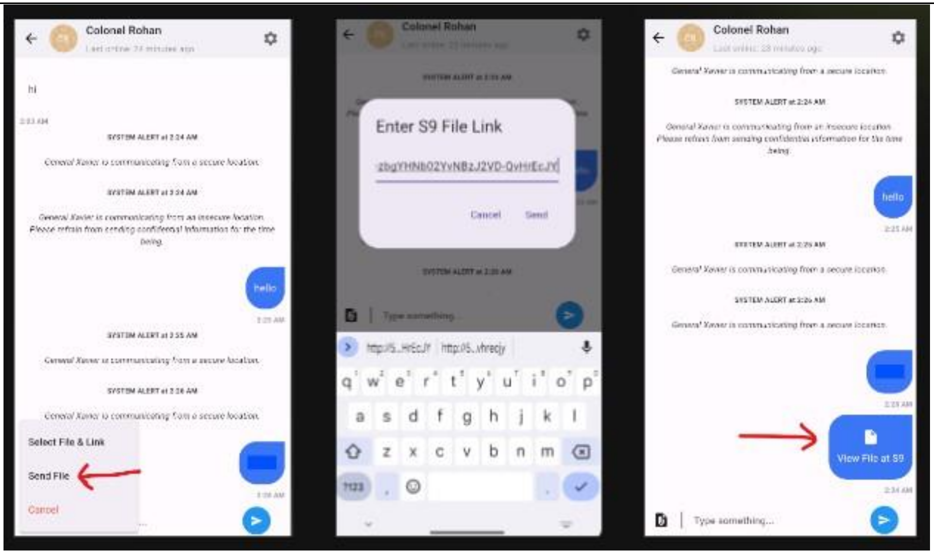
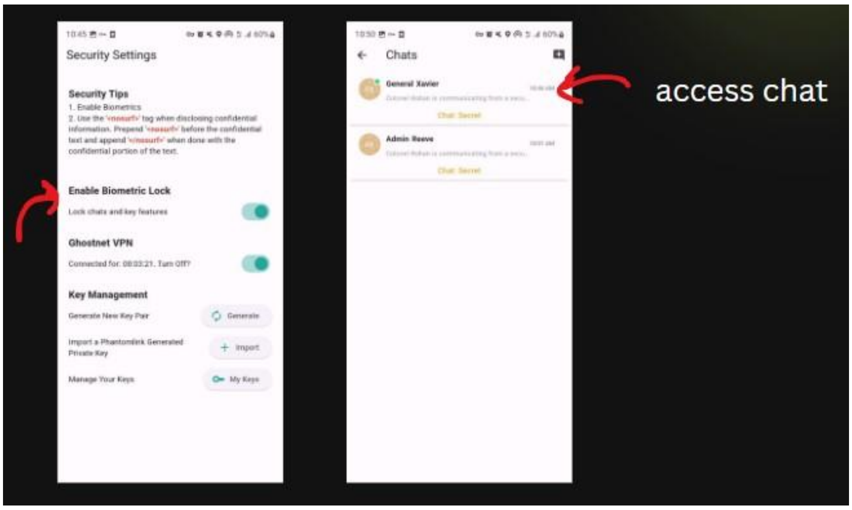
Feature/Function	**Security Implementation**
Real-Time Instant Messaging	*See End-to-End Encryption*
End-to-End Encryption	**ECDH Algorithm & P-256 Elliptic Curve** - *P-256 is well-supported and offers the right balance of security and performance.* - You can only access the message by decrypting it using a known public key and a corresponding private key. - Each user in the application has their own public-private key pair. Public keys are distributed publicly and encrypt the sender's messages. The receiver can only decrypt the sender's message with the matching private key. - Example:  Bob $#cs4$vxxv!~ Alice Hello Hello Bob's private key Alice's public key Database $#cs4$vxxv!~ Alice's private key Bob's public key Encryption Decryption Hello Send Hello $#cs4$vxxv!~ **Key Management (Generate/Select/Delete Keys)** - Users can *Generate* keys. One reason to generate new keys is when changing devices and you lost the old key (because you did not export it to S9). Another reason is to implement a user-controlled form of 'key rotation'. Through this, the amount of content encrypted with one key will be less so that the amount of content leaked by a single key compromise is also less.  Security Settings Security Tips 1. Enable Biometrics 2. Use the '<nosurf>' tag when disclosing confidential information. Prepend '<nosurf>' before the confidential text and append '</nosurf>' when done with the confidential portion of the text. Enable Biometric Lock Lock chats and key features Ghostnet VPN Connected for: 00:10:20. Turn Off? Key Management Generate New Key Pair Generate Import a Phantomlink Generated Private Key Import Manage Your Keys My Keys Success New Key Generated OK NEW 0089d48bb... 6471048f5...

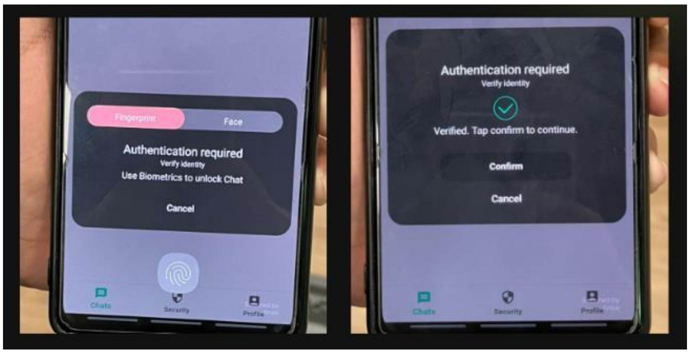
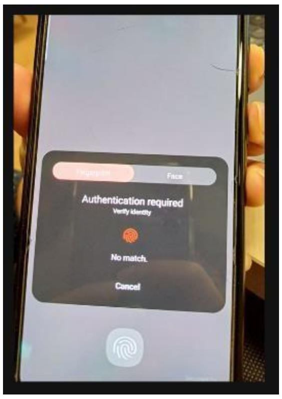
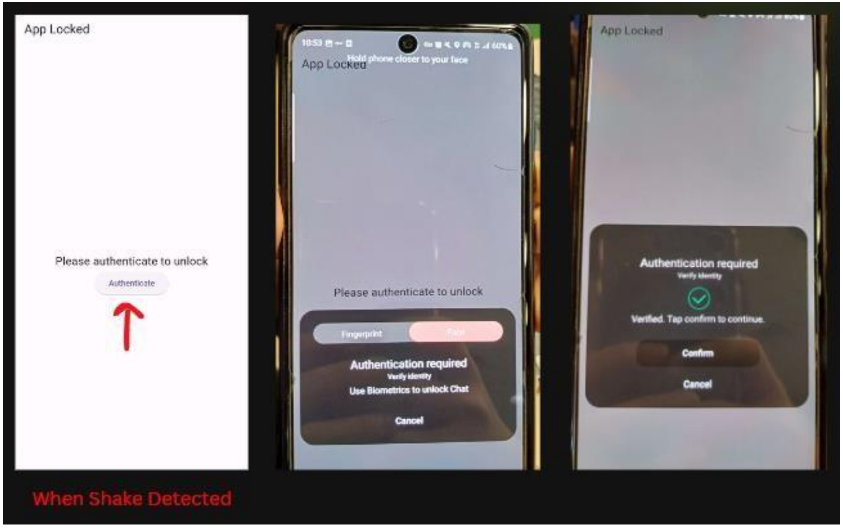
	- Users can *select* keys, important if they have different keys. This also forms part of the 'user-controlled key rotation'. Messages will be encrypted with the selected key. By frequently using different keys, fewer messages will be exposed if a single key is compromised. This mitigates a single point of failure in encryption keys.  Security Settings Security Tips 1. Enable Biometrics 2. Use the '<nosurf>' tag when disclosing confidential information. Prepend '<nosurf>' before the confidential text and append '</nosurf>' when done with the confidential portion of the text. Enable Biometric Lock Lock chats and key features Ghostnet VPN Connected for: 00:15:27. Turn Off? Key Management Generate New Key Pair Import a Phantomlink Generated Private Key Manage Your Keys 0089d48bb... 647104815... Key Selected Successfully Generate Import My Keys Close Chats Security Profile - Users can *delete* keys if they want to render that key obsolete. One reason to use this is when you lose your device, and you want to render keys stored by PhantomLink in your lost phone in Androids Secure Key storage obsolete. Messages that were used this key would be lost (unable to decrypt).  Confirm Delete Are you sure you want to delete this key? All messages sent with this key will be unreadable deleted
Built-In VPN	To use the PhantomLink App, you must first be connected to the Ghostnet VPN, otherwise PhantomLink will not let you in. This feature is to ensure that traffic is encrypted and secure even if a user is connected to insecure networks and therefore vulnerable to many types of network attacks. This is particularly critical for applications on mobile devices like phones as they will not always be in a secure location and will not always be used in a secure location.

	 10:42 Connect to Ghostnet You are required to connect to Ghostnet to access PhantomLink Disconnected 00:00:00 10:42 Tue, 13 Feb Update postponed. PhantomLink 10:11 Ghostnet ↓42.5 kbit/s 129.2 kB · ↑34.9 kbit/s 89.4 kB USB tethering turned on Cable charging (3 h 15 m until full) 10:45 Security Settings Security Tips 1. Enable Biometrics 2. Use the '<nosurf>' tag when disclosing confidential information. Prepend '<nosurf>' before the confidential text and append '</nosurf>' when done with the confidential portion of the text. Enable Biometric Lock Lock chats and key features Ghostnet VPN Connected for: 00:03:21. Turn Off? Key Management Generate New Key Pair Import a Phantomlink Generated Private Key Manage Your Keys Implementation-wise, the Ghostnet VPN uses the OpenVPN Protocol. The Ghostnet VPN server is an OpenVPN Server hosted on AWS.

GeoFence	Geofence is a useful feature for applications on mobile devices. Since PhantomLink will be used as a form of mobile communication, even if a user is in an insecure location, communication should still be allowed. However, it is restricted to reduce the sensitive information that is displayed. This is critical as what if a user is on public transport and communicating with a colleague? Someone could be shoulder-surfing them. Therefore, when a user is in an insecure location, defined as outside of the office, the chat history is locked, and the receiving party is alerted that the user he is communicating with is in an insecure location and therefore sensitive information should not be shared for the time being. Once the user is back in a secure location another alert is sent to notify the receiving party. Multiple locations can be defined if needed to compensate for those working from home.  Colonel Rohan Last online: 13 minutes ago Chat history is locked, please move to a defined secure location. TODAY SYSTEM ALERT at 2:24 AM General Xavier is communicating from an insecure location. Please refrain from sending confidential information for the time being. hello 2:24 AM Colonel Rohan Last online: 14 minutes ago test123 1:58 AM SYSTEM ALERT at 2:02 AM Colonel Rohan is communicating from a secure location. hi 2:03 AM SYSTEM ALERT at 2:24 AM General Xavier is communicating from a secure location. SYSTEM ALERT at 2:24 AM General Xavier is communicating from an insecure location. Please refrain from sending confidential information for the time being. hello 2:25 AM SYSTEM ALERT at 2:25 AM General Xavier is communicating from a secure location.

NoSurf Tags	NoSurf tags operate much like what is conventionally known as “spoiler” tags. The reason for implementing this is to provide an additional layer of security for sensitive information in chat history and reduce the effects of shoulder surfing. By ‘redacting’ sensitive information by default, sensitive information will not be shown unless the user clicks to reveal it. He can then click it again to hide it. This reduces the amount of sensitive information displayed by default for attackers to see when shoulder surfing.  2:28 AM drop the nukes at location delta 2:28 AM
File Management through S9	PhantomLink does not deal with files directly as it may not be the most secure way. Instead, files are managed securely by ShadowNine (S9), which was built for the purpose of secure file management. Files can be uploaded in S9. To share them, a user can generate a sharing link to send to the receiver. The following pictures describe the process:  Colonel Rohan hi SYSTEM ALERT at 2:24 AM General Xavier is communicating from a secure location. SYSTEM ALERT at 2:24 AM General Xavier is communicating from an insecure location. Please refrain from sending confidential information for the time being. hello SYSTEM ALERT at 2:25 AM General Xavier is communicating from a secure location. SYSTEM ALERT at 2:26 AM General Xavier is communicating from a secure location. Select File & Link Send File Cancel nukes invoice | nuclearSecret | File Is Checked | Create Link The url to visit the link is http://54.169.225.178:3000/viewfile?token=zbgYHNb02YvNBzJ2VD-QvHrEcJY

	 Colonel Rohan hi SYSTEM ALERT at 2:24 AM General Xavier is communicating from a secure location. SYSTEM ALERT at 2:24 AM General Xavier is communicating from an insecure location. Please refrain from sending confidential information for the time being. hello SYSTEM ALERT at 2:25 AM General Xavier is communicating from a secure location. SYSTEM ALERT at 2:26 AM General Xavier is communicating from a secure location. Select File & Link Send File Cancel Enter S9 File Link zbgYHNb02YvNBzJ2VD-QvHrEcJY Cancel Send View File at S9 Type something... When the file is clicked, the user will have to get through authentication checks (login and/or OTP) before their access rights are evaluated and file access is granted/rejected. *(This part is implemented by Shi Jie)*
Biometrics Authentication	If biometrics has been set up on the device, biometrics lock can also be enabled within the app to lock key features including locking chats (when they are accessed) and key deletion.  Security Settings Security Tips 1. Enable Biometrics 2. Use the '<mssurf>' tag when disclosing confidential information. Prepend '<mssurf>' before the confidential text and append '</mssurf>' when done with the confidential portion of the text. Enable Biometric Lock Lock chats and key features Ghostnet VPN Connected for: 08:03:21. Turn Off? Key Management Generate New Key Pair — Generate Import a Phantomlink Generated Private Key — Import Manage Your Keys — My Keys Chats General Xavier Chat: Secret Admin Reeve Chat: Secret access chat This aims to provide an additional layer of security and authentication. It can also protect when attackers get hold of someone's device or if a user leaves their device unlocked.

	Biometrics Success  Fingerprint Face Authentication required Verify identity Use Biometrics to unlock Chat Cancel Chats Security Profile Authentication required Verify identity Verified. Tap confirm to continue. Confirm Cancel Chats Security Profile **Biometrics Fail**  Fingerprint Face Authentication required Verify identity No match. Cancel
Theft Lock	There are cases where phones have been stolen right from their hands as someone is using them (and hence unlocked). To try to reduce the impact if such an event occurs, PhantomLink can detect phone shakes, by calculating G-Force supplied from the device accelerometer, and when detected lock the app. To unlock, biometrics authentication is required.  App Locked Please authenticate to unlock Authenticate When Shake Detected 10:53 App Locked Hold phone closer to your face Please authenticate to unlock Fingerprint Face Authentication required Verify identity Use Biometrics to unlock Chat Cancel App Locked Authentication required Verify identity Verified. Tap confirm to continue. Confirm Cancel The idea here is that when a phone is taken from someone, there will be a noticeable shake. The shake does not trigger if a device is rotated, or a user moves around normally.

3. Other Individual Contributions and Reflection

For this project, I was the Team Leader. As the Team Leader, I was responsible for ensuring that everyone was on the right track, doing work and that our project was integrated.

I created the GitHub Repository and Auth0 account to get the team started and assigned roles and tasks to my members.

Though I was not in charge of the implementation of Auth0 in PhantomLink, I helped Xavier with it as he was not very familiar with Flutter, Dart and how the app worked yet.

For this project, I took on a very big challenge. I decided to create a mobile app, something that I had never done before nor learned anything about. I had to do extensive research on how I could bring this idea to life before finally landing on the use of Flutter.

This was not the end of my challenges however, I had to self-learn how Flutter works, how to use it, the Dart programming language, and the basics of native Android. These are all concepts I have had no previous experience in, and I had to learn them from scratch while still striking a balance between all my other schoolwork and ensuring that I still had time to implement features.

I laid the groundwork for the PhantomLink app, building all the necessary foundational features, mostly independently, such as Instant Messaging so that the security features could eventually be implemented.

Since I knew I was one of the few people working on a mobile app, I tried my best to think of unique security features that are useful for mobile devices. Hence my focus for this project was mainly on built-in Mobile Device Management (MDM) features such as Geofence and VPN. I also thought of how I could use the device accelerometer to my advantage, a capability that not many had and that was how I came up with the Theft Lock.

I had to step out of my comfort zone for this project and at times I thought maybe I should have stuck to what I was familiar with so I could deliver more technical security features, but upon looking back at what I have accomplished, I am proud that I took this opportunity to explore and learn more about this new area and that I was able to still accomplish the goals that I wanted to achieve.

Overall, it was a great learning experience for me. I appreciate my team for their effort and help and Mr Vincent Phua for his advice. I have enjoyed this experience and I think the wide project scope allowed for a lot of exploration and useful learning experiences.

~ End ~