UTM UNIVERSITI TEKNOLOGI MALAYSIA

FACULTY OF COMPUTING
UTM Johor Bahru

SECP 1513: Technology Information System

Semester 01, 2024/2025

PROJECT PROPOSAL

“*InfinitePROTECH*” Application

Team Name:

InfiniteTECH

Team Members:

1. Chua Kai Loon	*(A24CS5071)*
2. Khairunnisa Binti Mohd Hazani	*(A24CS0095)*
3. Muhammad Adam Ashraff Bin Zamri	*(A24CS0119)*
4. Muhammad Hafiz Bin Reepei	*(A24CS0133)*
5. Tyler Chok Ke Qing	*(A24CS5068)*

Client Name:

1. Family
2. Friends

Table of Contents

1. Introduction

InfiniteTECH's proposal of the InfinitePROTECH system aims to address the worsening cybersecurity issue plaguing Malaysian Internet users. First, MyCERT, Malaysia's Cybersecurity Response Team, reported an increase in cyber incidents in Q3 2024, compared to Q2 2024 *[1]*. Particularly, in the report, there was an increase in the number of incidents of fraud and spam among other cybercrimes. This report sheds light on the urgent need to put in place preventative measures to prevent more Malaysians from being frauded as well as educating upon how to identify spam mail which may contain malicious links. Furthermore, Malaysia's Education Ministry has also admitted, based on a report by the MalayMail *[2]*, that in parts of Malaysia, there is a lack of education on digital skills, hence an even weaker knowledge base for ensuring the safety on the Internet. Thus, this highlights a need for an alternative way to educate the young children on how to ensure proper security on the Internet. Finally, the MalayMail also reported that the elderly in Malaysia have fallen victim to online scams and lost RM 255 million *[3]*. This is increasingly worrying as the funds lost may have meant retirement savings to the elderly who often lack the knowledge to recognise manipulative fraudsters. Therefore, it is important to implement educational initiatives as well as a protective measure to aid the elderly in recognising threats and consulting with their guardians before taking action.

Our solution, InfinitePROTECH a cross-platform application aiming to mitigate and reduce the aforementioned issues as well as beyond it. We would be focusing on three main aspects, "Detection", "Education" and "Assurance", with each incorporating various advanced technologies to aid our system. The first aspect, "Detection" would hold our "Fraud Detection Alert", "Fraud Detection History" as well as "Report a Fraud" features.

The "Fraud Detection Alert" would tap into existing databases of known fraudsters, scammers and bad actors to alert the user of any suspicious texts, phone calls or emails. This feature works through collaboration with the government and related agencies to access the databases of phone numbers, email addresses, and other means of communication with a history of fraud. With privacy being a crucial aspect, our detection system requires explicit user consent to function at all. The system will first obtain consent from the user on what application or medium it can screen for potential fraud. Then once permission is obtained, the system would scan the information of the sender of the text, call or email received by the user in real-time. All processed information would not be stored in servers, nor would the system scan the contents of the message in its entirety. The sender's information will then be cross-checked with governmental databases as well as our own databases. If the number is detected to have a history of fraud, our app would send a critical alert to the user with an accompanying "Block Sender" option to block the sender or "Ignore" and "Report False Positive" if the detected text, number or email was indeed authentic to improve our services.

Proceeding to the next feature, the "Fraud Detection History" showcases a history of the application's detected fraud and history of reported users. Finally, the "Report a Fraud" feature would allow users to report new fraudsters that they encounter and help others to avoid the same mistake. The system will automatically flag the reported number and if sufficient flags have been reported, it will go through manual verification by our team and if verified, the details entered into our database to prevent abuse.

The second layer of security implemented would be the checking of contents within the message. To ensure user privacy, this is all done on-device through Artificial Intelligence (AI) and Machine Learning (ML), it would scan the messages for any links and check the link for potential phishing-related scams. In the interest of privacy, the scan would be only for links and message contents would not be checked. Then, it would cross-check the link sent with a list of authentic links such as official banking websites, courier websites and other websites. If it is flagged as potentially phishing, it would behave similarly with the detected-fraud protocol, initiating a warning and allowing the user options on how to proceed.

For the next aspect, "Education", we aim to help educate the general public and raise awareness on how to ensure your own, your family and your friends' safety on the Internet. It would feature an "Education Module" with quizzes to educate and test your knowledge of cybersecurity on the Internet. For the younger generation, gamified concepts of cybersecurity such as creating strong passwords, identifying fraudulent links *(phishing)*, carefully allowing permissions access and more will be available. There will also feature educational articles detailing how to protect yourself as well as summarised news articles, powered by AI, detailing how new scam methods operate concisely. Finally, there will be a simulator which simulates different scenarios such as a malware attack on your device and guides on how to address the issue, if it ever occurs.

For “Assurance”, we will strive to ensure that our features would continue to function in its most basic form and carry out the essential task of protection, even when an internet connection is not available. Through processing on-device and trying our best to make sure all features are done locally without an Internet connection; we would ensure seamless transition between a connected device and a device without connection. Furthermore, a “Lockdown Mode” feature would be implemented to safeguard a device should it be detected to be compromised by malware. This would first require approval from the user’s Authorised Persons such as a guardian or parent. Then, once given permission, the device would disconnect from the Internet and any external source of entry and be essentially ‘locked down’. This is to prevent further theft of personal data and should only be used in extreme scenarios. “Lockdown Mode” can only be activated if there is at least one Authorised Persons and can only be deactivated by an Authorised Persons. Finally, we will also offer an AI-powered helpdesk and chatbot for users who may encounter any trouble or issues with our application.

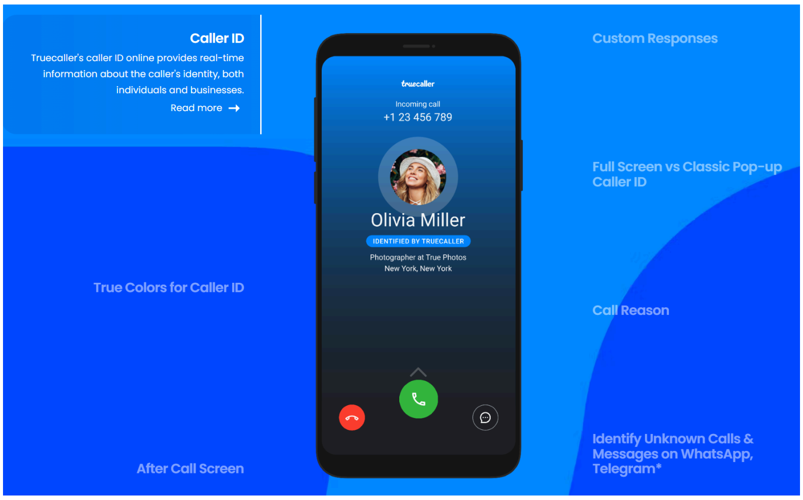
All the above aspects, and more combine into our application, InfinitePROTECH. Thus, users would be able to gain benefits through using our application. For example, with the “Detection”, scams can be completely avoided as they do not even reach the user. This could allow those who are unaware of the latest fraud methods to approach a call, message or email with more caution as our application has flagged it. In addition, users, primarily the youth and elderly can learn more about safeguarding their data and privacy on the Internet with our “Education” section. Younger children can take advantage of the mini-games created within this section to generate interest in protecting themselves on the internet and guardians can be assured that they have access to the best resource in ensuring that their family is protected from malicious bad actors. Finally, “Assurance” allows peace of mind for guardians, even when they are away from the elderly to ensure that their basic protection from fraudsters is met. Our offline-friendly approach also brings benefits of a seamless user experience across the board. Additionally, it eliminates possible “downtimes”, reducing the opportunities for malicious actors to target and defraud additional victims when they are disconnected from the Internet. Finally, “Lockdown Mode”, an extreme measure, allows compromised users to have an alternative route to safeguard their remaining data.

As for our competition, we have identified a few standout competitors which may pose a threat to our application’s appeal to users. They are: *“Caller ID” [4]*, *“Truecaller” [5]* and *“Getcontact” [6]*. All of these applications behave similarly with our application, such as screening calls and obtaining caller ID for the user to identify the caller. However, some of these applications lack features that we provide, such as the “Education” section, empowering users to learn how to better protect oneself on the Internet. Another limitation would be their detection coverage. Our application is able to detect information, provided with explicit user consent to detect calls, texts and emails whereas our competitors often only are able to detect calls via caller ID.

2. Existing Systems

Our application, InfinitePROTECH will have the ability to replace existing applications as it will be packed with a wide range of features which are not only improvements upon that of our competitors but also offer unmatched capabilities. Such features include, Fraud Detection Alerts, Fraud Reporting, Education Module, proper offline functionality and many more. Our app also will have optional paid options with lower pricing compared to our competitors. Furthermore, many features will not be locked behind a paywall as we will offer limited free tiers for some features which renew monthly for users to enjoy.

Our team identified a few existing systems, currently available in the market for users, namely, *“Caller ID” [4]*, *“Truecaller” [5]* and *“Getcontact” [6]*. All three of these applications enable users to identify unfamiliar callers by displaying names or tags from community databases or user contributions as well as other unique features.



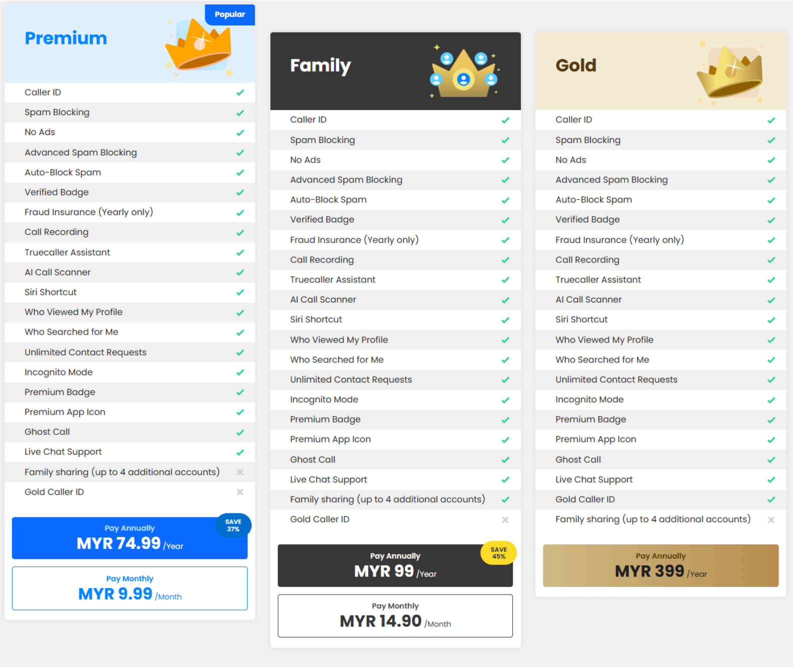
Caller ID

Truecaller's caller ID online provides real-time information about the caller's identity, both individuals and businesses.

Read more →
truecaller
Incoming call
+1 23 456 789
Olivia Miller
IDENTIFIED BY TRUECALLER
Photographer at True Photos
New York, New York
True Colors for Caller ID
After Call Screen
Custom Responses
Full Screen vs Classic Pop-up Caller ID
Call Reason
Identify Unknown Calls & Messages on WhatsApp, Telegram*

Figure 1: Truecaller Caller ID System [7]

The *Truecaller* application provides users with a dependable caller ID system that works offline for saved contacts and enables basic spam screening even without internet connection. However, additional features including real-time caller identification, full call history insights, and an ad-free experience are only available with a paid subscription.



Popular

Premium

Caller ID	✓
Spam Blocking	✓
No Ads	✓
Advanced Spam Blocking	✓
Auto-Block Spam	✓
Verified Badge	✓
Fraud Insurance (Yearly only)	✓
Call Recording	✓
Truecaller Assistant	✓
AI Call Scanner	✓
Siri Shortcut	✓
Who Viewed My Profile	✓
Who Searched for Me	✓
Unlimited Contact Requests	✓
Incognito Mode	✓
Premium Badge	✓
Premium App Icon	✓
Ghost Call	✓
Live Chat Support	✓
Family sharing (up to 4 additional accounts)	✕
Gold Caller ID	✕

SAVE 37%

Pay Annually
MYR 74.99 /Year

Pay Monthly
MYR 9.99 /Month

Family

Caller ID	✓
Spam Blocking	✓
No Ads	✓
Advanced Spam Blocking	✓
Auto-Block Spam	✓
Verified Badge	✓
Fraud Insurance (Yearly only)	✓
Call Recording	✓
Truecaller Assistant	✓
AI Call Scanner	✓
Siri Shortcut	✓
Who Viewed My Profile	✓
Who Searched for Me	✓
Unlimited Contact Requests	✓
Incognito Mode	✓
Premium Badge	✓
Premium App Icon	✓
Ghost Call	✓
Live Chat Support	✓
Family sharing (up to 4 additional accounts)	✓
Gold Caller ID	✕

SAVE 45%

Pay Annually
MYR 99 /Year

Pay Monthly
MYR 14.90 /Month

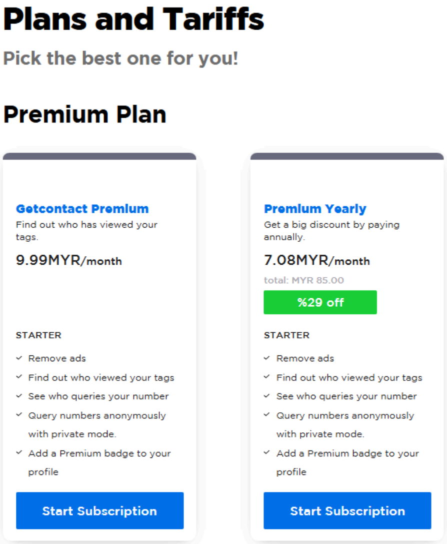
Gold

Caller ID	✓
Spam Blocking	✓
No Ads	✓
Advanced Spam Blocking	✓
Auto-Block Spam	✓
Verified Badge	✓
Fraud Insurance (Yearly only)	✓
Call Recording	✓
Truecaller Assistant	✓
AI Call Scanner	✓
Siri Shortcut	✓
Who Viewed My Profile	✓
Who Searched for Me	✓
Unlimited Contact Requests	✓
Incognito Mode	✓
Premium Badge	✓
Premium App Icon	✓
Ghost Call	✓
Live Chat Support	✓
Gold Caller ID	✓
Family sharing (up to 4 additional accounts)	✕

Pay Annually
MYR 399 /Year

Figure [2]: Truecaller Premium Pricing [8]

Similarly, *Getcontact* allows users to search for unfamiliar numbers and view tags such as “Scam” and “Telemarketer”, but its complete caller ID features are only available to premium customers. Additionally, concerns on the safety of users’ data privacy on the app persist as the app collects substantial information relating to the user.



Plans and Tariffs

Pick the best one for you!

Premium Plan

Getcontact Premium
Find out who has viewed your tags.
9.99MYR/month

STARTER
- ✓ Remove ads
- ✓ Find out who viewed your tags
- ✓ See who queries your number
- ✓ Query numbers anonymously with private mode.
- ✓ Add a Premium badge to your profile

Start Subscription

Premium Yearly
Get a big discount by paying annually.
7.08MYR/month
total: MYR 85.00
%29 off

STARTER
- ✓ Remove ads
- ✓ Find out who viewed your tags
- ✓ See who queries your number
- ✓ Query numbers anonymously with private mode.
- ✓ Add a Premium badge to your profile

Start Subscription

Figure 3: Getcontact Premium Pricing [9]

Additionally, in general, basic spam and fraud prevention features on Android and iOS smartphones are sometimes limited to banning certain phone numbers or using preloaded and often outdated spam lists. While these systems provide basic caller ID functionality, they lack the sophisticated AI-driven identification and dynamic database updates available in third-party programs. On top of that, they do not train users to recognise fraud so that they are not so reliant on fraud detection as false positives could occur or give tools for proactive fraud reporting to expand the list of blacklisted senders.

Although the three systems mentioned provide caller identification, their primary focus is on detection and blocking, failing to address the importance of education. This leads to semi-protected but still clueless users in regard to cybersecurity. Hence our application provides features to educate the users on how to recognize fraud through the Education Module. We also use AI helpers and live assistants to help the user if they face any problem while using our application.

Furthermore, many of these applications have constant advertisements in their free versions, which can detract from the user experience, and advanced capabilities frequently require paid memberships. Additionally, concerns regarding user privacy protection have been raised, especially in apps like *Getcontact*, whose data collection practices and sharing procedures have raised eyebrows. Our application is ad-free and safe to use since we aim to collaborate with the government to make sure our application is well known and trusted. Additionally, we would introduce a paid membership which only enhances the free-tier at a low and budget-friendly cost.

Features	Caller ID *[4]*	Truecaller *[5]*	Getcontact *[6]*
Call Blocking	Limited	Yes **Premium only*	Yes
Offline Functionality	Limited	Limited	Limited
Spam Blocking	Basic	Yes	Advanced
Advertisements	None	With Free Version	With Free Version
Memberships	None	Yes **High Pricing*	Yes **High Pricing*
Education Module	None	None	None
Contact Search	Yes **Saved Contacts only*	Limited	Limited
iOS Availability	Unavailable	Available	Available
Android Availability	Available	Available	Available

Table 1: Comparison of Existing Systems

The limitations of other applications highlight the need for a more comprehensive solution which encompasses improved fraud detection, user education, AI-driven system and privacy-conscious factors while staying available to consumers without sky-high pricings of premium memberships. Furthermore, a primary focus on the user experience and accessibility would enhance the application and provide for a more user-friendly approach, allowing those of all ages and demographics to utilise the application to its full potential.

3. Proposed System

InfinitePROTECH will implement various high-end systems to optimise the user experience and boost the interaction as well as functionality in our application. For our fraud detection feature, we tap into Amazon Neptune's *[10]* abilities as a graph database. It is capable of storing and querying relationships in near real-time with milliseconds latency to easily detect fraud patterns. Neptune allows for fast graph queries for our application to easily detect fraud scenarios such as credit card fraud and other fraudulent patterns.

Another one of the systems that we implement is Amazon DynamoDB *[11]*. This system is the best solution for minimizing and handling big data workloads with high-speed, low-latency performance. It is also a fully managed NoSQL database capable of scaling horizontally to support billions of records and millions of requests per second. Thus, it is ideal for storing our application's fraud detection alerts, user reports, and interaction logs. In the security aspect, the Amazon DynamoDB provides strong security measures to ensure the safety for the user. Some features are end-to-end encryption (at rest and in transit), role-based access control with AWS IAM integration, and monitoring and logging suspicious activities through AWS CloudTrail. This allows peace of mind on our administrative end as well as for the end-user. Other than that, we chose Amazon DynamoDB because the cost of the system is very adjustable, such that it uses pay-per-request pricing to ensure you only pay for what you use, and on-demand or provisioned capacity modes can optimize costs based on traffic. Hence, we are able to scale according to demand, without wasting on capital.

The second system we implement is AWS Storage Gateway *[12]*. It is a hybrid cloud storage service that gives our application on-premises access to virtually unlimited cloud storage. AWS Storage Gateway can simplify our application's storage management and reduce costs for key hybrid cloud storage use cases as well as ensure smoothness in interactions of the application. Features of AWS Storage Gateway include moving backups to the cloud, using on-premises files backed by cloud storage, and providing low-latency access to data in AWS for on-premises applications. Thus, our application can have low-latency access to data that is stored safely and durably in AWS. The gateways use a read-through and write-back cache, committing data locally, acknowledging the write operations, and then asynchronously copying data to AWS, reducing application latency.

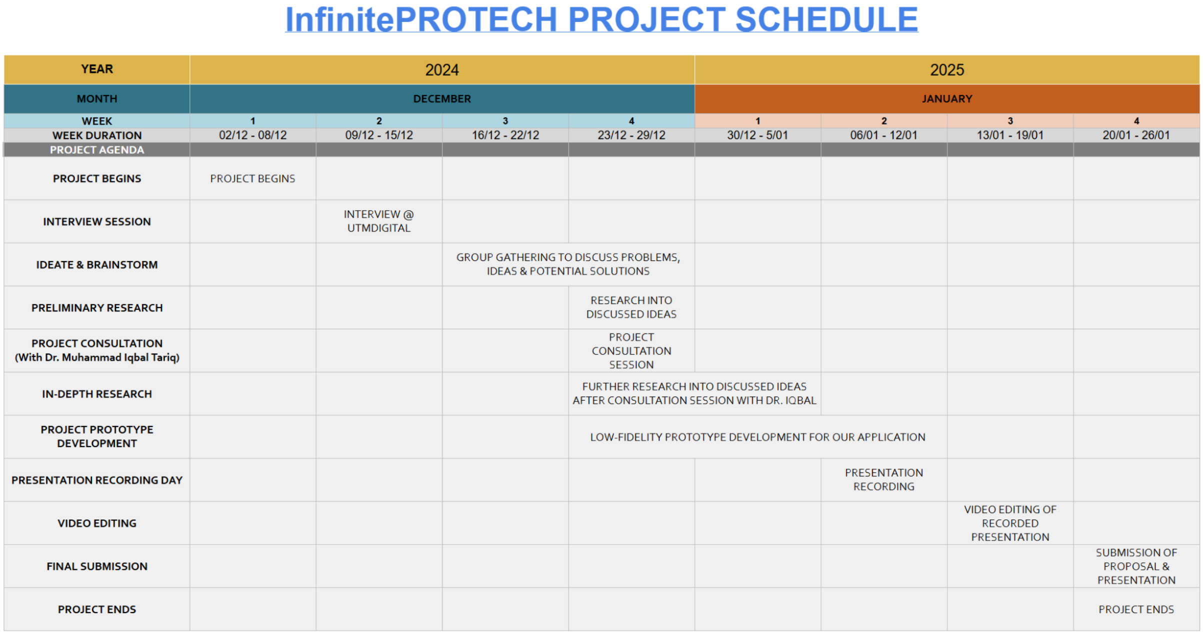
Additionally, Amazon Cognito *[13]* lets us add user sign-up, sign-in, access control, and broker AWS service access to InfinitePROTECH within minutes. It is beneficial for us to use it as it is a developer-centric, cost-effective service that provides secure, tenant-based identity stores and federation options that can scale to millions of users if required for our application. Amazon Cognito helps us create branded customer experiences, improve security, and adapt to our customers' needs. For example, it supports login with social identity providers and password-less login using WebAuthn *[14]* passkeys or SMS and email one-time-passwords. This enables us to ensure a good user experience in the login, sign-up aspects and ensuring the continued safety of our users' information and data.

In addition, Lockdown Mode will be introduced to users to protect an already-compromised device from further data theft. For detecting and predicting fraud in communication data, we implement TensorFlow *[15]* because it provides the ability to create artificial intelligence with that function. If a scam attempt is detected, the app will be locked down and disconnecting the device from the Internet by a pre-registered Authorised Person who can approve a lockdown. For the authorization, we integrate the system with secure Application Programming Interfaces (API) *[16]* because it has robust security controls. The system also implements a backup system, protected with Advanced Encryption Standard (AES) *[17]*. This is a safeguard of essential data before the lockdown is enforced.

With InfinitePROTECH, our users would first be greeted with a login or sign-up page. The user is prompted to enter their login credentials or access the application through password-less login methods such as passkeys, SMS, or email one-time-passwords. If they do not have an account, they will be given an option to sign up to our application. Once users get past the login page, they are greeted with our Dashboard, showcasing a general overview of what has happened in the past week. Icons to navigate to the "Detection", "Education" and "Others" sections would be at the bottom of the device. In the "Detection" section, users would be able to check on their entire history of fraud detection and if they were met with a critical alert, they would be prompted to this section. This page allows users to block the phone number, email or any other relevant communications medium of the sender that has been flagged as fraudulent. Other than that, the users are given an option to report fraud, if they encounter it and is not flagged by the system.

Next, in the “Education” section, a scrollable bar of articles would be placed at the top to notify users of fraud-related articles relating to prevention, or new methods of fraud that have been discovered. Below that would be our mini games section aimed at youths, featuring games about password cracking and an in-game currency to purchase premium membership just by playing and successfully winning the games. Finally, the “Others” section would contain the user’s account information, settings, permissions access list, a method to log out, and other miscellaneous information.

4. Project Schedule



InfinitePROTECH PROJECT SCHEDULE

YEAR	2024				2025			
MONTH	DECEMBER				JANUARY			
WEEK	1	2	3	4	1	2	3	4
WEEK DURATION	02/12 - 08/12	09/12 - 15/12	16/12 - 22/12	23/12 - 29/12	30/12 - 5/01	06/01 - 12/01	13/01 - 19/01	20/01 - 26/01
PROJECT AGENDA								
PROJECT BEGINS	PROJECT BEGINS							
INTERVIEW SESSION		INTERVIEW @ UTMDIGITAL						
IDEATE & BRAINSTORM			GROUP GATHERING TO DISCUSS PROBLEMS, IDEAS & POTENTIAL SOLUTIONS					
PRELIMINARY RESEARCH				RESEARCH INTO DISCUSSED IDEAS				
PROJECT CONSULTATION (With Dr. Muhammad Iqbal Tariq)				PROJECT CONSULTATION SESSION				
IN-DEPTH RESEARCH				FURTHER RESEARCH INTO DISCUSSED IDEAS AFTER CONSULTATION SESSION WITH DR. IQBAL				
PROJECT PROTOTYPE DEVELOPMENT				LOW-FIDELITY PROTOTYPE DEVELOPMENT FOR OUR APPLICATION				
PRESENTATION RECORDING DAY						PRESENTATION RECORDING		
VIDEO EDITING							VIDEO EDITING OF RECORDED PRESENTATION	
FINAL SUBMISSION								SUBMISSION OF PROPOSAL & PRESENTATION
PROJECT ENDS								PROJECT ENDS

Figure 4: InfiniteTECH's Project Schedule for the InfinitePROTECH Project

5. References

[1] **MyCERT.** (2024, December 26). *SR-028.122024: MyCERT Report - Cyber Incident Quarterly Summary Report - Q3 2024.* MyCERT. https://mycert.org.my/portal/advisory?id=SR-028.122024

[2] **MalayMail.** (2024, April 30). *Education Ministry admits gap in digital skills between rural, urban schools.* MalayMail. *https://www.malaymail.com/news/malaysia/2024/04/30/education-ministry-admits-gap-in-digital-skills-between-rural-urban-schools/131622*

[3] **MalayMail.** (2024, September 28). *Bukit Aman: Elderly online scam victims lose RM255m as fraud cases surge in 2024.* MalayMail. https://www.malaymail.com/news/malaysia/2024/09/28/bukit-aman-elderly-online-scam-victims-lose-rm255m-as-fraud-cases-surge-in-2024/151915

[4] Caller ID (2024). Retrieved from https://www.ayamote.com/

[5] Truecaller (2024). Retrieved from https://www.truecaller.com/

[6] Getcontact (2024). Retrieved from https://getcontact.com/en/

[7] Truecaller Caller ID (2024). Retrieved from https://www.truecaller.com/caller-id

[8] Truecaller Premium (2024). Retrieved from https://www.truecaller.com/premium

[9] Getcontact Premium (2024). Retrieved from https://premium.getcontact.com/en/

[10] AWS Amazon Neptune (n.d.) *High-performance graph analytics and serverless database for superior scalability and availability*.

https://aws.amazon.com/neptune/fraud-graphs-on-aws/

[11] AWS Amazon DynamoDB (n.d.) *Serverless, NoSQL, fully managed database with single-digit millisecond performance at any scale.*

https://aws.amazon.com/pm/dynamodb/

[12] AWS Storage Gateway (n.d.) *Provide on-premises applications with access to virtually unlimited cloud storage.*

https://aws.amazon.com/storagegateway/

[13] AWS Amazon Cognito (n.d.) *Implement a secure, scalable, and customized sign-up and sign-in experience in minutes.*

https://aws.amazon.com/cognito/

[14] WebAuthn Guide (n.d.) *A better alternative for securing our sensitive information online.* https://webauthn.guide/

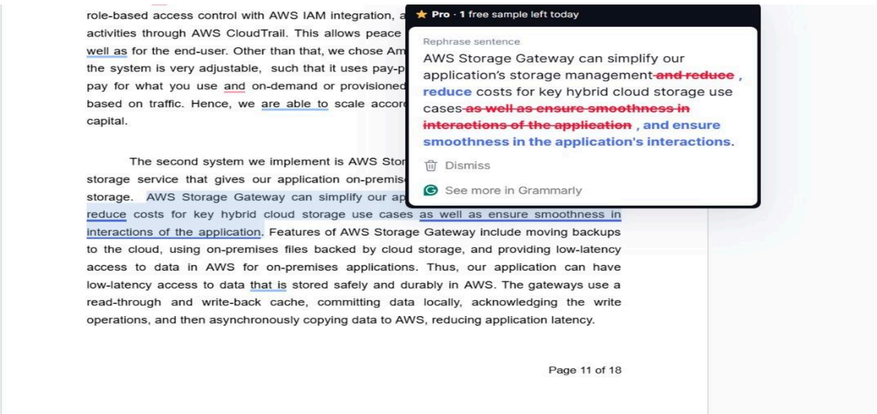
[15] LinkedIn (2023). *Fraud detection with Python and TensorFlow training course.* https://www.linkedin.com/pulse/fraud-detection-python-tensorflow-training/

[16] F5 (n.d.) *What is API security? Main types and use cases.* https://www.f5.com/glossary/api-security

[17] TechTarget (2024). *Advanced Encryption Standard (AES).* https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

Appendices

1. Grammarly *(For grammar-checking purposes)*



role-based access control with AWS IAM integration, a
activities through AWS CloudTrail. This allows peace
well as for the end-user. Other than that, we chose Am
the system is very adjustable, such that it uses pay-p
pay for what you use and on-demand or provisioned
based on traffic. Hence, we are able to scale accor
capital.

The second system we implement is AWS Stor
storage service that gives our application on-premis
storage. AWS Storage Gateway can simplify our ap
reduce costs for key hybrid cloud storage use cases as well as ensure smoothness in interactions of the application. Features of AWS Storage Gateway include moving backups to the cloud, using on-premises files backed by cloud storage, and providing low-latency access to data in AWS for on-premises applications. Thus, our application can have low-latency access to data that is stored safely and durably in AWS. The gateways use a read-through and write-back cache, committing data locally, acknowledging the write operations, and then asynchronously copying data to AWS, reducing application latency.

Page 11 of 18

★ Pro · 1 free sample left today

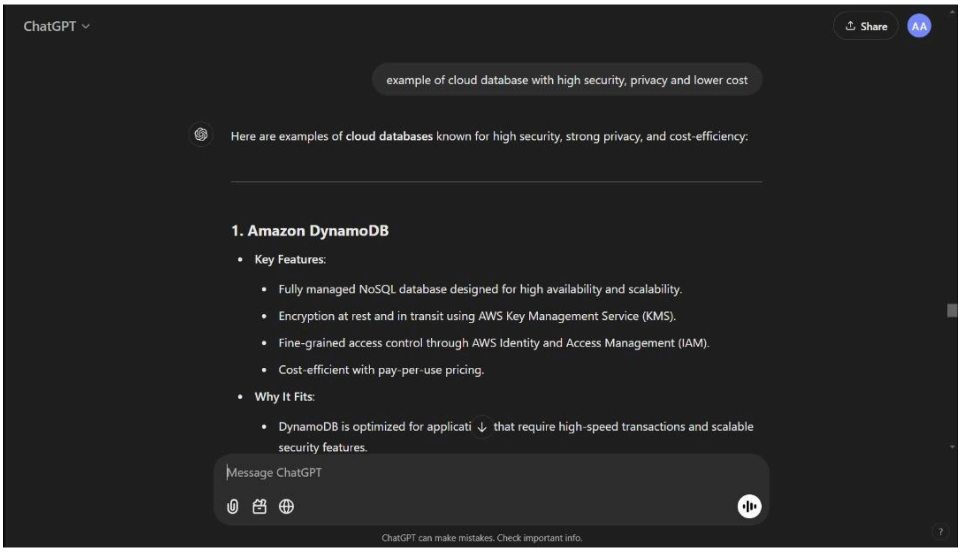
Rephrase sentence

AWS Storage Gateway can simplify our application's storage management ~~and reduce~~ , **reduce** costs for key hybrid cloud storage use cases ~~as well as ensure smoothness in interactions of the application~~ **, and ensure smoothness in the application's interactions**.

Figure 5: Screenshot AI Writing Assistance Using Grammarly

URL: Grammarly: Free AI Writing Assistance

2. ChatGPT *(For suggestions into integrated software)*



example of cloud database with high security, privacy and lower cost

Here are examples of **cloud databases** known for high security, strong privacy, and cost-efficiency:

1. Amazon DynamoDB

- **Key Features:**
  - Fully managed NoSQL database designed for high availability and scalability.
  - Encryption at rest and in transit using AWS Key Management Service (KMS).
  - Fine-grained access control through AWS Identity and Access Management (IAM).
  - Cost-efficient with pay-per-use pricing.
- **Why It Fits:**
  - DynamoDB is optimized for applicati ↓ that require high-speed transactions and scalable security features.

Figure 6: Screenshot Generative AI Assistance Using ChatGPT

URL: ChatGPT Chat History on Amazon DynamoDB