UPLB Cashier Notification Services: Data Security using Advanced Encryption Standard

Andrea Nicole Privado and Concepcion L. Khan

UPLB CASHIER
NOTIFICATION SERVICES

Rationale

from UPLB
Cashier's Office

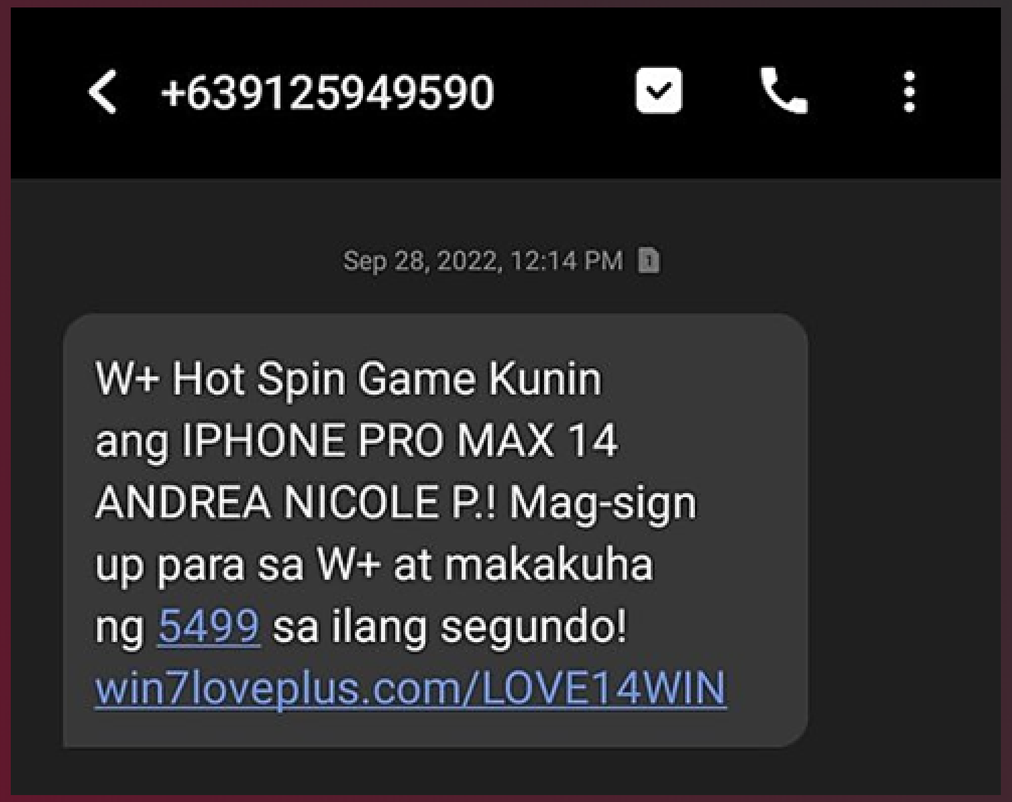
https://cdn-icons-png.flaticon.com/512/88/88144.png
https://img.freepik.com/premium-vector/smishing-concept-hacker-inserting-cell-phone-sms-fraudulent-use-alert-trap-messages_594511-426.jpg

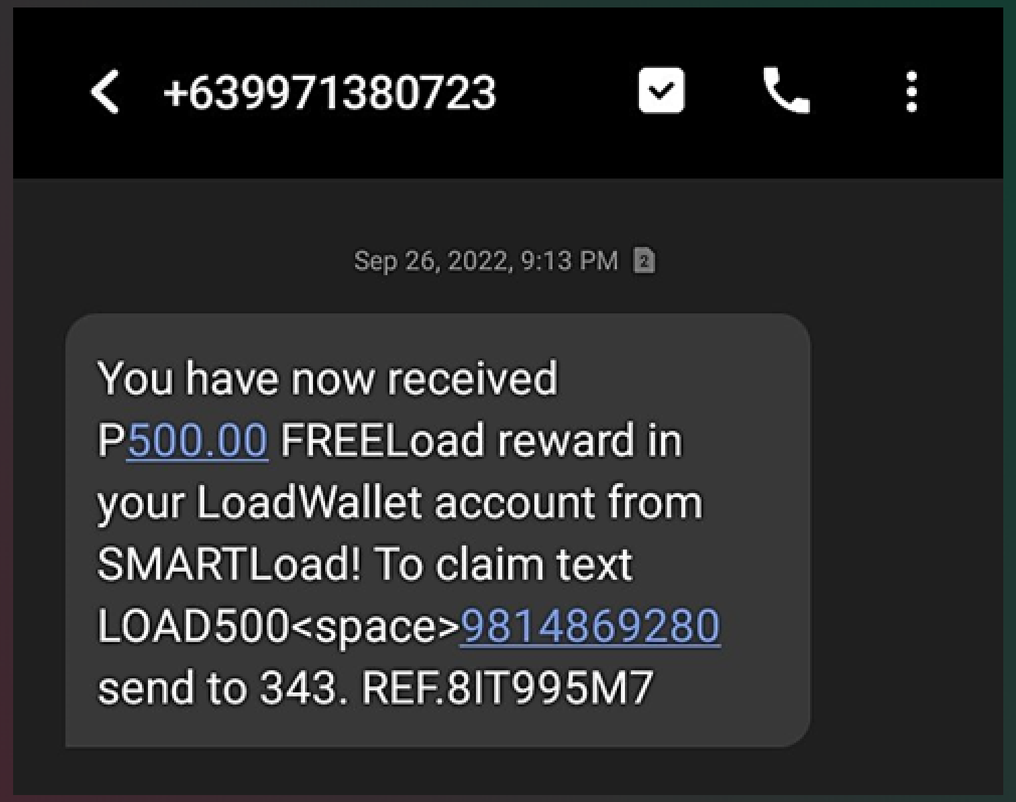
Rationale

from UPLB
Cashier's Office

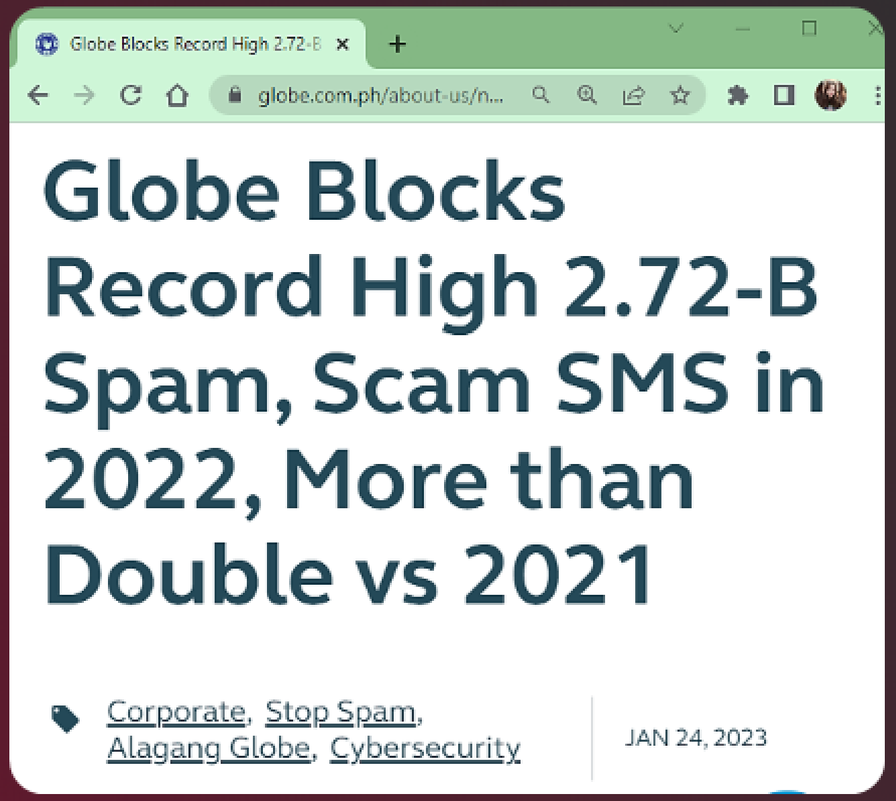
https://cdn-icons-png.flaticon.com/512/88/88144.png
https://img.freepik.com/premium-vector/smishing-concept-hacker-inserting-cell-phone-sms-fraudulent-use-alert-trap-messages_594511-426.jpg

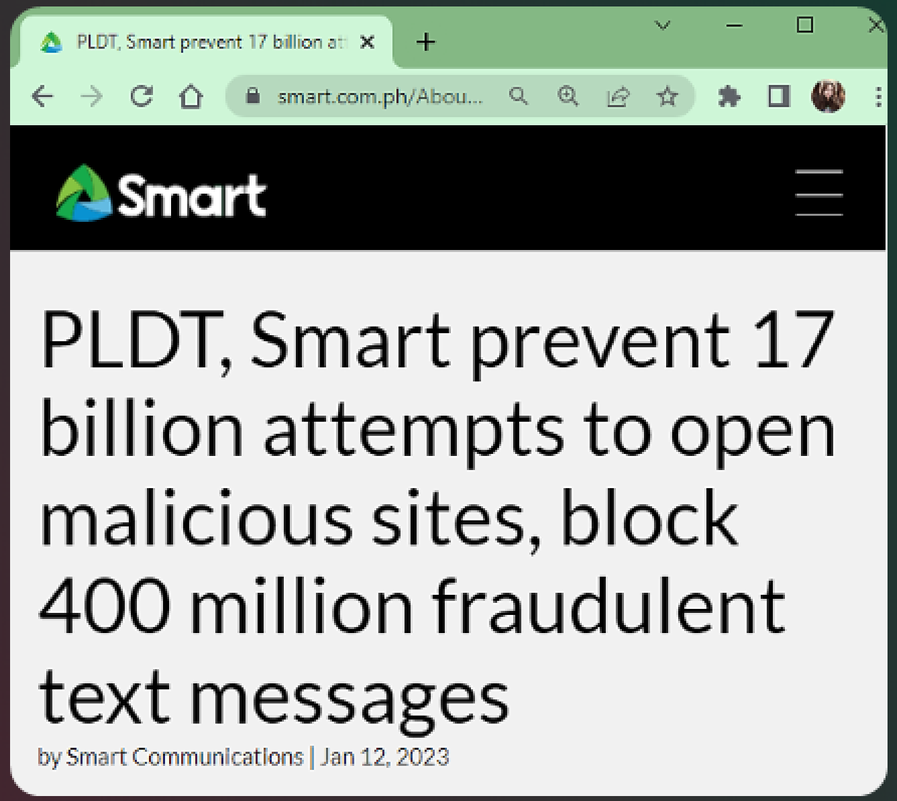
Smishing


+639125949590
Sep 28, 2022, 12:14 PM
W+ Hot Spin Game Kunin ang IPHONE PRO MAX 14 ANDREA NICOLE P.! Mag-sign up para sa W+ at makakuha ng 5499 sa ilang segundo! win7loveplus.com/LOVE14WIN


+639971380723
Sep 26, 2022, 9:13 PM
You have now received P500.00 FREELoad reward in your LoadWallet account from SMARTLoad! To claim text LOAD500<space>9814869280 send to 343. REF.8IT995M7

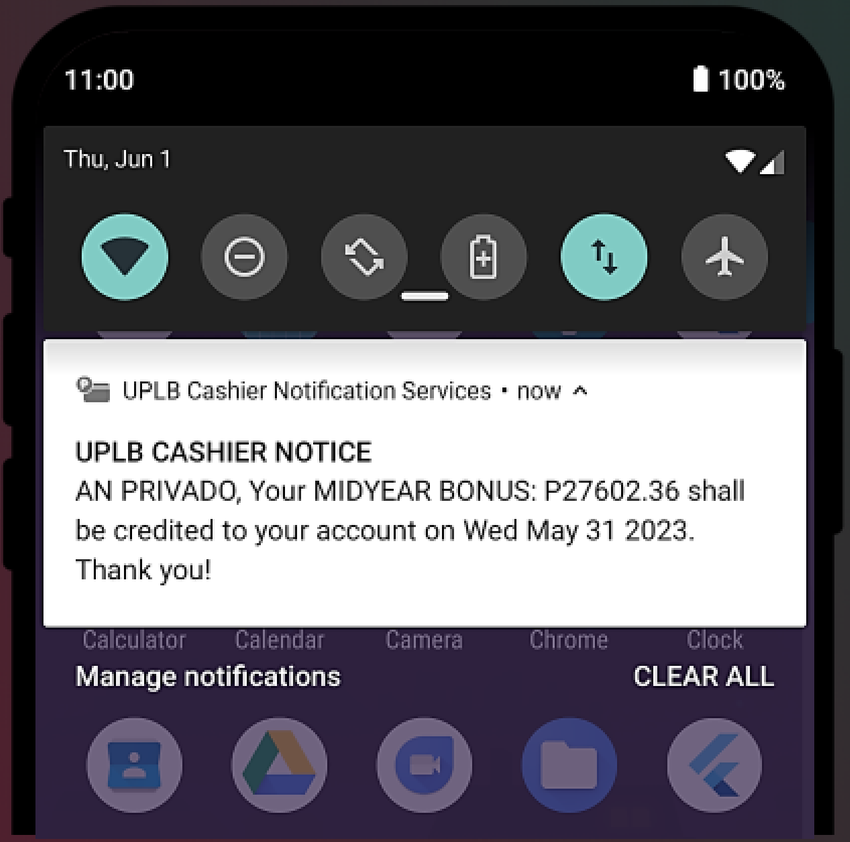
Actions of Network Providers





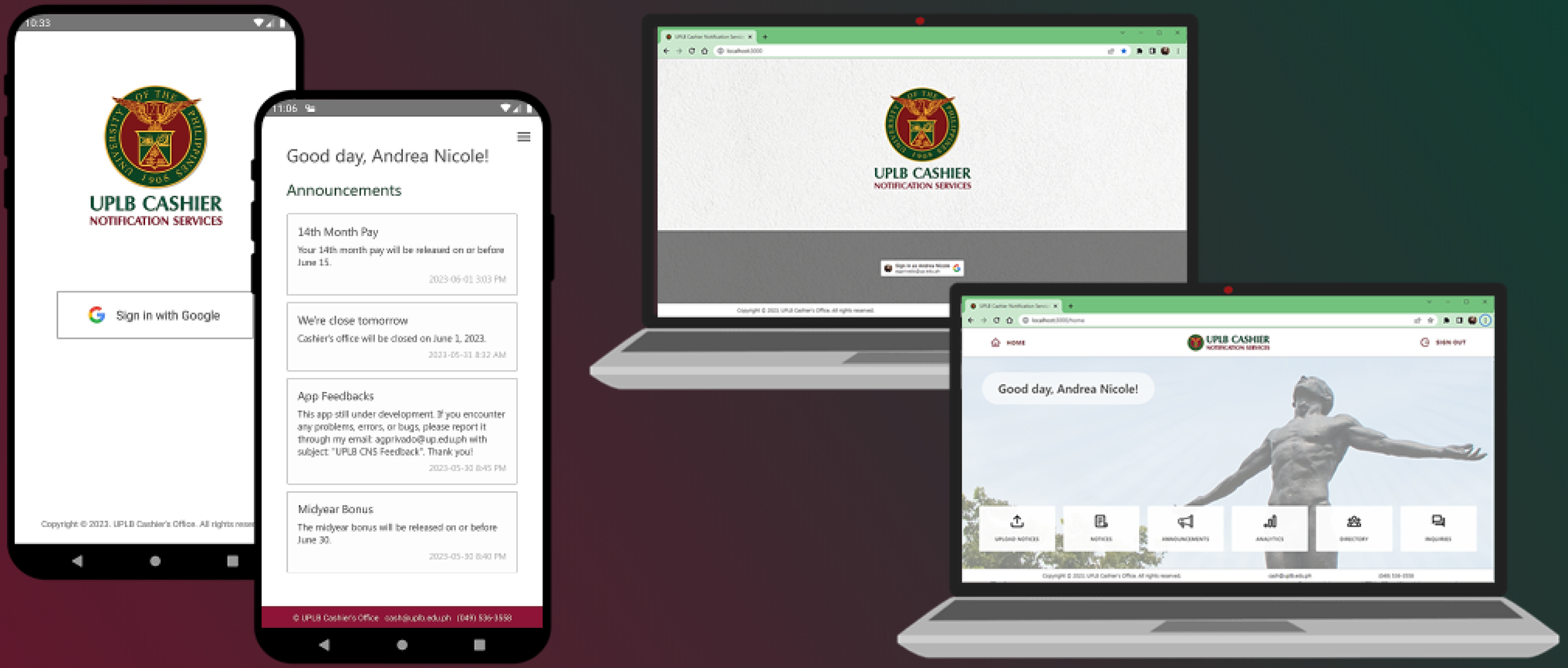
https://www.globe.com.ph/about-us/newsroom/corporate/globe-blocks-record-high-spam-scam-sms.html
https://smart.com.ph/About/newsroom/full-news/2023/01/12/pldt-smart-prevent-17-billion-attempts-to-open-malicious-sites-block-400-million-fraudulent-text-messages

Alternative to SMS Notification



Push Notifications

UPLB Cashier Notification Services

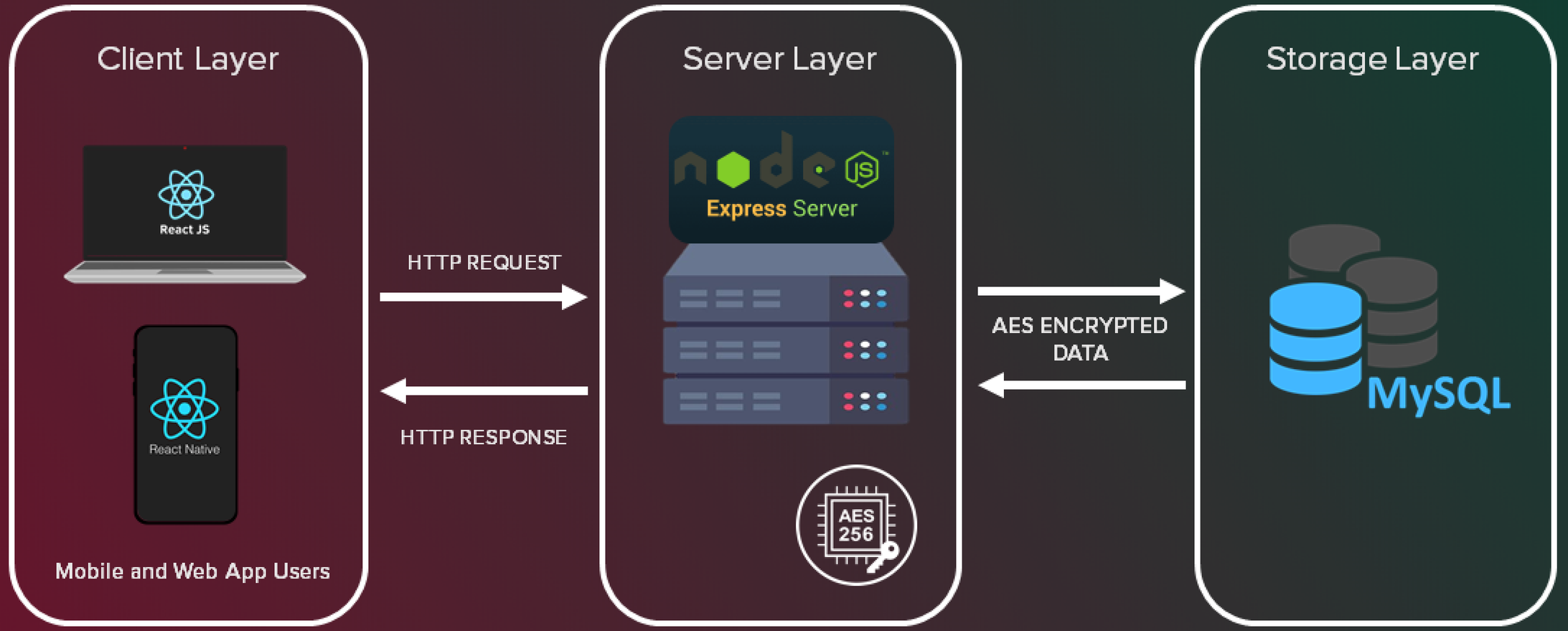


Objectives

1) Develop a mobile application for employee users to receive push notifications, monitor their notice history, and send an inquiry to the cashier's office.
2) Develop a web application for the administrator users to send push notifications to the recipients and for easy data management.
3) Implement end-to-end encryption on mobile app push notifications using AES.
4) Implement AES encryption on the data within the database.

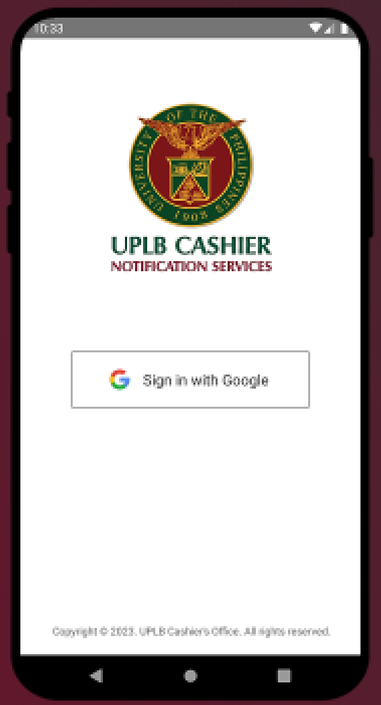
Software Framework & Tech Stack

Client-Server Architecture

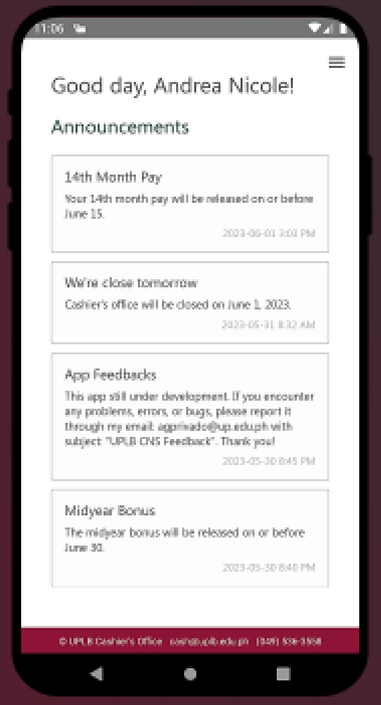


Mobile Application

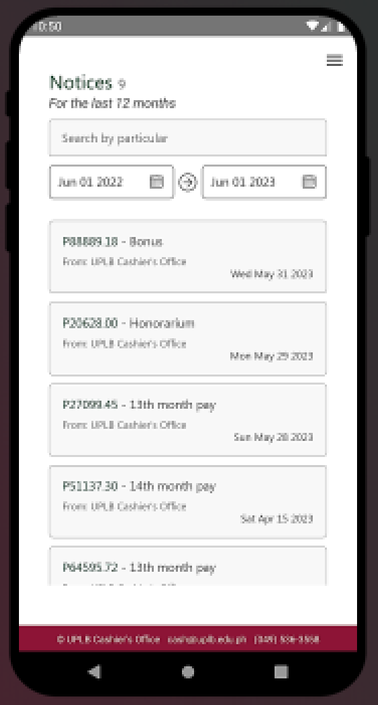
Features



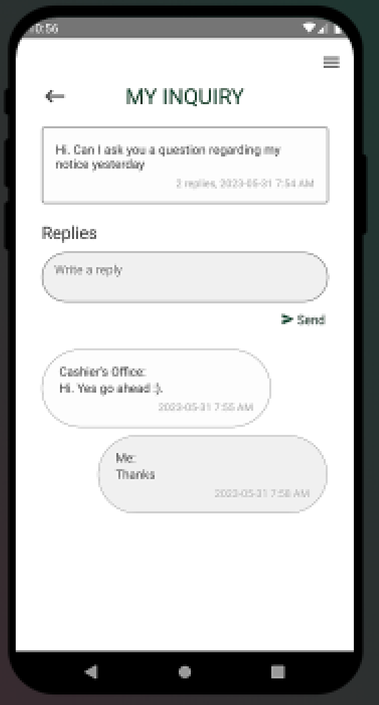
Google Sign-in



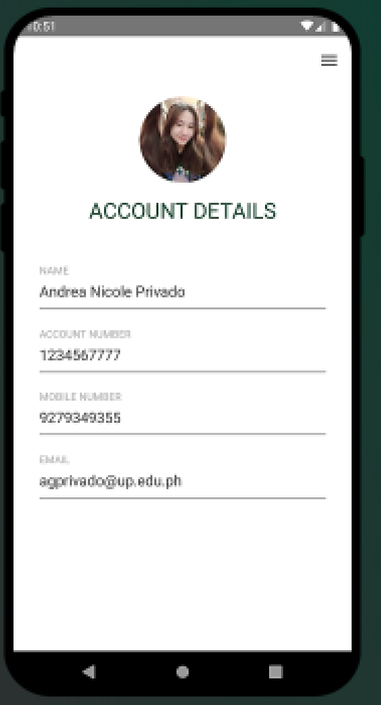
View Announcements



View, Search, and Filter Notices for the last 12 months



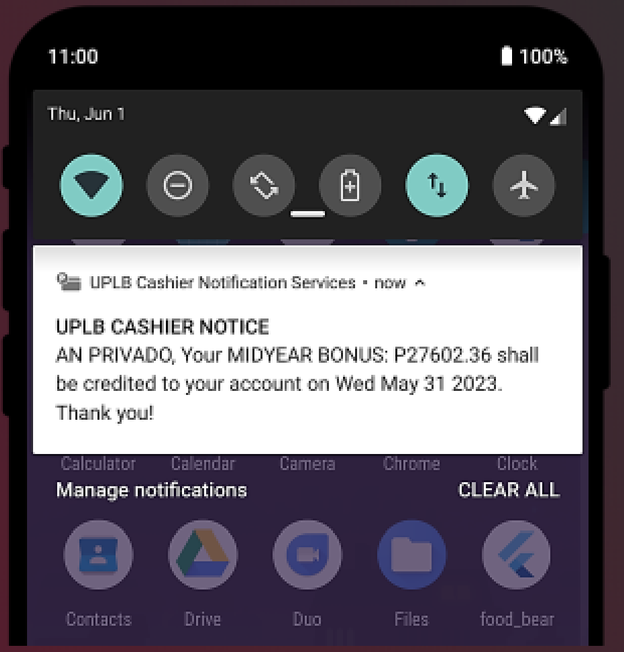
Submit and reply to an inquiry



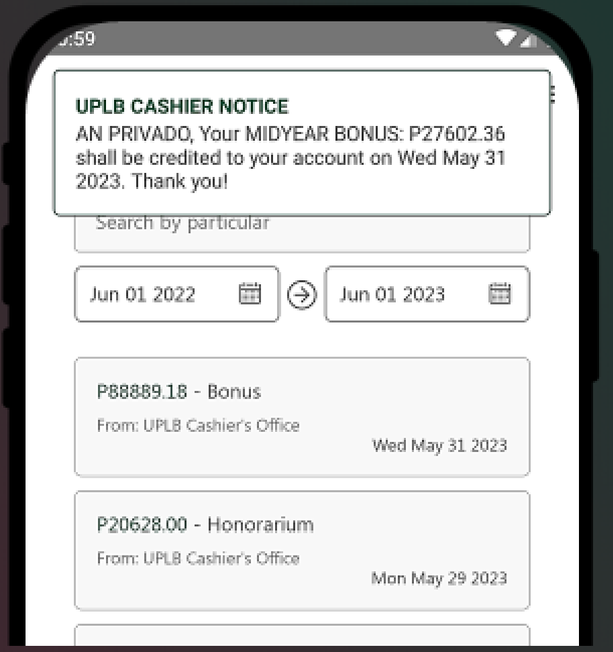
View Account Info

Mobile App Notifications

Types



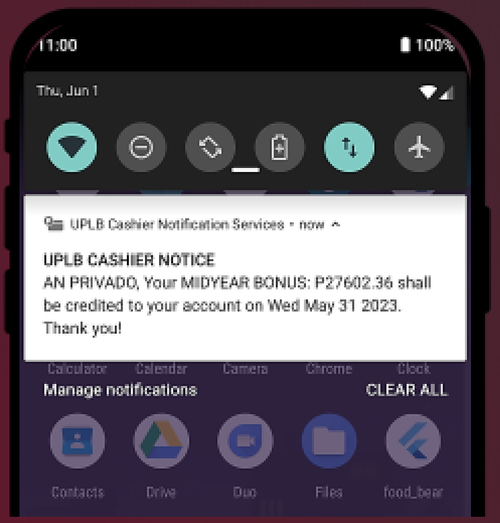
Push Notification



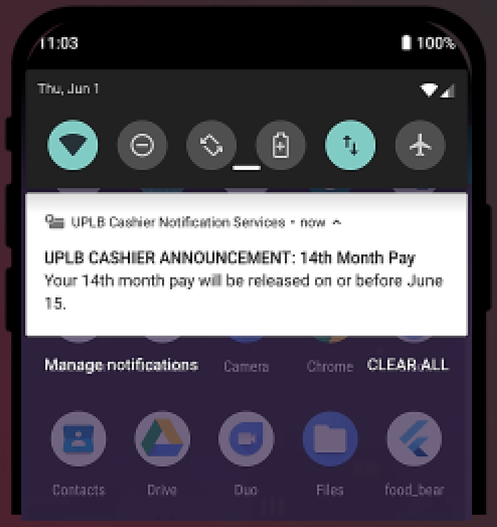
In-app Notification

Mobile App Notifications

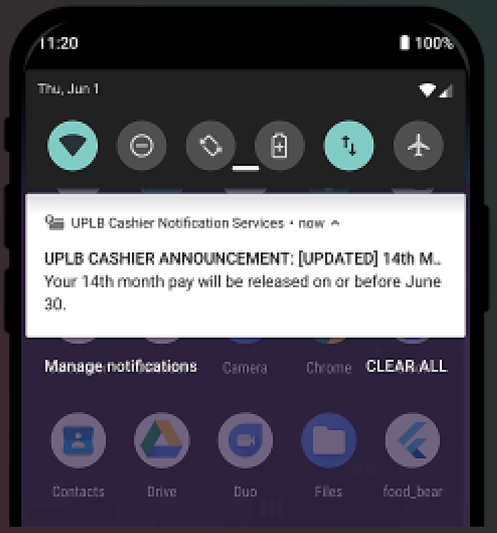
Categories



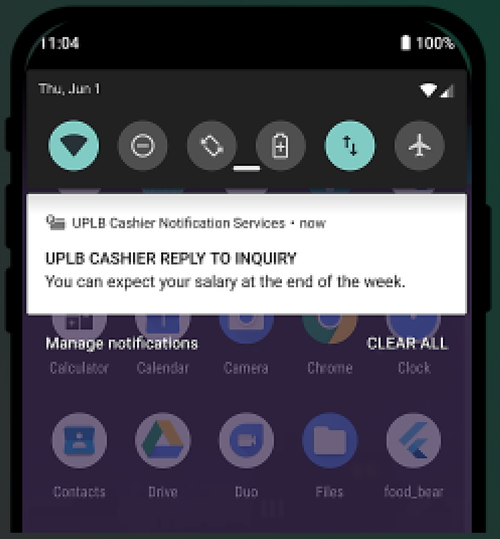
Individual notice



New Announcement



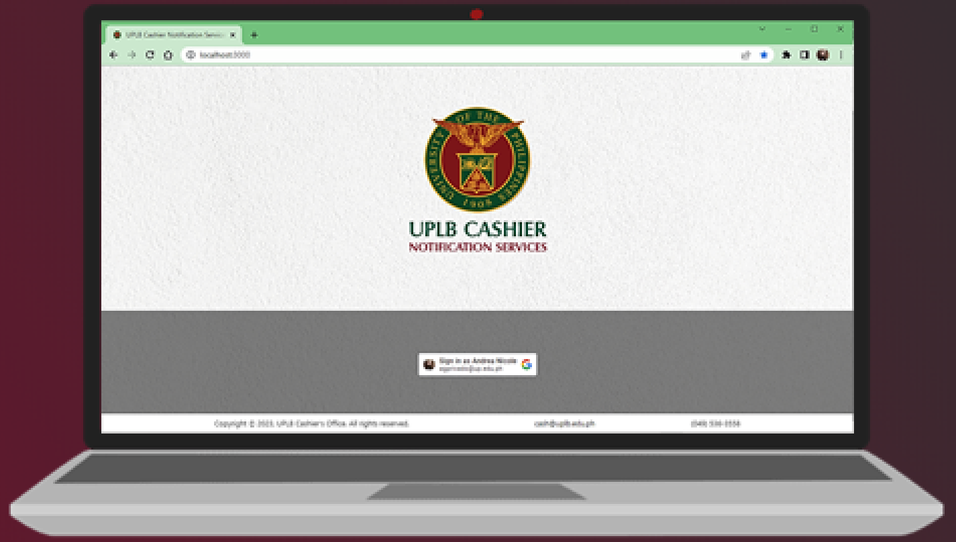
Edited Announcement



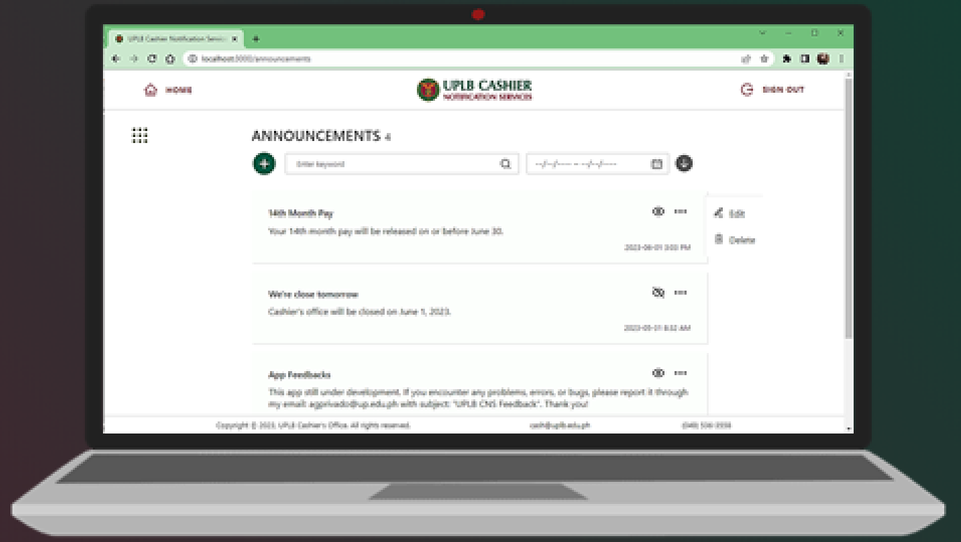
Reply to Inquiry

Web Application

Features



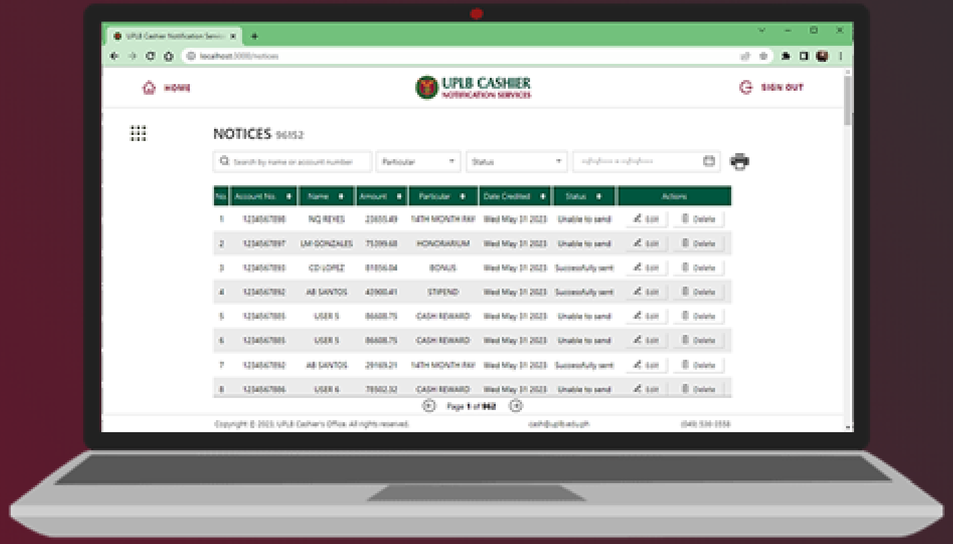
Google Sign-in



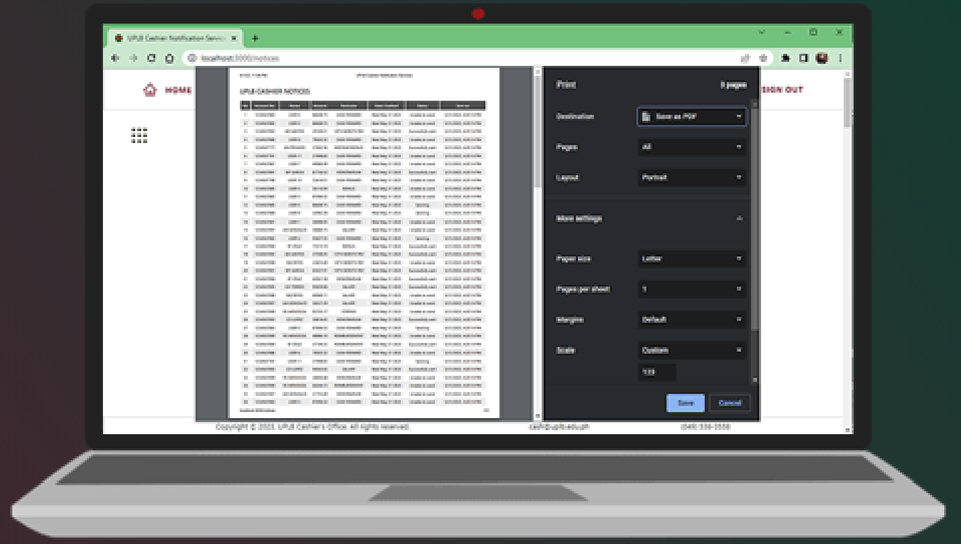
CRUD Announcements

Web Application

Features



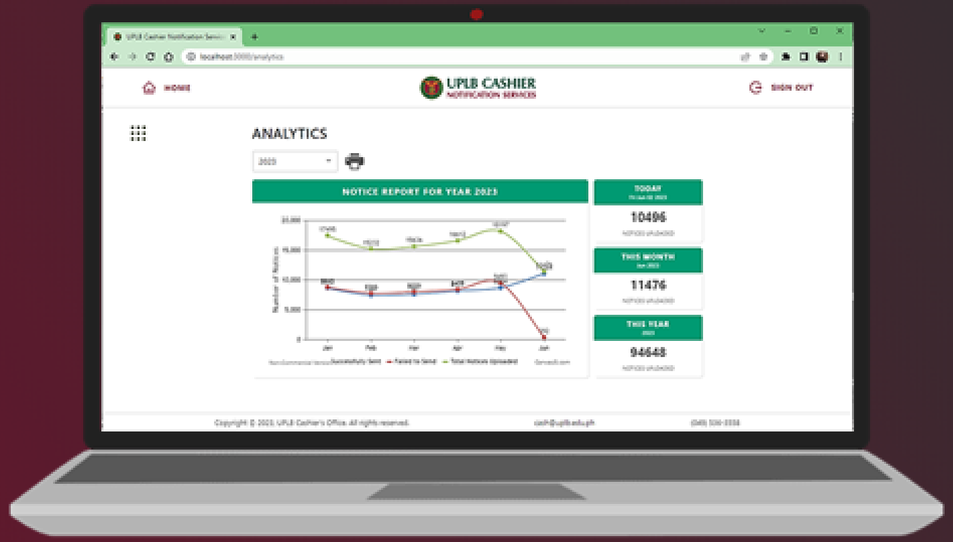
CRUD Notices



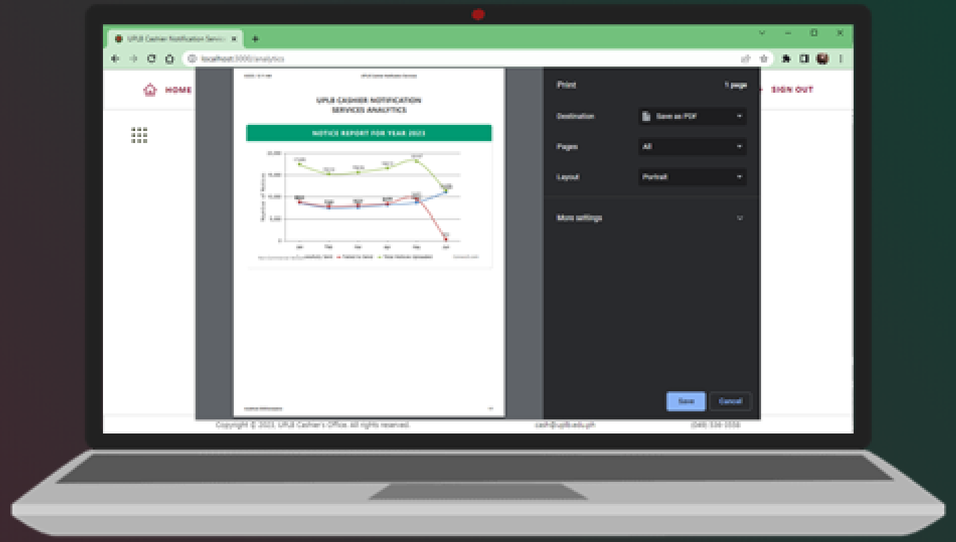
Print/Download Notices

Web Application

Features



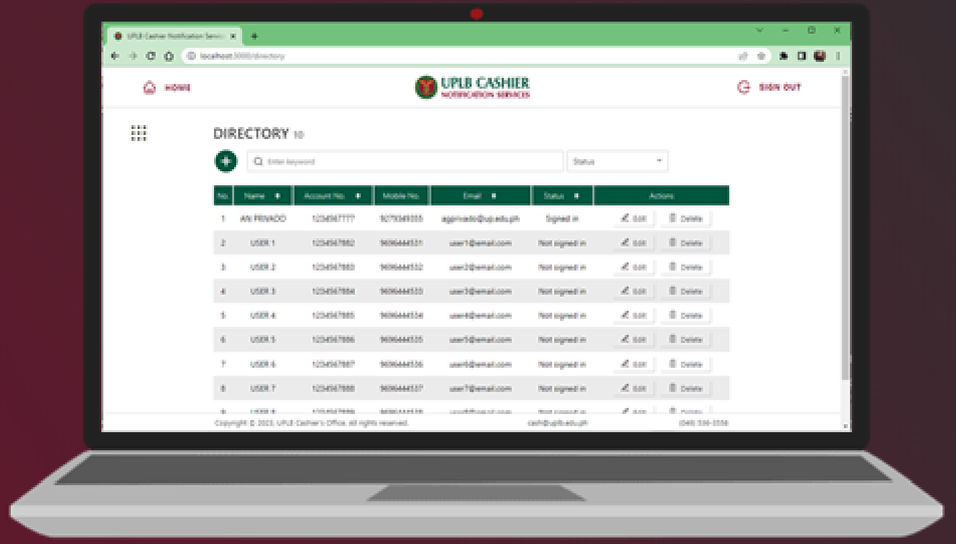
Analytics (yearly notice report)



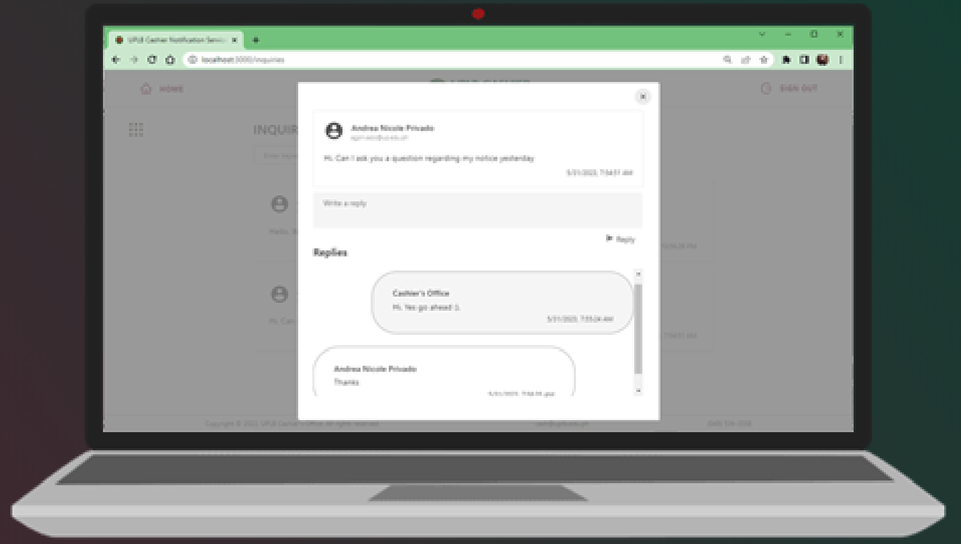
Print/Download Analytics

Web Application

Features



CRUD Mobile App Users



Reply to Inquiries

System Usability Scale Results

92.5

Mobile Application

10 participants
(3) LRC, (4) ICS, (3) IMSP

82.5

Web Application

2 participants
Cashier's Office Employee and Supervisor

System Performance and Scalability

100,000+

Stored data

(provided that most of the data are encrypted text)

50,000+

Volume of requests

System Efficiency

2 hours

SMS Bulk Messaging

2000 messages

(info from cashier's office)

5:10 mins

Push Notifications

2000 notices

(avg of 3 runs)

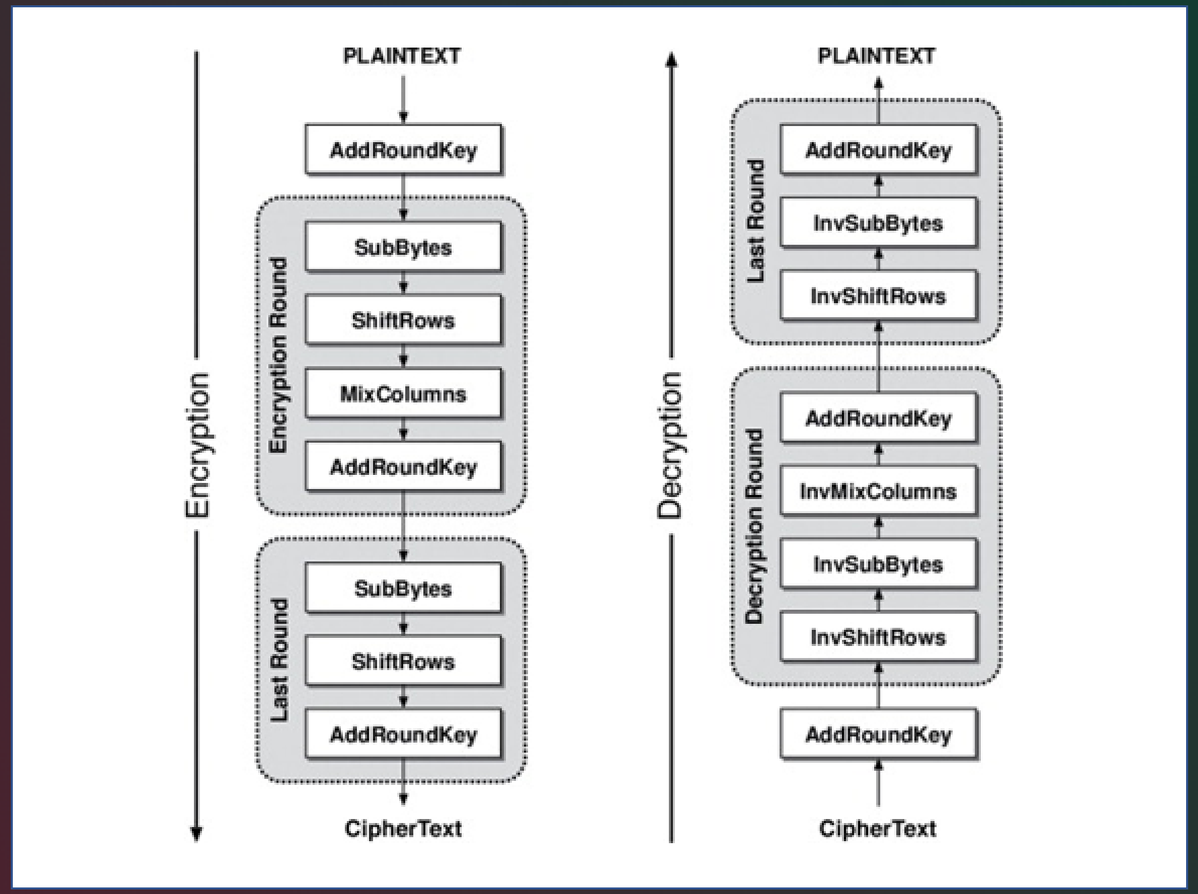
AES Algorithm

Advanced Encryption Standard (AES) 256 is a virtually impenetrable symmetric encryption algorithm that uses a 256-bit key to convert plain text into cipher text.

AES Encryption and Decryption

Algorithm

1. BYTE SUBSTITUTION
2. SHIFT ROWS
3. MIX COLUMNS
4. ADD ROUND KEY



https://ars.els-cdn.com/content/image/3-s2.0-B9780128022221000002X-f02-03-9780128022221.jpg

AES Encryption Configurations

14 encryption rounds

256-bit key

128-bit initialization vector (IV)

128-bit authentication tag

AES Encryption within the Database

```
mysql> select registered_name, account_number, email from users order by registered_name;
+-----------------+--------------------------------------------------------------+--------------------------------------------------------------+
| registered_name | account_number                                               | email                                                        |
+-----------------+--------------------------------------------------------------+--------------------------------------------------------------+
| AN PRIVADO      | UFHJF1E1lWx1wOD9hBWJZf/UTqiuQGePaWs5uATP0SToBRDChVE1p0z+ | ctmk3NZmKdh3zTRsYplqC2eIe2+M1r5sTBRPfNfYMq0l/NR0eLAhCyRmNHTAoF7y6dm+ |
| USER 1          | gRpzc0lJbHnmDhC4L/Jn05pCI4qIAzCf+Etxv5MkGWNmr6XoPeRRTv8X | aK2tsYL0m+azg8oCYQKODpF0RK152iaR+ByIYHHjwg4et21XO34xst3VLeoGTK4= |
| USER 2          | T3xgNrR9RT9y/1UETHVOY1DURzvdQ8W9PFs11Ocv4+PgCpmKCK7NXIgB | b2PEsYXMWkMAlI4xLoTPDvarhwFT1Gx3DQZhAD8Bm8NWyhLwEuerffJ5I/OGJAs= |
| USER 3          | Itu/QDgtK4wSCecp12ilOXGmK1rBsbnXrQvMCuH3PpGebIsgrWjnwdic | 6PjhqLcJACzvhH3aMsh5u8Rgxy1aHolquSn1KUr7U+9ubzdRCztAspwIWnAz2+Y= |
| USER 4          | ASda5/gPUUN54jEuy1XBQVF2cM5R5RLO28r5PbDJLgRYmve5DEfcB/5A | kW5yDMdl17mUiYu5b0/K4fTZWW2JWYfqiUAbN6OOjcwGvgCM2iJOYxmp2IscrDI= |
| USER 5          | gWBSToprsmPZDuJSHd68+7ABQQi8gvTc7mVaSDKPN/nYbLOXWyW3y9EE | FvbO9cmZnK4xZLD6Jep40kUXQsEdnI6dVrvx9ghYqJqJg4zz8XfNTF+5PhXvCYQ= |
| USER 6          | UGkeWjqM3CHUhl1d8HMFLJ1HNUsQc0rPKJWyrD/pAVSFMsgvYf+FjxVz | iqsavd8vDLAcS9uUB2Jjoxed2fir6dFtsxaDfqK1n1eNCy1WtvvDXVZ63UuHamw= |
| USER 7          | G8zCZuR8puQIKyNWTy4Lt8BCHiAIIsLynhDqIGSqyjtEkZd5Oq3iwoto | 44+y7hcEpKkrYJDJ0nFhRcZBrkmnvHy+J2SVQx8NL8v8q2HKMtUB0W/obvzpH2M= |
| USER 8          | 1/YQk7Gi+DN2HsT9ranzbgEa9tWObzTrjgHv9EYMS1KMWcxN8xUAe1n/ | BZbaJZYP2T17SKsZjIOUdjKSENpfb2PI6F/D5rYiZ613xDvj7pKSdbHsEya4/P4= |
| USER 9          | BbAF0dKFZFlBiOLf9toQDvBXLQJYLNgUle3IBwoYt+ujOY7ZSzvcZRFN | eeW2PtZbWNNE0SqlRkFqYPJU9c6oki9k14RXInwJyxJ/8QdBVg0zSntgBQ== |
+-----------------+--------------------------------------------------------------+--------------------------------------------------------------+
10 rows in set (0.00 sec)

mysql> select registered_name, amount, particular from notices limit 20;
+-----------------+--------------------------------------------------------------+--------------------------------------------------------------+
| registered_name | amount                                                       | particular                                                   |
+-----------------+--------------------------------------------------------------+--------------------------------------------------------------+
| LM GONZALES     | YPgMIKxlOrLtsciyDMI5nI19Tto5nXHBE0VPtLEjHWoODj/M3QQaFQ== | gaKu4oClJQxj9mCtYuF7xyxaTetHSVwJ7KzLSz4Xw/sfEimUKkNKHEe6ra3RVg== |
| LM GONZALES     | xxNbs04Hy1P9y936Y1NvzdZ8W+T1GMlylfmEYVZtkWZjiOHqHlX3bQ== | 4LcfHsi9kpuSh9iu8xusIAf0z6lBKbZ2jrhIxZ9SmGQlNj5Vyr7h |
| RS MENDOZA      | HKVfdly9vs7LnBI3vS53N+mBuIvoOTVG9/rNr+FcBIlJrA818fLPAw== | e1yyurfpBH1LkiJswRP1sk73wcmPHPqyPueh3VBHbLknAGoOawW8sFWg |
| AB SANTOS       | sbaB+PuCE6Xm3yEAFueLMQF0McT9v9I9d36nsm36tws1/uaZGrWt6w== | cP/8FHfeLkXpl+U5T3sNzpPItcEOk8APPiSzTPn6zZVpq8Cldbi3/7p8 |
| IJ RAMOS        | 6NCClHkuLB+XD7WFUxShw0LLKaLRpvMQAuXFCheSaaa3+tTM58iFHw== | L8KMzBw7U6TJbqy4mQjU1p0QshT99ZDdkEd56x5J/ghdrk9irw== |
| AB SANTOS       | nGaw3U7Avy5at4IBdSLUJbSd4QwZamkZCoS+ewA3UsYel2phX5Puhw== | iw/BcEBFcsXH/iWXsbe6VM8hTUD377rRNLwEm8yToVTEJSaNNRptvjwJH3Ku |
| GH TORRES       | htKzNsevoLZ5aeb5ooJMXSswO1K7L+Npf78JmQopC53wjTwDAZyNng== | /uDQP4H7AGEtMV1vj+pvWrMa4neZMq830i8J0p2k87191Sa7zI31RMZc |
| CD LOPEZ        | plXVGXUX1SvZh1dZtxfNUnXIMQ9zJd2VNJMXOrrTDXCtqJKl10ZcMw== | KTNhTfsP06zPCgcuERL7ZDW5L9uyxANPRiDOaNjulj7rL7pC/A== |
| RS MENDOZA      | LYYYVq+7A0Hu3IN9RYiAPufzAFisIJcRkYSoZc92vLc3esuhqYUn7A== | udyaaQa5YfGJi65QSc5BhP7TbTLb0zNw4fRP0cf5XZsZz0XbHMY= |
| AB SANTOS       | ZH0OSZoGVUdYLJ8QZbBHnTHq3RVf6UsKMNkds5QfYViyM6IMaNyGsQ== | 8y26/Snr81qD6p2FUui+K/YsaENS8PlNgzu9+wCoRg9SA6946XOc |
| RS MENDOZA      | DXene+9auNvoP8ZVjttBiq6yR50dCA6MszEwJsgsNM0xb05/nl+vVg== | SEfi5BVe/1s8Me3tk/5kp4HqVM4LSLsDy1XGaAuUAqGKERQB0B6uDTmTWNYl |
| RS MENDOZA      | OcyTOYYgf6GvHc4Ucp916dKOLpIiE+s5MGiAqb+carpB6/31vgW/HA== | ishzJEV3C1QJNVVKy53TCxfcYHNFBYGSAJmqQD3GxOEqMcqtYTw= |
| EF CRUZ         | bufITOhjZUdwgxL1Qp5Z5wvEIBJX3BhszDWREGQgnOBBYD8nYR9YzQ== | bBSdcGR8U72BWy0SWmmQYM3X6tEqm6DHqhxn5MqLNt1kiNgCXw0= |
| NQ REYES        | P7QhgCD3Y1ZEf28Hh7sU8qsqhqtonyLUQKlPt4xTdCNAVatkkIalpQ== | 73WulTZGuP36e05T0Q2m8LC34ewfZllEY08qj4qG+h16B2eNESdvEmUW0bsLfQ== |
| LM GONZALES     | U5OubFRHZxi2OhwXPmA1ZIocLgfMO+8M9rvZQrkg8SnER1SXkki1WQ== | dMckEcEMwgcF8G0BZs5IPHD+vw2f88c+BcjDglLVlsJb4AmQJLcE5f+DURf/ |
| NP GARCIA       | QOr8KSev2oaEnwY9Weis22ToeQ0mqsww9R2jnl/DiP6STsEzyRi82Q== | thJbMI/JGV51qs7rkyloE3D95dNtW2fvFO5eVYqtw3uaU0IaRYNZgqZoXHIFIw== |
| EF CRUZ         | poTbAkthm3YaljUFI5fTeq48aJSHfHZ0j1QwFqh7ws7oxcDGTFWHVw== | PHZSaGt9CaJIE794L3b7W2K0TFaFPp4z4JQMDIZhtj+O4rPXEQ== |
| EF CRUZ         | ojzIpiuCwlwuuTpUUDHvhgMgINXUe53DkpIp2bZjQ1Zbr1fo4/Tb/A== | SxSceJLsQ/v/Wtpp7SGUPPLwnlI0qNrZpiWnaF3zjPcjhS0UXg== |
```

Web Vulnerability Scan Result

Acunetix

Acunetix
by Invicti

Comprehensive Report

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Scan Detail

Target	https://uplb-cns.onrender.com
Scan Type	Full Scan
Start Time	Jun 19, 2023, 9:54:53 PM GMT+8
Scan Duration	33 minutes
Requests	21148
Average Response Time	69ms
Maximum Response Time	22358ms

URL Tested: client-side URL

SQL Injection Testing Result

SQLMap

"All Tested Parameters do not appear to be injectable."

```
[16:53:41] [ERROR] all tested parameters do not appear to be injectable. Try to increase
values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that
there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use
option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent', skipping to
the next target
[16:53:41] [INFO] you can find results of scanning in multiple targets mode inside the CSV
file '/tmp/sqlmapoutputo12vpemq/results-06222023_0443pm.csv'
```

URL Tested: one of the server's HTTP request URLs
Parameters tested: 4

Conclusion

- The system has above-average to excellent usability
- The system has been developed with security measures in place and is resilient against common SQL injection and web-based attacks.
- Incorporating AES encryption into the system mitigates the security risks linked to the storage and transmission of sensitive data.

Recommendations & Future Work

- Mobile OTP Sign-in for Mobile App Users
- A quick reply feature or an AI-based response system for admin users on the inquiries page.
- Test and deploy the mobile application on both Android and iOS
- Notification module can also be used to develop software with mobile notifications for other UPLB departments or even university-wide notification services.

UPLB Cashier Notification Services: Data Security using Advanced Encryption Standard

Andrea Nicole Privado and Concepcion L. Khan

UPLB CASHIER
NOTIFICATION SERVICES