Presented to the College of Computer Studies Department

De La Salle University – Manila Campus

Term 1, A.Y. 2025 - 2026

CCINFOM - S24

Proposal for Database Application

Section 1: Group Composition

Hallare, Zach Benedict I.

Campo, Benette Enzo V.

Martin, Kurt Nehemiah Z.

Ravelo, Georgina Karylle P.

Section 2.0 Rationale for DB App Development

Malicious digital attacks such as phone scams, phishing links, ransomware, and identity theft are rising threats in the Philippines and worldwide. Excel spreadsheets cannot handle the complexity of tracking perpetrators, linking multiple attack types, and managing victim reports. A Java + SQL database application offers a structured and scalable platform for storing incidents, identifying attack patterns, and blocking malicious entities. It provides IT services by delivering cybersecurity protection, database management, and user support. This system enhances safety and operational efficiency through automated monitoring, notifications, and reporting.

Building on this foundation, the app helps victims by recording the malicious attacks they experience, linking each report to the perpetrator and attack type, and building a history of incidents for every victim. When multiple victims report the same perpetrator, the system can automatically escalate the perpetrator's threat level to "Malicious," allowing administrators to take further action. It also monitors victims who are repeatedly targeted, updating their account status and notifying admins to provide support or training. Finally, it generates reports showing how often victims are attacked, helping them stay aware of their cyber risk.

System Scope and Boundaries:

- Intended Users: Victims (public users), system administrators, and cybersecurity staff. Victims submit reports of attacks, while admins validate and process them. Cybersecurity staff review patterns, investigate threats, and coordinate with external agencies if needed.
- Interfaces: Victims access a secure Java-powered interface to submit and track reports. Admins and staff use an internal Java-based web dashboard with analytics and management tools.
- Integration of Blocked Data: Confirmed malicious perpetrators' identifiers (phone numbers, URLs, accounts) can be exported and optionally shared with telecom providers (telcos), internet service providers (ISPs), or government cybersecurity agencies.
- Data Privacy and Security: All victim and perpetrator data will be encrypted at rest and in transit, protected by role-based access controls, and anonymized in reports. The system will comply with the Philippine Data Privacy Act of 2012 (RA 10173). Security audits, intrusion detection, and multi-factor authentication for admins will be implemented.

Section 3.0 Records Management

Core Record	Fields	Assigned To
Victims Record Management	**Fields:** VictimID, Name, ContactEmail, AccountStatus, DateCreated **Viewing a Record with Other Related Records:** View a victim record and the list of attacks they reported.	Campo, Benette Enzo V.
Perpetrators Record Management	**Fields:** PerpetratorID, Identifier (Unique traceable detail), IdentifierType, AssociatedName, ThreatLevel (UnderReview / Suspected / Malicious / Cleared), LastIncidentDate	Hallare, Zach Benedict I.

	Note: An identifier refers to the unique piece of information used to distinguish and track a perpetrator in the system (Example: 09171234567, 203.177.42.18, phishingscam@fake.com). **Possible IdentifierTypes:** - Phone Number - Email Address - Social Media Account / Username - Website URL / Domain - IP Address **Viewing a Record with Other Related Records:** View a perpetrator and the list of victims and attack types linked to them.	
Attack Types Record Management	**Fields:** AttackTypeID, AttackName, Description, SeverityLevel (Low / Medium / High) **Viewing a Record with Other Related Records:** View an attack type and all perpetrators associated with it.	Martin, Kurt Nehemiah Z.
Administrators Record Management	**Fields:** AdminID, Name, Role (System Admin / Cybersecurity Staff), ContactEmail, DateAssigned **Viewing a Record with Other Related Records:** View an administrator record and the list of incidents or evidence they validated.	Ravelo, Georgina Karylle P.

Section 4.0 Transactions

Transaction 1: Incident Reports Transaction

- **Assigned To:** Campo, Benette Enzo V.
- **Core Records Used:** Victims Record Management, Perpetrators Record Management, Attack Types Record Management, Administrators Record Management
- **Transaction Record: IncidentReports**

- **Attributes:**
    - IncidentID
    - VictimID
    - PerpetratorID
    - AttackTypeID
    - AdminID

    - DateReported
    - Description
    - Status (Pending / Validated)

- **Services/Operations:**
    - Read the victim's record to confirm account status.
    - Verify if the perpetrator's identifier already exists in the database.
    - Update an existing perpetrator's record or insert a new one if needed.
    - Select the appropriate attack type.
    - Assign an administrator for validation.
    - Create a new incident report linking VictimID, PerpetratorID, and AttackTypeID with the date and description.
    - Trigger a system check to detect repeat offenders and notify the administrator if thresholds are reached.

Transaction 2: Evidence Upload Transaction

- **Assigned To:** Hallare, Zach Benedict I.
- **Core Records Used:** Incident Reports Transaction, Administrators Record Management
- **Transaction Record: EvidenceUpload**
- **Attributes:**
    - EvidenceID
    - IncidentID
    - EvidenceType (Screenshot / Email / File / Chat Log)
    - FilePath
    - SubmissionDate
    - VerifiedStatus (Pending / Verified / Rejected)
    - AdminID

- **Services/Operations:**
    - Link uploaded evidence to an existing incident report.
    - Store file path or storage location in the database.
    - Allow administrators to update verification status.
    - Notify cybersecurity staff if verified evidence strengthens a malicious pattern.

Transaction 3: Perpetrator Threat Level Update Transaction

- **Assigned To:** Martin, Kurt Nehemiah Z.
- **Core Records Used:** Perpetrators Record Management, Incident Reports Transaction, Administrators Record Management
- **Transaction Record: ThreatLevelLog**
- **Attributes:**
    - LogID
    - PerpetratorID
    - OldThreatLevel

- NewThreatLevel
- ChangeDate
- AdminID

- **Services/Operations:**
  - Read perpetrator's record from the Perpetrators table.
  - Count unique victims reported in Incident Reports.
  - If the threshold is met (e.g., 3 or more victims in 7 days), escalate ThreatLevel.
  - Insert a log entry documenting the change.
  - Notify cybersecurity staff of the update.

Transaction 4: Victim Account Status Update

- **Assigned To:** Ravelo, Georgina Karylle P.
- **Core Records Used:** Victims Record Management, Incident Reports Transaction, Administrators Record Management
- **Transaction Record: VictimStatusLog**
- **Attributes:**
  - LogID
  - VictimID
  - OldStatus
  - NewStatus
  - ChangeDate
  - AdminID

- **Services/Operations:**
  - Read the victim's record from the Victims table.
  - Count the number of incidents reported in the last month.
  - If the victim has more than 5 incidents, update their AccountStatus to "Flagged."
  - Insert a log entry in VictimStatusLog documenting the status change.
  - Notify the administrator that the victim has been flagged for assistance.

Section 5.0 Reports to be Generated

Report	Assigned Member	Description
Monthly Attack Trends Report	Martin, Kurt Nehemiah Z.	**Core Records / Transactions Used:** Incident Reports Transaction, Attack Types Record Management, Perpetrators Record Management, Evidence Upload Transaction **Description:** Generates a monthly summary showing the number of incidents grouped by attack type and perpetrator, including time-of-day patterns. Includes the number of evidence submissions per incident to help gauge report credibility. The user

		selects Month and Year.
Top Perpetrators Report	Hallare, Zach Benedict I.	**Core Records / Transactions Used:** Incident Reports Transaction, Perpetrators Record Management, Victims Record Management. **Description:** Ranks perpetrators (phone numbers, domains, accounts) by number of linked incidents in a selected month and highlights their known attack types. The user selects Month and Year.
Victim Activity Report	Campo, Benette Enzo V.	**Core Records / Transactions Used:** Victims Record Management, Incident Reports Transaction, Perpetrators Record Management **Description:** Shows the number of attacks reported per victim in a given month, highlighting frequently targeted victims and the perpetrators who targeted them. The user selects Month and Year.
Incident Evidence Summary Report	Ravelo, Georgina Karylle P.	**Core Records / Transactions Used:** Evidence Upload Transaction, Incident Reports Transaction, Administrators Record Management **Description:** Lists all evidence submissions within a selected period, showing type, submission date, verification status, and the administrator who reviewed them. The user selects Month and Year.

Section 6.0 Declaration of Generative AI Use

This proposal was drafted and written by the group members. Generative AI was used only for proofreading and for brainstorming possible transactions and reports to ensure compliance with project requirements. The final content, structure, and details of the records, transactions, and reports were determined and written by the group.