

GOVERNANCE PORTFOLIO

Group 3 - Gabrielle

Table of Contents

GOVERNANCE PORTFOLIO	Group 3 - Gabrielle	1
Table of Contents		2
Introduction		4
Roles and Responsibilities		7
Functional And Non-Functional Requirements		7
Functional Requirements		7
Non-Functional Requirements		9
Users		10
Customers		10
Owners		11
Initial Use and Misuse Case Diagrams		12
Final Use and Misuse Case Diagram		14
Use Case Scenarios		16
Misuse case Scenarios		16
General Activity Diagram		17
RACI matrix		20
Architecture Schematics		24
Overview of the System		24
Data Collection Layer:		25
Data Processing and Analysis Layer:		26
Database Integration Middleware:		26
Data Storage Layer:		27
Security and Monitoring Layer:		27
Reporting and Compliance Layer:		27
Web Application Layer:		28
Backup and Recovery systems:		28
Security and Resilience in the D.I.A.M.O.N.D System: A Comprehensive Approach		29
Data Protection and Privacy Compliance		29
Biometric Data Security		30
System Security Protocols for Data Integrity and Protection		31
Intrusion Detection Systems and Security Audits		32
Resilience Measures against Cyber Threats		33
Data Backups and Disaster Recovery		34
Physical Security Measures		34
Maintaining system Integrity and Reliability		36
Test Plan		37
Introduction		37
Test Objects		37

Test Estimation_____	38
Test Scope_____	39
Test Strategy_____	40
Assignment of Responsibilities_____	42
Test Approach_____	43
Test Cases Design_____	44
Exit criteria_____	54
Performance_____	56
Balanced Scorecard_____	56
Security Dashboard_____	62
People-device Symbiosis in Secure System Architecture_____	64
Introduction_____	64
Integrating System Design with Mitigation of Security Threats from Human Factors_____	64
User Acceptance and Self-reporting of Risks and Incidents_____	65

Introduction

The project “Driver Identification After Monitoring Offense using Numerous Databases”, also known as the “D.I.A.M.O.N.D” system, is a unique and complex approach to resolving public driving misconduct and to hold the person committing the offence responsible to it. As part of the systems governance (COMP60721) module, our group has undertaken the task of assessing the requirements and risks involved with the system and designing an appropriate architecture that accounts for all of the risks in order to build a resilient system that can withstand most of the external threats and can be expected to perform without any downtime.

The process of designing such a system was a gargantuan task that could not have been possible without the contribution of each and every member of the team. Instead of dividing and assigning separate tasks to each member of the team, we instead opted to tackle each subtask or a problem together with everyone’s input first with one or more members of the team leading the task. Then, with everyone’s input taken into consideration, the task was executed and then reviewed for further changes by others, with an open discussion for any disagreements or doubts, where we made changes to the drafted response if required. The workflow for the group, in fact, was the Deming cycle as once described in the class during the contact hours as per fig 1.

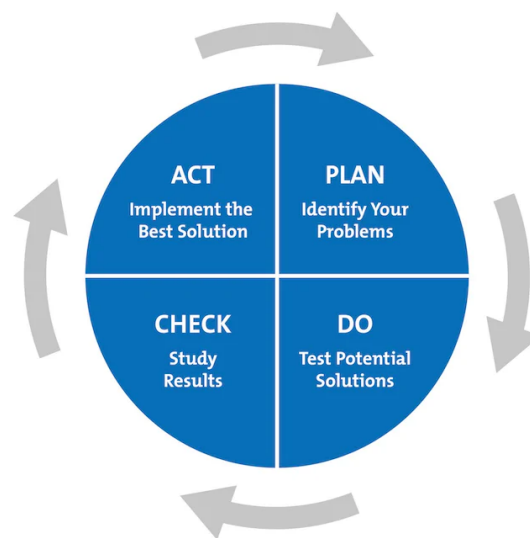


Fig 1: The Deming Cycle

Without a doubt, each of the designs, architecture, and metrics mentioned in the portfolio has gone through multiple reviews and iterations, with many drafts before

finalising one final answer. Where applicable, we will also discuss and add labelled diagrams of the previous prototypes which can help us understand the process of designing such a system.

With that said, here is a brief overview of the contribution of each member of the team. Please note that the contributions recorded in this portfolio are merely on sections where they led the discussion, as we made sure that every member contributed to at least some extent in each of the tasks so that we are aware of each choice and action that we have taken in this project.

- **Rahul Balaji (11449565)**

The Group representative. Lead the team in terms of defining the problems ahead and the appropriate actions to take. Enumerated and broke down the tasks ahead and moderated all discussions. Worked on the Security and Resilience design of the system, as well as on the use-misuse case final design, Played a role in designing the dashboard as well as a few security components like integrating SOAR and a few other components in the architecture.

- **Hemanth Sathyaseelan (11405780)**

Led the discussion on the use case topic, discussing the roles and responsibilities of each person involved in the system, along with how the system must be accessed. Designed the functions each actor on the system can call upon in order to trigger actions within the system through designing the activity diagram. Also took part in the design of the security dashboard.

- **Prabhjot Singh (11388349)**

Actively led the discussion on the Architecture of the system, where he suggested the approach of segregating the system by various layers of action instead of grouping them by government departments and the tasks they undertook, in addition to brainstorming the structure of the individual components and resilience measures with the team. Also led the discussion on designing the dashboard component.

- Rushil Shekhar (11358084)

Led the discussion on the use-misuse cases for the system, as well as expanding upon the threat actors and motives for the system. Also played a major part in defining the actions that can be taken to break the system in terms of physical endpoint components. Designed the security dashboard and defined the functions of the components.

- Sri Venkata Satya Sai Pawan Kartik Chitrapu (11413021)

He led the team on the activity diagram as well as the discussion in the balanced scorecard for the system performance along with metrics analysis. Furthermore, he focused on the system's security measures along with targets and tolerance for each measure. In addition to that, he played an integral role in designing and defining the system dashboard and RACI matrix.

- Hanwen He (11414209)

Led the discussion on the test plan and wrote the final test plan of the system. Defined the system's functional and non-functional requirements and wrote the use case and misuse case scenarios used in the use-misuse case final design. Also played an integral role in the discussion of deciding the database access order.

- Miguel Ricardo Lladó Herrera (11372444)

Led the discussion on the scorecard of the system, as well as the database access order, which is the order in which we try and access the offender's public records in order to identify the person. Also played a significant role in the activity diagram discussion.

Finally, we would also like to thank Professor Daniel Dresner and Professor Youcheng Sun, for providing us with the opportunity to connect and learn from them as well as from various experts in the field, which has been the guiding compass for the approach we have taken to this module as a whole.

The following pages will now guide you through a series of deliverables specified in the coursework handbook with detailed explanations of the decisions taken in terms of the design of the system along with justification.

Roles and Responsibilities

In the following section, we will discuss the roles and responsibilities of the system, the stakeholders, and all the other actors/people who play a part in this system, from law enforcers that avail this service, as well as the offenders who break the traffic laws that trigger this system.

The DIAMOND system proposed by the group is used within and amongst the government agencies and law enforcement themselves, for the welfare of the general public, keeping sensitive and private information out of reach of any third-party individuals or groups. As it is a government-owned software, it does not apply to the same rules as third-party applications that request government data, which is subject to a lot more analysis and scrutiny and also must comply to delete any information received after a particular period of time. However, as this section mainly deals with the actors of the system, we will discuss compliance in a later section in the portfolio.

Functional And Non-Functional Requirements

Before defining who uses the system, who its customers will be or who owns it, the first question that we asked ourselves was “What are our overall expectations of the D.I.A.M.O.N.D system?”. Thus, defining the functional and non-functional requirements helped us form a proper idea of the users, customers, owners and the use-misuse case diagram.

Functional Requirements

Biometric Analysis

The DIAMOND System should automatically bio-analyze the driver's photo captured by the acquisition camera and extract his/her facial features.

- The system must automatically process the driver's image in real-time.
- Must extract and store biometric features accurately.

Record Search and Image Comparison

The DIAMOND System should be able to identify drivers efficiently and accurately using multiple databases and the likeness of the driver created by DMNLBIT.

- The system should perform the efficient and precise matching of driver images against a database.
- Uses DMNLBIT for image comparison to confirm the driver's identity.

Report generation

The system should automatically record the detailed information of the offence, generate a traffic violation report and send it to the local authorities.

- Auto-compile detailed reports on traffic violations.
- Automatically send reports to appropriate local authorities.

Report Review and Notification

The system needs to be able to allow authorities and police officers to review reports of violations and send legal notices to offenders.

- Interface for authorities to review and notate reports.
- System to facilitate the sending of notices to offenders.

Handle violations

The system should be able to allow the police to go through the previous offence records of the offender and enable them to take further legally enforceable actions such as remote engine shutdowns.

- Provide access to offenders' historical records.
- Enable authorities to take necessary actions based on records.

Record management

- The system should enable law enforcement and traffic management internal staff to manage traffic offences

Non-Functional Requirements

Reliability

- The system must operate reliably, with minimal downtime and accurate identification processes

Security and Data Integrity

- The system should safeguard sensitive data against unauthorised access and breaches. And ensuring the accuracy and consistency of the violation and driver data throughout its lifecycle

Compliance

- The system must comply with legal and regulatory standards regarding data protection and privacy, such as GDPR

Auditability

- The system should have comprehensive logging for all transactions to support audits and investigations

Scalability

- The system should be capable of handling increasing amounts of data and users as the number of vehicles and drivers grows.

Maintainability

- The system should be easy to update and maintain, with clear documentation for any changes or upgrades.

Users

The first question, though obvious, that we put forward when we started to design the system was:

- 1) Who will be using this?
- 2) For what purpose would they want to use it? i.e. what is their objective to use this system?

The Users of the DIAMOND system are the law-enforcement agencies - in this case, the Police. The system is also used by law-enforcement personnel to identify and penalise speed limit perpetrators that get tagged by various equipment such as speed cameras or Automatic Number Plate Recognition (ANPR) sensors. Access to the DIAMOND system is given solely to the law-enforcement agency, and no other outside party has the ability to utilise the system. Although the users are now defined for the system, that does not entail all the people who interact with it. After all, it is important to define and categorise every person that can trigger any action of the system, which brings us to the external “actors” of the system. They can further be classified into the customers and the owners of the system.

Customers

When speaking about customers for a product, they comprise the individuals or entities that derive some sort of benefit from the given product.

In the case of the DIAMOND system, we can consider the customers to be the general public. The perpetrators are identified using their licence plate information, or their personal information such as their driver's licence, passport data, or biometric residence permit information. In some cases the drivers in question are also identified and verified using a machine learning model called “Does My Nose Look Big In This” (DMNLBIT), which uses social media photos to develop an image of the driver.

Ultimately the system is employed to enforce road rules and regulations, apprehending offenders with the overarching goal of ensuring the safety of roadways and the citizens who utilise them.

Owners

Finally, when referring to the owners, we mean the individuals or entities that own, maintain, and control the given system.

In this scenario, the ownership and control of all sensitive information used in the system lies with the government entities and does not provide access to any third-party individuals or collective entities. Even among the different government entities that make up the system's crucial components, the information from one governing body is kept abstracted from the others. There is a separation of duty and responsibility that is maintained within the system in order to prevent any abuse of authority.

Each agency has exclusive access to information pertaining to its own functions and nothing more. The DIAMOND system ensures that every cross-verification activity or conclusive operation is done locally within each governing system, and only the conclusive result generated by the DIAMOND system is used for further decisions or analysis.

Here we can see the various governing bodies involved in the ownership of the system:

- Identity and Passport Office - maintains the datastore of passport information of all individuals residing in the country.
- Driver and Vehicle Licensing Agency (DVLA) - maintains over 50 million driver records, their licence data, and over 40 million registered vehicles, including vehicle licence plate information.
- Home Office - Maintains the biometric data of foreign nationals currently residing in the UK.
- National Police Department - Maintains the Police National Database that holds the offence records and evidence records.

Initial Use and Misuse Case Diagrams

During the initial stages of the system planning, the use case diagram was rapidly prototyped as a simple base that could be expanded upon further, ultimately accommodating greater complexity. This initial use case diagram was developed with the intention of gaining a basic understanding of how the system works and its basic functionality.

In this initial diagram, the police can access the system by logging into the DIAMOND system using a single sign-on. Once the police are signed into the system, they can access the Police National Database, and view the number plate details of a particular car by requesting information from the DVLA. They can also request for passport information from the Home Office to verify the identity of the driver. It is also essential for the police to be able to cross-verify the details of a citizen using their ID and their passport.

The DMNLBT is also listed as an actor in this initial plan. In this way, it is given a function call which verifies the face of the driver by constructing a representational build of the face using the images which can be pulled from social media sites.

Once the police identify the assailant, the local authority in charge issues speeding tickets and the driver who was speeding receives it.

The initial use case diagram is given in Fig 2.

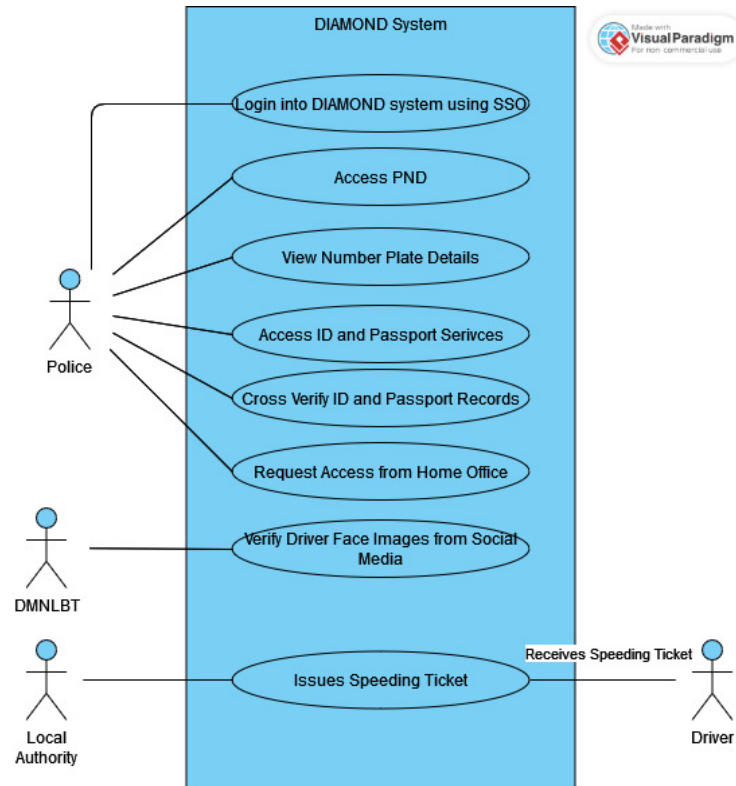


Fig 2: Prototype use-case diagram

On building further on the use-case diagram and adding an attacker for consideration in the misuse cases. It can be seen that the attacker can use fake login credentials to access and log into the DIAMOND system. The attacker can also flood social media websites with fake images of a person to get fake results for the DMNLBT system and make it less efficient in identifying and verifying the face of the driver. In simple terms, it can also be said that using a Man In The Middle Attack the attacker can issue speeding tickets to innocent citizens and change tickets which were originally issued by the local issuing authority.

Using these functions and concepts some of the misuse cases were added to the original use case diagram which can be seen in Fig 3.

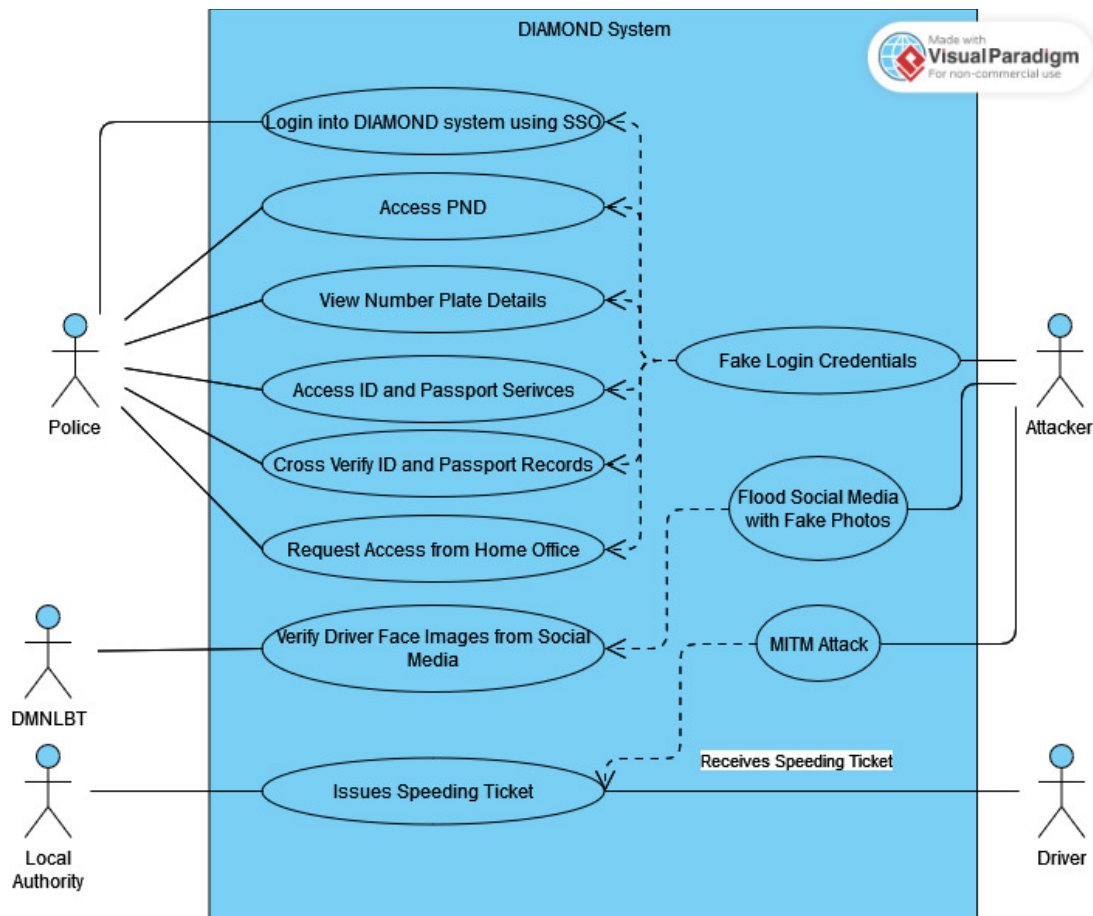


Fig 3: Prototype use-misuse-case diagram

Final Use and Misuse Case Diagram

Using the shown initial use and misuse case diagram, a more refined and complex version of the diagram was developed. In the new model, a more in-depth look at the functions was provided which would help anyone looking at the system for the first time to better understand and gain a deeper understanding of how the proposed system functions.

In the refined version of the model, particular use cases which trigger the function calls were added to the system. For example, when the offender over speeds, it triggers their picture to be captured by the speed cameras. Another example of this is the attacker performing a social engineering attack on the registered keeper to get the vehicle information.

In this version of the diagram, a data processing and analysis layer is created as an additional function is used for image comparison. Various data sources such as the biometric data from the foreign national database controlled by the home office, the passport information stored within the passport database and the registered keeper and vehicle information which is owned and controlled by the Driver and Vehicle Licensing Authority are all compared in this layer and the offender information is then processed and passed further to record the offence.

A concept which was particularly discussed amongst the group was the importance and the sensitivity of this data which was used within the DIAMOND system. Hence, the group decided collectively that no third party should have access to this information and this system was designed and developed to exist between all the various government agencies and as an additional system which co-exists and divides the system into more individual components for better debugging and security measures. The final use and misuse case diagrams for the proposed system which show all the owners, their functions and the various activities taking place within the system are in given Fig 4.

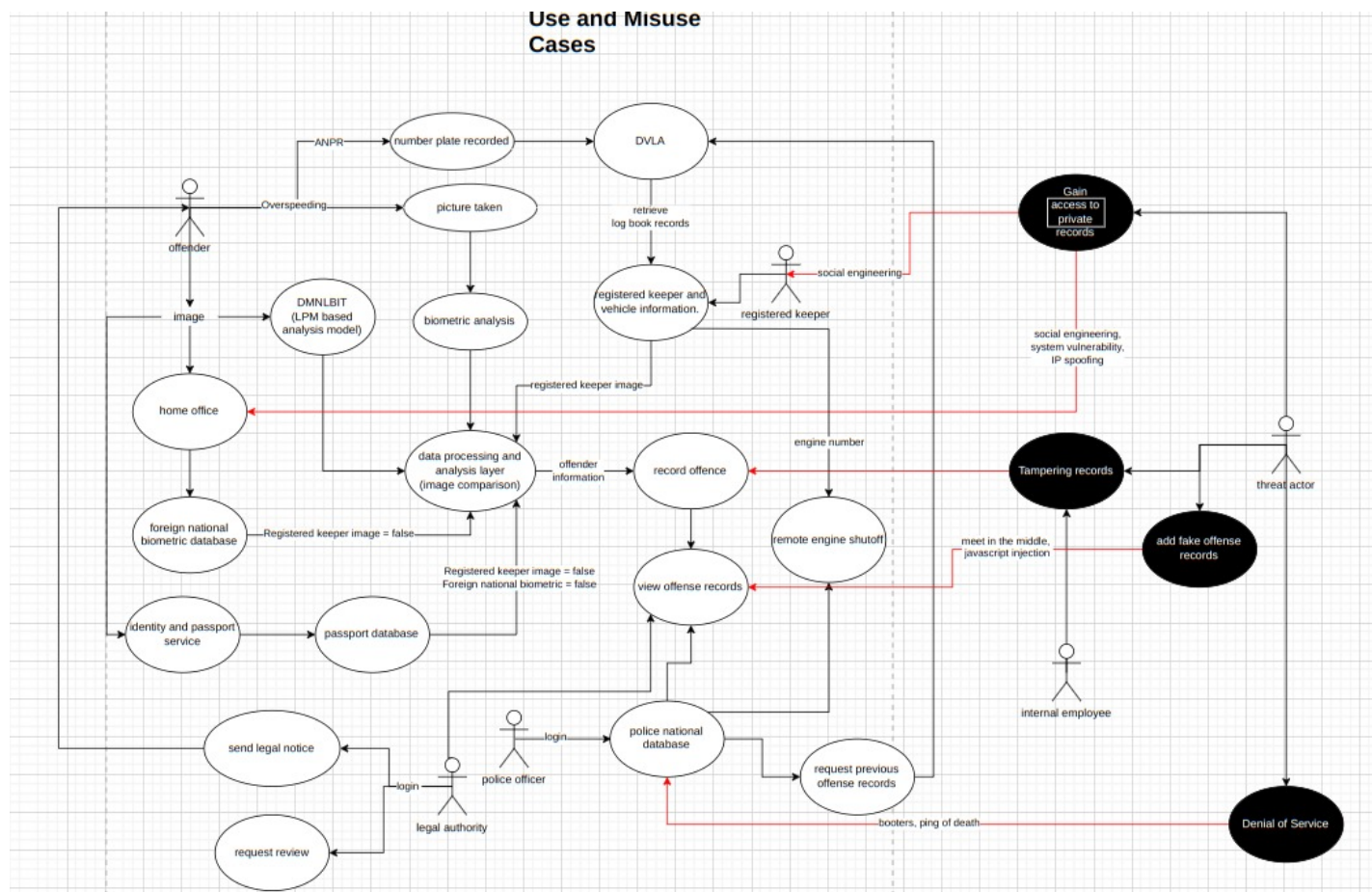


Fig 4: Use-Misuse Case Diagram

Some of the Use and Misuse scenarios as presented in the final diagram are given below.

Use Case Scenarios

- **Traffic Violation Detection - System, Driver:** Detecting and recording instances of traffic violations using automated camera systems.
- **Biometric Analysis - System:** Analyse the captured images and extract the biometric features.
- **Driver Identification - System, DMNLBIT:** Identifying the driver who committed the offence using image recognition and biometric analysis against multiple databases with the likeness of the driver created by AI (DMNLBIT).
- **Violation report generation (system) and review by local authorities (Local authorities):** The report will be sent to the local authorities and reviewed before issuing speeding tickets.
- **Offence Record Creation:** Creating a record of the offence, including time, location, type of violation, and the identified driver.
- **Notification Issuance (System issue to car owner):** Sending notifications to the offending driver or the registered vehicle owner regarding the violation.
- **Data Management (Administrator):** Securely managing and storing all data related to traffic violations and driver identifications

Misuse case Scenarios

- **Stolen data - Hacker :** A hacker gains unauthorised access to data by exploiting a system security vulnerability. The hacker downloads a database containing personal biometric data and sells this information to a third party.
- **Records and Reports Tampering - Internal Staff:** Some internal staff illegally modified reports and driver and vehicle information in the system.
- **Exploit system vulnerability - Hacker:** An attacker discovers a technical vulnerability in the DIAMOND system's software and exploits it to gain unauthorised access. This could involve bypassing security mechanisms to alter




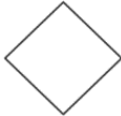

traffic violation records, inject malicious code, or disrupt the system's operations. The attacker's goal could be to erase evidence of traffic violations, insert fraudulent data, or compromise system integrity for further malicious activities such as launching a Denial of Service (DoS) attack to disable the system's functionality.

- **Man in the middle attack(MITM Attack) - Hacker:** Hackers use man-in-the-middle attacks to send fake reports to authorities.
- **Sensitive information leaked - Employees/Internal staff:** Employees do not receive adequate training and inadvertently disclose sensitive information in the database

General Activity Diagram

A general activity diagram was created to show the general flow of the system and how various decision points affect the state generated by the system and the end result.

The legend for activity diagram is as follows.

Symbol	Description
	Start Node
	Action State
	Control Flow
	Decision Node
	End State

The activity diagram for the proposed system was created as shown in fig 5

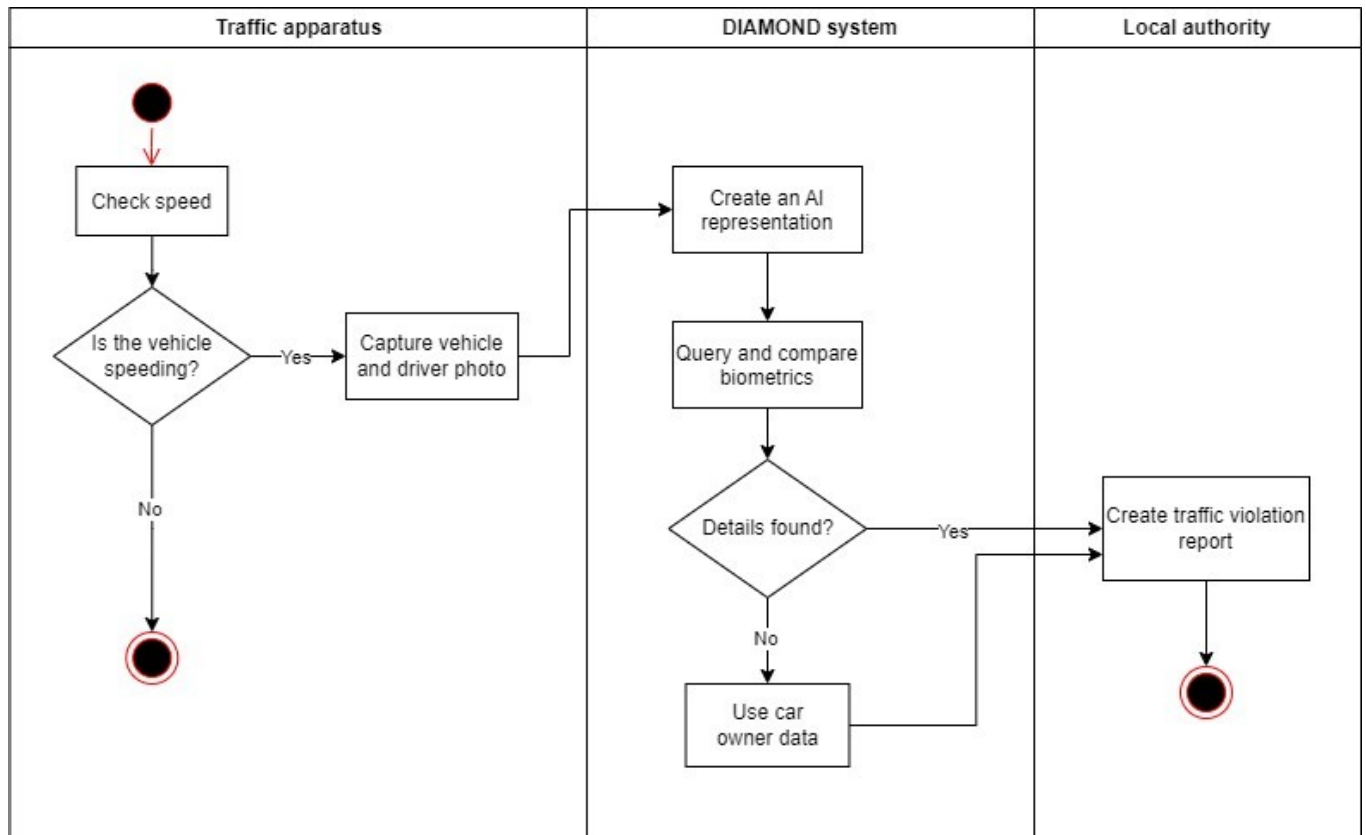


Fig 5: General Activity Diagram

The diagram outlines an integrated approach to traffic management involving three primary entities: the traffic apparatus, the DIAMOND system, and the Local Authority. The traffic apparatus serves as the initial point of contact in the process, equipped with speed detection technology to monitor vehicles. Upon identifying a vehicle exceeding the speed limit, the apparatus automatically captures photographic evidence of the incident, including images of the vehicle and the driver.

The DIAMOND system is an advanced technological proposal that processes these images. Utilising artificial intelligence, it constructs a digital avatar or representation of the driver for the purpose of authentication. The system then executes a biometric comparison against a stored database. If a match is found, confirming the identity of the driver, the DIAMOND system compiles this information and forwards it to the Local Authority.

The Local Authority is the final component in this process. It is responsible for generating an official document, known as a traffic violation report, based on the verified

information provided by the DIAMOND system. This report is crucial as it forms the basis for issuing a ticket to the offender for the speeding violation.

In the event that the DIAMOND system is unable to find a match for the driver's biometric details, the process does not stall. Instead, it utilises the vehicle's registration number to trace the owner's identity through the DVLA (Driver and Vehicle Licensing Agency) records. The resulting information obtained is then employed to prepare the traffic violation report, which is linked directly to the vehicle's licence plate rather than the individual driver.

To further elaborate on the system's functionality, a supplementary activity diagram was developed. This additional diagram serves to clarify the data flow between the involved organisations and the DIAMOND system. It illustrates the sequence of actions, decision points, and communication pathways that enable the seamless transition of data from the moment a traffic violation is detected to the issuance of a speeding ticket.

The comparison process in the activity diagram is shown in the diagram given below:

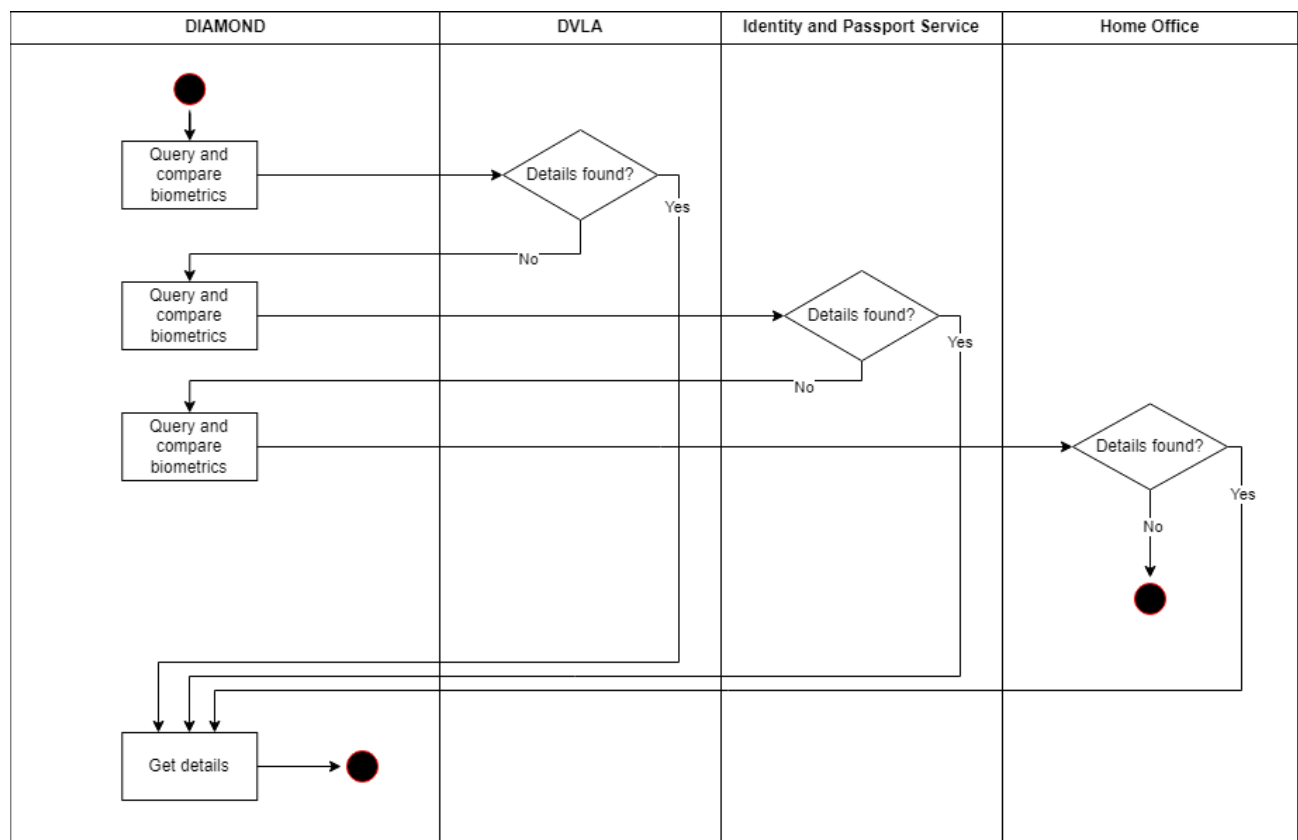


Fig 6: Comparison process in activity diagram

The DIAMOND system initiates its search for driver details by querying the DVLA database. If the required details are found within the DVLA's records, the system captures this information. Should the search come up empty, DIAMOND doesn't stop there; it cycles back to initiate a new search, this time reaching out to the Identity and Passport Service. The process repeats as necessary, with DIAMOND querying the Identity and Passport Service's records for the needed details.

In the event that the Identity and Passport Service does not hold the relevant information, the DIAMOND system extends its search to the Home Office's databases. At each of these stages, if the DIAMOND system successfully finds the details it's searching for, it proceeds to store the data and subsequently forwards it to the Local Authority. The Local Authority is tasked with utilising this data to compile traffic violation reports and issue speeding tickets.

The various government organisations and the data which they allow for use in the DIAMOND system are the following:

- Driver And Vehicle Licensing Agency : Stores information about the driver's licence and also the information regarding the information about the vehicles licence plates. The DVLA also contains the registered keeper information.
- Identity and Passport Services : Stores passport information and also other identity documents of the citizens which are of sensitive nature.
- Home Office : Stores the information in the Foreign National Database which contains the information of foreign nationals currently living in the country.
- Police National Database : The PND allows the police to view offence records and also request previous offence records from the DVLA.

RACI matrix

The RACI matrix is used when multiple entities are involved to define and delegate duties clearly and to specify the responsibility boundaries between each entity. This helps in preventing duplicating or overlapping of tasks and ensures that the duties are distributed appropriately and optimally. The key components of the matrix are:

- Responsibility (R)

These entities are responsible for carrying out the designated tasks. They may, however, choose to involve other entities when finishing the tasks.

- Accountability (A)

This entity may not directly carry out the tasks but is answerable for the outcome. They ensure that the work is being carried out and are responsible for handing over the task to an appropriate entity.

- Consulted (C)

This entity acts as the subject expert and is consulted when a task is being carried out. It may be consulted by either the entity accountable for the task or the entity carrying it out.

- Informed (I)

This entity is kept informed of the progress made at an overview level and is usually a one-way communication.

In the DIAMOND system, the following entities and stakeholders are involved:

- Government,
- IT Team,
- System operators (usually law enforcement officers and bureaucrats),
- The University of Brigadoon, and,
- Drivers and traffic violators.

The RACI matrix attempts to define the duties and responsibilities of the above entities in the traffic violator identification process.

	Government	IT Team	System Operators (law enforcement officers)	Local law enforcement authority	University of Brigadoon	Drivers and traffic violators
Designing administrative policies for DIAMOND	R, A	-	C, I	I	-	-
Designing the AI model	-	-	-	-	R, A	-

	Gover nment	IT Tea m	System Operators (law enforcement officers)	Local law enforceme nt authority	University of Brigadoon	Drivers and traffic violators
Designing and engineering DIAMOND	I	R, A	C	-	-	-
Maintaining DIAMOND	I	R, C	C	-	-	-
Evaluating/Tes ting DIAMOND	I	R, A	C	-	-	-
Violation Identification	-	-	R, A	C	-	I
Violation Reporting	-	-	R	A, C, I	-	I
Violation Investigation	-	-	I	R, A		I
Compliance and law enforcement	I	-	I	R, A	-	I

- Designing administrative policies for DIAMOND

Designing the administrative policies on how to effectively utilise the DIAMOND system to improve traffic policing is the primary responsibility of the government. It is also the accountable entity as the policies and vision are set by it. DIAMOND's operators, usually government officers, are looped into this discussion and are consulted and kept informed.

- Designing the AI model

The AI model is primarily designed at The University of Brigadoon, which is solely responsible and accountable for it. No other stakeholders are involved in the development process. The government integrates it into its system as-it-is.

- Designing and engineering DIAMOND

Designing and engineering the system itself is a technical task and involves the IT team. The system's operators are consulted to ensure that feedback is received from operational and law enforcement perspectives. At the highest level, the government is kept informed of the progress, resources that are allocated, consumed, and the budget.

- Maintaining DIAMOND

The system is primarily maintained by the IT team. Designated experts within the team are consulted to ensure that the system performs at optimal levels and is properly maintained. The government is kept informed of the system's state at all times. System operators may be consulted for feedback or other opinions when carrying out maintenance tasks.

- Evaluating/Testing DIAMOND

The system is primarily evaluated and its operational status is tested by the IT team with consultation from IT experts. The government is kept informed of the evaluation and testing results to ensure that it can frame its administrative policies as required. Since the system is operated by the operators, they are consulted for their feedback on the system's ease of use, accuracy, performance, and other metrics.

- Violation Identification

The system's operators are primarily responsible for identifying violations and tracking the violators. Local law enforcement authorities may be consulted in this process. The driver/violator may be contacted once identified.

- Violation Reporting

Once the identification process is complete, the violation is then reported to the local authority. Since the required information is passed on to them,

they're accountable and answerable for the incident's further progress. Since they're the point of contact, they may be contacted during this process. The violator is kept informed about the incident/case progress.

- Violation Investigation

At this point, the local authority has taken over the incident and is responsible and accountable for wrapping up the formalities. The system's operators and the violators, both, are kept informed about the progress as deemed necessary.

- Compliance and law enforcement

The government is kept informed about traffic policy enforcement to ensure its policies are shaped correctly. Since the local authority is responsible for filing the traffic violation at this point, they are responsible and accountable for this process. The driver/violator is kept informed and may be summoned when required.

Architecture Schematics

The architecture for the D.I.A.M.O.N.D system has been designed on a complex, multi-layered framework that has been designed to handle cases of public driving misconduct in an effective manner. This section of the report extensively goes into detail about the comprehensive schematics of the system, which also puts into perspective the intricate interplay of the data collection, processing, storage, compliance, security, as well as resilience measures that have been put into place to ensure that we have a robust and resilient system in place.

Overview of the System

Talking about the general overview of the system, as is evident by the schematic, the system has been structured into different layers depending on the set of functions that are performed by individual components of the system, in contrast to structuring the system in a way that each governmental organisation gets its own individual layer, which was deemed inefficient and non-resilient, with concerns being raised about Trust and compliance pertaining to the handling of the data in an off-premises environment.

The structure proposed to replace the separation by departments is classified as below.

- 1) Data Collection Layer
- 2) Data Processing and Analysis Layer
- 3) Data Integration Middleware
- 4) Security and Monitoring Layer
- 5) Reporting and Compliance Layer
- 6) Data Storage Layer
- 7) Web Application Layer
- 8) Backup and Recovery Systems

The following Layers are then interconnected to each other with firewalls and load balancers to allow the exchange of data in a secure and fail-safe manner. Below is a diagram of the overall architecture of the system.

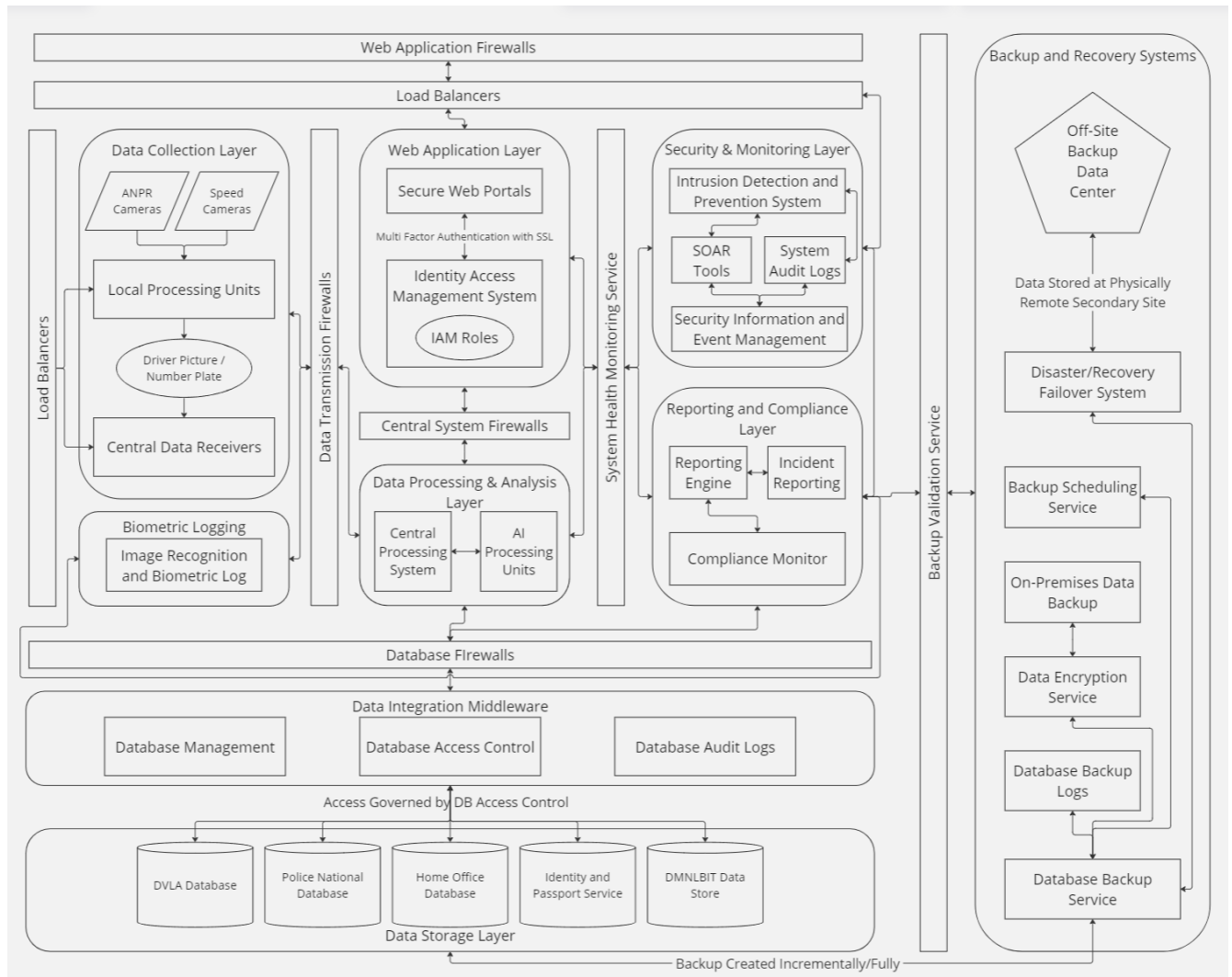


Fig 7: Architecture of D.I.A.M.O.N.D

Let us now take a look at the individual Layers of the system and discuss the function of each, and their subcomponents.

Data Collection Layer:

As the name suggests, this Layer deals with the collection of data from all the physical endpoints present in the system. The ANPR cameras and the speed cameras cannot just be directly connected to the network and given access to the databases for storage due to the concern of the attacker gaining access to the rest of the network even if they hack one of the data capturing endpoints. It is imperative that we treat those endpoints with caution and less trust than internal databases, as it is essentially in a “demilitarised zone” of the network.

The endpoints are connected to local processing units and then to central data receivers. The local processing units scan the data collected and transform it into a readable format by the system, and then write it to the central data receivers which in return collect data from all the endpoints present and then transfer it to the data processing and analysis layer.

Data Processing and Analysis Layer:

The Data processing and Analysis Layer deals with the decision-making role of the system. It decides if the offender identified matches with the identification from the other sources and gives the final verdict of the offence. It is the central unit that is connected to the web application layer for display, as well as the data integration middleware to gather and transfer data. It is also connected to the system health monitor so that both the security and the compliance layers can actually monitor the activities of the central processing unit.

Database Integration Middleware:

The Database Integration Middleware is concerned with three main operations in the system.

- 1) To read/write data to the databases, taken care of by the database management component.
- 2) To record the access requests as a log for audits which is handled by the audit log component.
- 3) To restrict/grant access to data via an API depending on requests from various components in the system, which is implemented by the database access control.

Data Storage Layer:

The layer where all the data is segregated, stored in different databases and then retrieved for use later when required. Since this layer deals with personally identifiable information (PII) and sensitive personally identifiable information (SPII), heavy restrictions must be placed on what modules can access this layer directly. In this design, only the database integration middleware and the backup and recovery system can interact with the data storage layer.

Security and Monitoring Layer:

This layer deals with the overall monitoring of the system activity, ever vigilant for any suspicious requests or actions. It is connected to the load balancers and the firewalls to monitor their activity and can be configured dynamically as required using the SOAR (security orchestration automation and response) tools available in the market, which can automatically launch scripts and simple commands to automatically respond to simple attacks when they are detected by the intrusion detection systems or the SIEM (security information and event management) tools. This component makes up the majority of the dashboard that can be viewed by the cybersecurity team. The other component that is also a part of the dashboard is the reporting and compliance layer.

Reporting and Compliance Layer:

The reporting and compliance layer deals with all the rules, laws and regulations the system must comply, or meet with in order to maintain the public's data in a secure manner and thereby gain public trust in using their data ethically.

This system mainly has components that deal with recording the offence reports with the reporting system and the compliance monitor ensures that the reports written and the data handled by the system are compliant with the laws regarding data handling such as the GDPR (General Data Protection Regulation).

Web Application Layer:

This is the topmost layer of the system, which consists of the user interface that is used to interact with the overall system by all users. The access to the web application layer is further secured by using multi-factor authentication to devalue passwords. The identity access management system assigns the role to the user based on which the data they view and the actions they can perform change, ensuring separation of duties and abstraction of information. The secure web portals allow the user to log in and authenticate their session on the system.

Backup and Recovery systems:

This component is crucial for the integrity and resilience of the entire system. It is mainly concerned with ensuring that all the data within the system is regularly backed up and can be quickly recovered in the event of data loss or a system failure. The backup and recovery systems are designed to handle several key functions:

- **Off-Site Backup:** Data is replicated and stored securely at a physically remote location, which provides protection against site-specific disasters such as fires or floods.
- **Disaster Recovery Failover System:** In case the primary system goes down, the failover system ensures that operations can continue with minimal disruption by switching to a backup system.
- **Backup Scheduling Service:** This service automates the process of backing up data at regular intervals, ensuring that the most recent data is always available.
- **On-Premises Data Backup:** For added security and faster recovery times, a copy of the data is kept on-site.
- **Data Encryption Service:** To protect the data's confidentiality, both in transit and at rest, encryption services are employed.

- **Database Backup Logs:** This function keeps detailed records of all backup activities, providing an audit trail that can be reviewed for security and compliance purposes.
- **Database Backup Service:** This service manages the backup of database contents, ensuring that all data is duplicated and preserved according to the backup policy.

The Backup and Recovery Systems work in conjunction with the Database Integration Middleware and the Data Storage Layer, providing a comprehensive strategy for data preservation and disaster recovery. This multi-faceted approach guarantees that the system can withstand and recover from a variety of potential threats, securing the continuity of operations and safeguarding sensitive information.

Security and Resilience in the D.I.A.M.O.N.D System: A Comprehensive Approach

The D.I.A.M.O.N.D system, designed for monitoring and reporting offences, due to the nature of its work, requires robust security and resilience measures to protect sensitive data and ensure uninterrupted service. Here, we delve deeper into these measures, covering data protection, system security protocols, and more.

Data Protection and Privacy Compliance

For the purposes of the D.I.A.M.O.N.D System, the focus on Data Protection and Privacy Compliance is critical given the inherent nature of the data and to maintain a Chain of Custody.

As such, the system in place here is in complete adherence to the General Data Protection Regulation (GDPR), and measures to incorporate consent mechanisms, purpose limitation, principles of least privilege, and data minimization to prevent any misuse of data have been taken in the same direction.

To quote an example, at points where biometric data is to be processed, consent is explicitly from the user, which ensures the ethical use of data and ensures compliance.

In addition to this clear transparency in data handling towards users, each data processing activity is documented properly and logged to ensure that any action performed on the data can be traced back as per the need of the hour.

Biometric Data Security

Biometric Data is a central and important part of the DIAMOND system and hence its security and access are of paramount importance. To make sure that Biometric data cannot be forged, access to the system is regulated through a role-based control system. This ensures that only authorised personnel can access the stored biometric information, hence minimising the chance that a foreign entity might be able to replicate or forge the information contained in these systems.

All of this is done through a combination of different mechanisms at each step of the process:

- **Collection and Transmission Security:** In the data collection stage of the D.I.A.M.O.N.D system's operations, the captured biometric identifiers, such as fingerprints and facial likeness, are subject to stringent cryptographic measures. Utilising state-of-the-art encryption protocols, the data is rendered unusable to third-party interceptors during transit, thereby preserving the confidentiality of the sensitive information at hand.
- **Storage and Encryption:** Once it has been transmitted to the central data receivers, the system's biometric data needs to be encrypted once again for static defence, which is also commonly referred to as encryption at rest, which is going to be facilitated by algorithms like AES-256. This ensures that stored data is safeguarded against unauthorised access and preserves the biometric details of the individual.
- **Access Control:** As we progress to the analysis phase, the system incorporates a robust Identity Access Management (IAM) framework. This mechanism specifies precise roles and privileges, ensuring that any access to the biometric data in question is reserved only for authorised personnel whose roles necessitate such interaction. This upholds the principle of least privilege and

successfully mitigates the risk of internal misuse.

- **Audit Logs and Security Monitoring:** The architecture design also includes database audit logs and security monitoring layers. These components of the system are crucial to the system in order to keep detailed logs of who accesses biometric data and when. This is done because such logs can help identify any unauthorised access attempts or policy violations whenever an audit is done on the system.
- **Compliance and Reporting Layer:** Referring to the architecture in question, the reporting and compliance layer that has been put in place ensures that biometric data handling complies with legal requirements, such as GDPR, and that any breaches are promptly reported.

System Security Protocols for Data Integrity and Protection

This section highlights the various security protocols that have been implemented in the DIAMOND System to ensure the protection as well as the integrity of the data as it flows through the system. It also highlights the protocols in place to prevent malicious attacks at points that are prone to attacks.

- **Web Application Firewalls:** Firewalls have been configured at the web application layer to monitor all the HTTP traffic that comes in through the outward-facing web portal and block any malicious traffic that might try to exploit vulnerabilities in the web application.
- **Central System Firewalls:** A part of the Data Processing and Analysis Layer, these firewalls protect the central system and act as a barrier between trusted and potentially untrusted systems, only allowing traffic based on predefined rules ensuring the security of the system.
- **Data Transmission and Database Firewalls:** Data Transmission firewalls are specifically designed to secure the data as it is transmitted across different components of the system, preventing unauthorised access or malicious manipulation of the data.
Database firewalls are also configured adjacent to the database layer to help protect the system against attacks on database servers or other code injection attacks such as SQL injection.

- **Identity Access Management:** Implementation of IAM policies allows us to define different users and roles within the system and to allow them to access specific aspects at certain levels within the system. A good implementation of these roles is crucial in ensuring that only the authorised personnel are able to access the right resources at the right time.
- **Multi-Factor Authentication with SSL:** A common practice in today's computing world, MFA with SSL has been implemented at the web application layer to bolster the security of the system. This layer facilitates additional security by requiring the user to authenticate themselves by using multiple factors, such as biometric information or by using codes generated using Multi-Factor Authentication apps. This is further secured using the Secure Sockets Layer or SSL for encryption during the transmission of data.

Intrusion Detection Systems and Security Audits

As is the case with even the most secure systems, in case an intruder does get access to some parts of the system, an Intrusion Detection and Prevention System is crucial to protect the system from further tampering and damage. An IDPS system constantly monitors the network and the system for suspicious and malicious activities and detects any violations in policies that have been set by the administrators. The system takes measures to block these suspicious activities and alerts the system administrators of the same.

We use strategically placed Network-Based IDPS systems for monitoring the traffic on the network and Host-Based IDPS systems for monitoring the individual components of the system. The combination of these two allows us to monitor the traffic and detect intrusions throughout the entirety of the system.

In addition to this, Security Audits are a big part of the DIAMOND system as they would be conducted at multiple points throughout the year and also done externally annually. By putting the DIAMOND system through penetration testing and other checks such as code reviews, we can identify the vulnerabilities within the system that need to be patched or issues that need to be addressed. Prompt action on these vulnerabilities is also a big part of maintaining the security of the system.

Resilience Measures against Cyber Threats

Because of the nature of work that the DIAMOND system is used for, it is crucial that it is resilient against most cyber threats so as to not hamper its integrity as well as the availability of the system. As such, we have developed a multifaceted approach that allows the DIAMOND system to be resilient against cyber threats that would otherwise cause extensive harm to the system:

- **Rate Limiting Measures:** As there is always a possibility that an attacker might try to take over a system using brute force, we have considered rate-limiting measures as a way to make sure that the system cannot be hijacked by a user making too many requests within a short period of time, thus mitigating any disruption to services in the DIAMOND system and bolstering the system against brute force attacks. This has been implemented using Load balancers. During the discussion period, the suggestion was made to also include the “Recaptcha” code system, but was ultimately rejected as it was not feasible to have a user do a captcha to prove he is not a bot for every request as they process hundreds of traffic offences every day.
- **Implementation of Content Delivery Networks:** In cases where an attacker might try to attack the system using a DDoS attack to deny services to the authorised personnel, CDNs can enhance the resilience of the system, as they control the system’s ability to handle large requests and distribute loads across the network, making it largely unfeasible for DDoS attacks to succeed.
- **Security Information and Event Management (SIEM) Tools:** A useful tool in every cybersecurity expert’s arsenal, SIEM tools have been considered and implemented in the architecture design to make sure that any security alerts generated by the system are analysed in real-time. By analysing these events, SIEM tools allow immediate detection of security incidents, further allowing the administration to act on them.
- **Security Orchestration, Automation, and Response (SOAR) Tools:** A further complement to the SIEM tools, SOAR Tools allow us to formulate workflows and create automated responses to these security incidents. Integrating with the SIEM tools, SOAR can handle security incidents automatically and without any delay. In time-sensitive situations, this can be the difference between a resilient and a non-resilient system as no human interaction is required.

- **Zero Trust Design:** The separation of the various components of the system and providing each function access only to layers and data on the network that is necessary for them to carry out their tasks is a principle that has been derived from the zero trust framework that has been the recent industrial standard. This architecture implements the principle of least privilege in the system.

Data Backups and Disaster Recovery

Disaster recovery makes up a big chunk of the entire system design as there is always a possibility, no matter how small, that the system might not be able to sustain itself against an attack. In such cases, if the data is destroyed or loses its integrity, it is crucial to have data backups and disaster recovery systems in place in order to be able to bounce back from the security incident in the shortest amount of time possible.

As such, the system includes a proper implementation of backups, including full backups, as well as incremental backups, which carry the information that has been changed since the last backup at a lower cost.

In addition to this, the presence of both on-premises and off-site backups provides a level of resilience that is extremely hard to get past. On-premises backups allow the system to bounce back from minor cyber incidents, while in case of complete data loss, off-site backup provides a slower yet more reliable data storage where the data might be stored on the cloud or in the form of physical media, away from the system premises. This ensures data availability at all levels, no matter the damage caused by the cyber incident.

In addition to this, the backup procedures are regularly tested to make sure that the data integrity as well as the recovery protocols are in order and compliant. This is done to make sure that the system is effective and allows fast recovery with minimal downtime for the system.

Physical Security Measures

In addition to all the security measures highlighted so far, the implementation of physical security measures is highly important in the overall security of any system as social engineering attacks and physical disasters are one of the leading causes of cyber incidents. Hence, it is important to have defences that protect the physical infrastructure that hosts the entire system. A few proposed measures are:

- **Access Restriction for Data Centers:** Any access to the servers that house the data for the system is strictly controlled and governed by policies that ensure only authorised personnel are given access. This is done by the use of identity verification and authorization methods that include but are not restricted to ID Access Cards, Biometric Scanning, and physical checkpoints that are governed by trained guards.
- **Climate Controls and Mitigation Measures:** In addition to human interference, data systems are prone to environmental risks such as fires and high humidity. To ensure protection against such risk factors, climate control systems are installed inside data centres to ensure that heat levels and moisture levels in the air remain conducive to the optimal health of the systems. Further, mitigation measures such as fire suppression systems must be installed to respond in case of accidental fires.
- **Security Personnel and Surveillance:** Central to the security of any system, on-site security personnel are instated and are responsible for the security and surveillance of the physical infrastructure for the DIAMOND system. Using CCTV surveillance, regular patrols, and conducting security checks, these personnel ensure complete security at the physical data centres. In times of crisis, they provide an immediate emergency response and act to protect the systems from damage.
- **Physically Resilient Infrastructure:** To make sure there are no interruptions or loss of data or damage to the infrastructure, a number of physical resilience measures such as backup generators and natural disaster resilient data centre buildings are taken into consideration. These ensure that the system is safe from unprecedented natural disasters as well as power shortages.

These physical security measures are paramount to the actual existence of the entire system and make sure that the system is resilient towards physical damage and safe from human-induced physical damage.

Maintaining system Integrity and Reliability

- **System Updates:** This is Done by implementing regular patch management schedules and vulnerability scans. Updating system softwares regularly ensures that the overall system health is maintained, as patch updates include bugfixes and security updates.
- **System Audits:** Takes place periodically in terms of integrity checks and performance monitoring. Running regular checks on system configurations and logs ensures integrity, and monitoring system performance can make identifying potential issues related to security or system functionality easier.

Test Plan

Introduction

The DIAMOND System is an innovative solution designed to enhance traffic law enforcement through the integration of biometric technology and real-time data analysis. It aims to streamline the identification of drivers who commit traffic offences by automatically analysing photographic evidence and cross-referencing it with a vast array of databases.

Our test plan will ensure that the DIAMOND System meets high accuracy, safety, security, and operational efficiency standards. Through rigorous testing, we will validate the system's capabilities in facial recognition, data integrity, report generation, and the enforcement of legal measures. The overarching goal is to confirm that the system reliably supports traffic management while upholding the principles of public safety and legal compliance.

Test Objects

The primary goal of DIAMOND system testing is to ensure that the system is trustworthy:

- **Safety:** Verify that the system operates without causing any harmful states, ensuring the well-being of all users and stakeholders.
- **Reliability:** The system consistently performs its intended functions under specified conditions, delivering the required service accurately.
- **Availability:** The system is operational and accessible when needed, maintaining high uptime for critical functionalities.
- **Resilience:** The system exhibits robustness to disruptions and can quickly recover from any event or failure.
- **Security:** The system is protected against both accidental and deliberate threats, safeguarding sensitive data and operations.

Having established the primary goals of DIAMOND system testing, which focus on trustworthiness aspects like safety, reliability, availability, resilience, and security, it's

also crucial to extend our attention to other vital areas of system assessment. These include:

- Ensure the system under test conforms to functional and non-functional requirements
- Ensure the system meets the quality specifications defined by the client
- Ensure that the system and its associated resources are used in accordance with local laws, regulations, and policies
- Critical Bugs/issues should be identified and fixed before going live

Test Estimation

The Test Estimation section of the DIAMOND System Test Plan is designed to provide a comprehensive projection of the time, resources, and budget that will be required to thoroughly test the system's functionalities and non-functional aspects. This forecast not only aids in strategic planning and allocation of resources but also sets the stage for tracking progress and identifying potential bottlenecks. Our goal is to establish a realistic and flexible testing timeline that accommodates the complex nature of the DIAMOND System while maintaining a high standard of quality assurance.

Duration of Test

The initial estimation for the testing phase is X weeks from the commencement of the testing cycle, with a provision for a 2-week buffer in case of unforeseen delays. This timeframe will be determined based on the scope of the test, past experiences, and industry standards for systems of comparable complexity.

Resources

- A team of multiple test engineers with at least one senior test leader among them
- Access to necessary testing tools and allocation of hardware and network infrastructure for test environment setup

Cost

- Personnel costs based on the number of engineers and estimated hours
- Licensing fees for specialised testing tools and software.
- Operational costs for maintaining test environments.

Risk Factors

- Potential integration issues with external Databases.
- Unavailability of specialised testing tools or delays in procurement.
- Dependency on the completion of development phases for certain features.

Test Scope

The Test Scope section outlines the specific areas of the DIAMOND System that will be subjected to rigorous testing. This section defines what will be included and excluded in the testing process, ensuring that our focus remains on the most critical aspects of the system.

Inclusions

Critical functions of the system

Test that the main functions of the system are working in an optimal manner. This includes biometric analysis, recording of and image comparison, generation and dispatch of reports, etc.

Non-functional requirements of the system

Ensure that the system is trustworthy, even in the case of some unexpected events Including Reliability, Security and Data Integrity, Compliance, Auditability, Safety, and Resilience...

Exclusions

Resources and services for third-party integration, including testing and evaluation of AI models, hardware testing of data entry devices ANPR and cameras

Test Strategy

Unit Testing

Focus on individual modules or layers to verify their functionality.

Some automated unit testing frameworks like JUnit (for Java applications) or NUnit (for .NET applications) can be utilised. And Employ Test-Driven Development (TDD) practices where tests are written before the code.

Integration Testing

To ensure seamless collaboration and data transfer between different components and layers of the system.

Implement Continuous Integration (CI) systems, such as Git pipelines, to automate the building and testing of integrated code.

System Testing

Conduct comprehensive testing on the complete system to ensure all requirements are met.

Define test cases based on requirements and user stories. Use a combination of manual and automated tests to cover functional and non-functional aspects under varied conditions and loads

Security Testing

Implementing penetration tests and vulnerability scans to assess the system's defence mechanisms.

Static analysis tools and application security scanners like OWASP ZAP can be used to conduct automated vulnerability scans and supplement with manual penetration testing. Perform regular security audits and review codes for potential security issues.

Performance Testing

Assess system performance, focusing on response times, throughput, and stability under different loads.

Use tools like Apache JMeter or LoadRunner to simulate high loads and measure response times, throughput, and system behaviour under stress.

Usability Testing

Evaluate the system's user interface and user experience to ensure it is intuitive and user-friendly.

Conduct user testing sessions, gather feedback through surveys, and employ A/B testing to refine the user interface and experience.

Conformance Testing

To check adherence to legal and regulatory standards, particularly in data and privacy, such as GDPR.

Regularly review compliance with GDPR and other relevant standards. Schedule external audits if necessary to ensure adherence to legal requirements.

Regression Testing

Regularly re-test the system to ensure that new changes or updates have not adversely affected existing functionalities.

Implement automated regression testing using tools like Selenium to ensure new changes do not break existing functionalities. Run regression tests as part of the CI pipeline.

Acceptance Testing

Conduct final testing to ensure the system meets the end-users requirements and is ready for deployment.

Facilitate User Acceptance Testing (UAT) by providing end-users with test scenarios and gathering their feedback. Ensure that the final product meets the defined acceptance criteria.

Assignment of Responsibilities

The Assignment of Responsibilities section of the test plan defines the roles and responsibilities of each member of the test team. This includes designating who is responsible for each type of test, who will manage the test environment, and who will handle documentation and reporting.

Test Manager

- Oversees the overall testing process
- Ensures adherence to the test strategy and schedule.
- Responsible for communication with stakeholders and final approval of test results.

Test Engineers

- Execute and document specific tests (unit, integration, system)
- Identify and report bugs and issues

QA Analysts

- Ensure quality assurance and compliance with standards. McCall Software Quality Model introduced by James A. McCall in the 1970s can be used to model quality factors,
- Review test plans and cases for completeness

Security Analysts

- Focus on the security aspects, especially data protection in compliance with GDPR.
- Conduct penetration tests and security audits

Performance Analysts

- Test system performance under various traffic loads.
- Monitor and report on the system's scalability

UI/UX Designers

- Ensure the system's interface is user-friendly, especially for law enforcement officials.
- Conduct usability tests and gather feedback.

Developers

- Address and fix bugs identified during testing
- Implement features based on feedback from testing

Test Approach

The test cases set will be created for each tester using white-box and black-box testing methods. The tests will be executed in TestLog by a tester and each test case is marked as Pass / Fail. The tester should leave notes on actual results and any other relevant details when possible.

When test cases are marked as Fail, bug reports will automatically be created and assigned to a developer. The developer makes the change and returns it to the responsible tester. The test manager reviews the test report in the Test log for final approval.

In white-box testing, the quality team will compute cyclomatic complexity $V(G)$, which can be used to allocate test modules appropriately. The module whose value of $V(G)$ is more than 10 will be asked to be re-constructed by developers, and less experienced testers will test modules whose value of $V(G)$ is less than 5. The Modules whose value of $V(G)$ is less than 10 or more than 5 will be allocated to experienced testers. In black box testing, we will use some techniques like equivalence class partitioning and boundary value analysis.

For test cases, we design test cases based on focusing on the internal functionality of each layer of the system architecture and the interaction with other system layers or components, which are described in the following test case template.

Test Cases Design

For the design of test cases, we start from the test objectives to test the internal functionality of each layer and the interaction with other components or layers, as well as to further validate the resilience and security of the whole system. Below is our test case template.

Test Cases Template

Project Name: <DIAMOND>

Group Number:<3>

Test Case ID	Test description	Test steps	Test Data	Expected result	Actual result	Pas s / Fail	Test comments
PT1-1	Multi-Factor Authentication and Verification	1. Navigate to the login page. 2. Enter valid user credentials 3. Respond to multi-factor authentication prompt	Valid username and password; MFA token	User is granted access after successful MFA verification.	TBD	TBD	MFA should be mandatory for all users.
PT1-2	Role-Based Access Control Functionality	1. Log in as a user with a specific role. 2. Attempt to access features and data permitted for the role. 3. Attempt to access features and	User credentials with predefined roles	User can access features and data for their role; access to other features is denied.	TBD	TBD	Ensure all roles are tested

		data not permitted for the role.					
PT1-3	Verify that the system recognizes and rejects weak passwords.	Open the Create Account or Change Password screen. Enter a weak password that is easy to guess. Submit the request.	Weak password, such as "123456".	The system displays an error message that the password is not strong enough.	TBD	TBD	Verify that password complexity requirements are enforced.
PT1-4	Tests if the account is locked after multiple incorrect attempts.	Enter a valid username and an incorrect password. Repeat this operation for more than the number of attempts the system sets.	Valid username and incorrect password.	The account is temporarily locked and cannot be logged in.	TBD	TBD	Check that the system is effectively protected against bruteforce breaking attacks
PT1-5	Session Timeout and Management	1.Log in to the system. 2.Remain inactive for the duration of the session timeout period. 3.Attempt to perform an action after the timeout period.	User credentials	Session times out and requires re-authentication	TBD	TBD	Timeout periods should align with security policies.

PT1-6	User Interface Workflow Verification	1.Log in to the system. 2.Navigate through various sections according to user role. 3. Perform typical user actions.	User credentials ; workflow scenarios.	The user can navigate and perform actions without errors.	TBD	TBD	Note any UI elements or workflows that are not intuitive.
PT1-7	Information Abstraction and Data Display	1.Log in as a user with restricted data access. 2.Navigate to areas with sensitive data. 3.Verify that data is displayed according to access level.	Restricted user account.	Sensitive data is abstracted, and only appropriate information is displayed.			Pay special attention to PII and SPII data handling.
PT1-8	Test firewall configuration and effectiveness	1. Configure firewall rules 2. Try various network requests 3. Monitor and log firewall responses		Firewalls allow or deny traffic based on security protocols.			Note any unexpected firewall behavior.
PT2-1	ANPR and speeding camera data capture and transmission validation	1.Position vehicle within ANPR and speeding camera range.	License plate images and speeding images	Accurate license plate data and driver's photo is			Check for any data corruption or loss during transmission.

		<p>2.Trigger license plate capture event</p> <p>3.Confirm data is sent to local processing unit.</p>		<p>captured and transmitted to the local processing unit.</p>			
PT2-2	Local Processing Unit Data Transformation Test	<p>1.Input raw data from ANPR and speed cameras.</p> <p>2.Observe the transformation process in the local unit.</p> <p>3.Check the output data format for system compatibility.</p>	Raw data from cameras.	Data is correctly transformed into a readable format for the central system.			Transformation errors must be logged and analyzed.
PT2-3	Central Data Receiver Aggregation Test	<p>1.Send data from multiple processing units to the central receiver.</p> <p>2.Ensure all data is aggregated correctly.</p>	Processed data from local units.	Central receiver aggregates all endpoint data accurately.			Pay attention to any data loss or mismatch.

		3.Validate the central data for completeness and accuracy.					
PT3-1	Offender Identification Match Test	<p>1.Input known offender data into the system</p> <p>2.Process data to match with existing records.</p> <p>3.Review the final decision output from the system.</p>	Offender biometric and identification records.	The system correctly identifies matches with existing data sources and outputs the correct verdict.			Any mismatches or errors should be noted for further investigation.
PT3-2	Data Integration and Transfer Test	<p>1.Ensure that data from the Data Collection Layer is received.</p> <p>2. Monitor the processing and subsequent data transfer to the Web Application Layer.</p> <p>3.Verify the integrity and accuracy of the data post-transfer.</p>	Processed data ready for transfer	Data is accurately integrated and transferred to the next layer without loss or corruption.			Delays or interruptions in data transfer should be examined.

PT3-3	System Health Monitoring Verification	<p>1.Observe the central processing unit during operation</p> <p>2.Simulate various processing loads and monitor system health metrics.</p> <p>3.Check that security and compliance layers receive accurate activity data</p>	Variable data processing loads.	System health is maintained , and any issues are reported to the security and compliance layers.			Notes on system performance under different loads are important for scalability and availability assessments.
PT4	Verify Data Segregation and Retrieval	<p>1. Insert PII (personally identifiable information) data into the system</p> <p>2.Query the database to retrieve the inserted data.</p>	Simulated PII data entries.	Data is correctly segregated into the respective database and can be retrieved accurately.			Ensure that the middleware enforces access controls.
PT5	Intrusion Detection and Response Test	<p>1.Simulate an intrusion attempt</p> <p>2.Monitor for alerts and automated responses</p>	Intrusion patterns.	Intrusion is detected, and an alert is generated with an appropriate response initiated			Note response times and any false negatives or positives.

PT5-1	IDPS Alert Generation and Response	1. Simulate known attack vectors. 2. Monitor the IDPS for alerts. 3. Check automated system response.		IDPS detects attacks and triggers appropriate alerts and responses			Record any failure or delay in detection or response.
PT6-1	GDPR Compliance Verification	1.Review report generation for compliance with GDPR 2.Audit a sample of offence reports for data handling adherence.	Generated offence reports	All reports comply with GDPR requirements, with data handling processes properly documented.			Document any areas of non-compliance .
PT7-1	Verify Read/Write Operations	1.Send a write request to the middleware to store data in the database. 2.Send a read request to retrieve the data.	Sample data record for the database	Data is written and read accurately through the middleware			Check for data integrity and any potential errors or losses.

PT7-2	Audit Log Accuracy Test	<p>1.Perform various database actions through the middleware.</p> <p>2.Review the audit logs for accuracy of the recorded actions.</p>	Database access requests	All access requests are correctly logged with timestamps and user details.			Special attention to unauthorized access attempts.
PT7-3	Data Access Control Validation	<p>1.Attempt to access the database via API with varying permission levels.</p> <p>2. Verify that access is granted or denied according to the requestor's permissions</p>	API requests with different access levels	Access is controlled according to predefined rules; unauthoris ed requests are denied.			Include tests for both successful and unsuccessful access attempts.
PT8-1	Full Backup Process Verification	<p>1. Initiate a full backup of the system's data</p> <p>2. Confirm completion of the backup process.</p> <p>3. Verify integrity and</p>	Current operationa l data from the system.	Full backup is completed successfull y with data integrity maintained			Note the time taken for backup and any discrepancies in data size.

		completeness of the backup data.					
PT8-2	Incremental Backup Functionality Test	1.Make a change to the system's data 2.Perform an incremental backup 3.Validate that only new or changed data has been added to the backup.	Updated records post-initial full backup.	Incremental backup adds only new or changed data since the last full or incremental backup.			Verify that the backup size corresponds to the volume of changes.
PT8-3	Disaster Recovery Simulation	1.Simulate a disaster scenario with data loss. 2.Activate the disaster recovery plan. 3.Restore data from the latest backup.	Backup data set	System data is restored to the most recent state before the disaster, within the acceptable recovery time objective (RTO).			Document the restoration process, any issues encountered, and the time to recover.
PT9	Protocol has no deadlock	Start with the communication process		Should establish communication successfully	TBD	TBD	

PT10	Data encryption	1. Check data encryption in transit 2. Inspect secure session		Data is encrypted using an advanced version of the encryption algorithm			
PT11	Failover Mechanism	1. Simulate primary server failure 2. Observe failover		Automatic switch to backup server			
PT12	CDN and Rate Limiting Effectiveness Verification	1. Initiate high-volume requests to simulate DDoS 2. Analyze CDN traffic distribution and rate limiting	High-volume network traffic	CDN effectively distributes load; rate limiting prevents service disruption.			Document any lag or failure in traffic management.

Explanation of Test Case Template:

PT1: Test cases focus on the functionality within the **Web application layer** and its interaction with other layers.

PT2: Test cases focus on the functionality within the **Data Collection Layer** and its interaction with other layers.

PT3: Test cases focus on the functionality within the **Data Processing and Analysis Layer** and its interaction with other layers.

PT4: Test cases focus on functionality within the **Data Storage Layer** and its interaction with other layers.

PT5: Test cases focus on functionality within the **Security and Monitoring Layer** and its interaction with other layers.

PT6: Test cases that focus on functionality within the **Reporting and Compliance Layer** and its interaction with other layers.

PT7: Test cases that focus on functionality within the **Data Integration Middleware** and its interaction with other layers.

PT8: Test cases that focus on functionality within the **Backup and Recovery Systems**

PT9-11: Supplemental test cases for non-functional requirements of the system to ensure that the system is trustworthy.

Exit criteria

- **Completion of All Test Cases:** All planned test cases must be executed, and results documented.
- **Defect Resolution:** Critical and high-priority defects must be resolved and retested. A certain threshold for acceptable minor defects can be set.
- **Quality Metrics Satisfaction:** Specific quality metrics such as defect density, code coverage, or test pass rate must meet predefined thresholds.

- **Stakeholder Approval:** Key stakeholders must review and approve the testing outcomes.
- **Documentation Completion:** All test documentation should be finalised, including test cases, defect logs, and final test reports
- **Compliance Verification:** The system must be verified for compliance with relevant standards and regulations.

Performance

Balanced Scorecard

BALANCED SCORECARD - DIAMOND SYSTEM

		OBJECTIVE	MEASURE	SCALE	EXPECTED	ACTUAL	DEVIATION	PLAN OF ACTION
CUSTOMER		Maintain high levels of customer satisfaction	Customer Satisfaction Index	Average rating (1-10)	9	8.7	-0.3	Implement customer feedback loop and improve service based on feedback.
		Enhance data privacy	Number of privacy breaches	Count (Breaches per year)	0	0	0	Strengthen encryption and access controls.
		Ease of use	User Interface (UI) Usability Rating	Average rating (1-5)	4.5	4.2	-0.3	User training. User manual.
		Enhance Customer Support	Average resolution time	Average time in minutes	≤ 5 m	6 m	1	Hire more support staff.
		Improve System Accessibility	Accessibility score	Percentage (0-100%)	90%	85%	-5%	Update UI/UX design (e.g. better and readable fonts)
IMPROVEMENT		System components' response time	Average response time of components	Milliseconds (ms)	25ms	60ms	-35 ms	Code optimisation. Hardware upgrade.
		License plate and facial recognition accuracy	Accuracy rate	Percentage (0-100%)	99%	95%	-4%	Improve the AI algorithms.
		Better fault tolerance	Number of component/system crashes	Incidents per month	≤ 2	5	3	Implement backup systems. Regular testing
		Security audits by external auditors/security consultants	Number of audits per quarter	Count per quarter	1	1	0	Schedule audits and follow the recommendations
		System security	Number of security vulnerabilities addressed	Percentage (0-100%)	100%	90%	-10%	A proper plan of action and roll out of security updates to address vulnerabilities in the system.

OBJECTIVE		MEASURE	SCALE	EXPECTED	ACTUAL	DEVIATION	PLAN OF ACTION
OPERATIONAL	System uptime	System availability	Percentage (0-100%)	99,999%	99,96%	-0,039%	Use of backup power sources.
	Security mock drills	Number of drills conducted	Count per year	4	4	0	Plan regular drills. Allocate resources
	Response time	Response time at the 99th percentile (P99)	Percentile and Milliseconds (ms)	P99 (100 ms)	P90 (100 ms)	NA	Implement Load Balancing. Hardware upgrade.
	Stress handling	Maximum number of concurrent connections system is able to handle optimally	Number of connections	50,000	35,000	-15000	Upgrade hardware, increase number of servers, use load balancers, cache data when necessary, switch to better distributed algorithms
	Streamline maintenance	Maintenance downtime	Hours per month	< 1 h	2 h	1 h	Develop predictive maintenance capabilities
	System integration	Integration success rate	Percentage (0-100%)	100%	100%	0%	Use modular architecture for easy integration
	Backup	Backup success rate (%)	Percentage (0-100%)	100%	98%	-2%	Routine auditing and evaluation of backup systems.
	Disaster recovery	Recovery time objective (RTO)	Minutes to full recovery	20 m	30 m	-10 m	Test recovery plans regularly. Mock drills.
	Cost-effectiveness	Cost per detection	£ per detection	<£1	£1.1	£-0.1	Optimise system resource utilization. Improve data usage.
	Security training sessions	Number of sessions per quarter	Count per quarter	1	1	0	Schedule regular sessions, update training material, incentivize attendance.
FINANCIAL AND RISK MANAGEMENT	Compliance adherence	Compliance rate	Percentage (0-100%)	100%	100%	0%	Stay updated with regulations and compliance training

Fig 8 & 9: Balanced Scorecard - DIAMOND System

The Balanced Scorecard presented here is structured to ensure that the DIAMOND system's operational and strategic performance aligns with the set objectives. The scorecard spans across essential views: Customer, Improvement, Operational, and Financial and Risk Management. Each of these perspectives is tied to specific, quantifiable objectives, such as maintaining customer satisfaction and enhancing data privacy, which are central to the system's interaction with users and their data.

Any system that deals with sensitive data and accesses sensitive systems ought to be secured with strict security measures. Because DIAMOND ingests large volumes of data, operates on a very large scale, and has access to sensitive and personally identifiable data, strict measures must be adopted. Assurance about the system's reliability and attack resiliency can only be conveyed through quantifiable and objective measures. The balanced scorecard designed for this system details the various security measures that must be adopted. These measures can be broadly classified into Defence, Mitigation, and Recovery.

There are 2 broad ways through which an attacker can gain access to the system's internals:

1. One or more internal components of the system are vulnerable

A complex system like DIAMOND has multiple internal components that interact seamlessly. Data is always in transit between these components. Multiple tools, frameworks, and technologies are leveraged to make such a complex system work. It is possible that these tools or frameworks are plagued with vulnerabilities and may work as an attack vector for a malicious actor. Malicious actors in the past have chained one or more vulnerabilities to cause greater damage. Therefore, there is a need for a proper vulnerability address system. Because a complex and large-scale system like DIAMOND may have multiple vulnerabilities, there must be a proper addressal mechanism.

2. One or more administrator account(s) are breached

One or more administrative accounts may be breached via social engineering attacks. It is therefore necessary to ensure that the staff is equipped with sufficient knowledge and insights about the attacks. This requires that there be a separate mechanism through which the security training sessions are carried out.

Because the system can be breached in different ways, different measures need to be adopted. The balanced scorecard is an attempt to explain these security measures in a manner that can be measured.

Security measures:

Security vulnerabilities within the system

A system may have multiple vulnerabilities. This can act as a baseline of how secure the system is. Furthermore, it is also necessary that we look at the individual severity of these vulnerabilities. It makes sense to divide these vulnerabilities into categories such as critical, medium, and low. The measure of each category may then give us an insight into the system's security.

- Measure: The number of overall vulnerabilities and the number of vulnerabilities belonging to critical, medium, and low classifications.
-
- Aim/Target: No critical vulnerabilities must be present in the system at any given time.
-
- Tolerance/Threshold: Consider 2 similar scenarios where a particular system is affected by:

“x” number of low-severity vulnerabilities, and,
“x” number of medium-severity vulnerabilities.

In both cases, the number of vulnerabilities is the same. However, the 2nd scenario has more severe vulnerabilities and may have severe consequences/lasting damage. Since the medium-severity vulnerabilities are likely to cause more damage in comparison, it makes sense that they be addressed first. Furthermore, it is possible that the scanning tools used may report false positives or that the system has low-impact vulnerabilities that do not warrant immediate attention. Therefore, there can exist a tolerance or a threshold value for the number of vulnerabilities. Anything beyond this threshold warrants an immediate action. However, it is not simply possible to define this value and is situation-specific.

Security training sessions

- A system's security is also dependent on the user and their actions. It is therefore important that the staff be made aware of the threat landscape and is trained accordingly. The number of training sessions per quarter provides an insight into how trained and equipped the staff is when it comes to security awareness.
- Measure: Number of training sessions conducted per Q/Year.
- Aim/Target: The number of training sessions is highly dependent on the staff's awareness of the security landscape. However, there should be at least 1-2 training sessions per quarter.

Security mock drills

- Mock drills may help evaluate how equipped the team is to handle security issues and vulnerabilities. Such drills help point out loopholes in the disaster management and recovery process and shed light on areas that need more improvement.
- Measure: The number of mock drills conducted per Q/Year along with the success rates and feedback.

Compliance adherence

- Systems that deal with sensitive data are expected to adhere to a set of standards revolving around information security and systems. These ISO standards help ensure that an organisation is putting best practices into use to safeguard its critical infrastructure and data.
-
- Aim/Target: Minimum relevant standards that deal with information security and information systems should be adhered to and met at all times.

Frequency of backups

- A system may be attacked by ransomware. In such cases, it becomes vital that the affected data is restored/replaced by a clean copy to prevent system

downtimes (since the DIAMOND system requires and operates on data). The system's resiliency to such attacks can be defined by backup policies.

- Measure: The frequency of incremental backups and the range of data it covers.
- Aim/Target: Incremental snapshots should be taken overnight.

Security audits by consultants/experts.

- Most organisations put their systems through security audits to get an opinion from a different perspective. This helps them identify security issues within the system that may have been missed for whatever reasons.
- Measure: Number of audits performed per quarter.
- Aim/Target: At least 2 comprehensive audits per year.

The measures and targets should be chosen based on:

- Their relevance
- The existing standpoint from a security point of view
- The scale at which the system is operating

The chosen numbers may change depending on various circumstances. The best way to ensure that the right numbers are being deployed and utilised is to continuously evaluate the system, reflect on the results, and look at the trends. These evaluations can be done as part of routine audits. A declining trend in one or more important parameters may mean that the security quality and position are being compromised and may lead to breaches. At the same time, an upward trend should not give room towards leniency/relaxation concerning the adopted security measures.

Security Dashboard

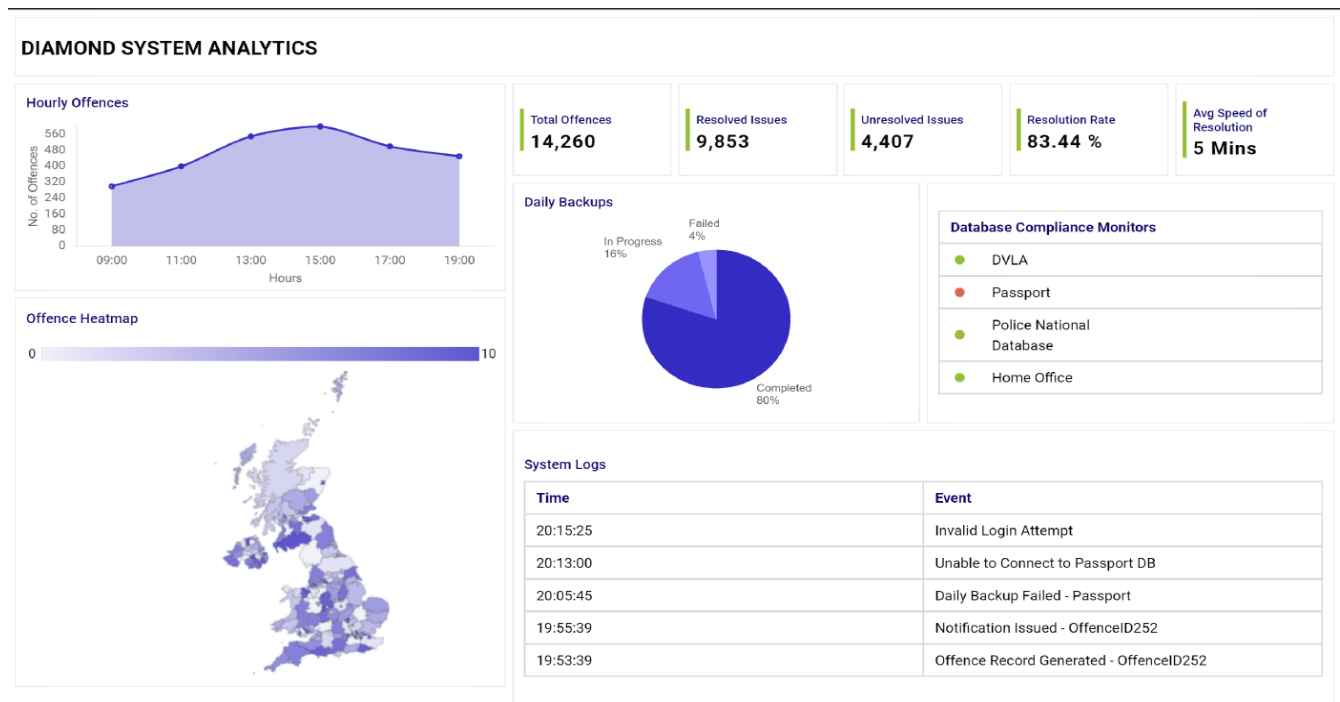


Figure 10: Security Dashboard

The following security dashboard was developed using various measurements which the group considered essential to be included for status monitoring, alerts and warnings. Some of the features that were included were inspired by other groups.

The security dashboard is designed for use by various government agencies which include the DVLA, Police, Home Office etc. The dashboard can be accessed by these organisations to understand and gain insights.

The DVLA and Police can recognise hotspots for speeding and make necessary arrangements for avoiding speeding incidents and reducing accidents. The heatmap is a perfect example which can be used to identify hotspots and regions with a higher rate of speeding.

An hourly traffic monitor can also be used to check the times and the number of offences registered for each hour. This can help identify overall trends.

The number of resolved and unresolved issues can be used by the various agencies to identify the number of issues which need to be resolved. This can also be used to identify points of failure within the system.

A database compliance monitor is also set up to ensure that the databases of various agencies are compliant with regulatory standards. It also ensures compliance with various security standards, for example, access controls and encryption. The database compliance monitor also checks for the quality and integrity of the data stored within each of the databases.

An event log is generated in order to see warnings as well as error messages. This allows for a better understanding of points of failure within the system during downtime. The logs generated also show when offence records are generated and also when the notification is forwarded to the offender. This helps understand the total time taken by the DIAMOND system from the triggering of the speed camera, recognition of the driver or vehicle details, extracting the relevant information from the databases of the different government agencies and issuing the speeding ticket to the assailant.

People-device Symbiosis in Secure System Architecture

Introduction

People-device symbiosis in secure system architecture refers to the seamless integration and interaction between the human users and the technological system, ensuring that both elements support each other in achieving the desired outcomes, particularly in terms of system security and efficiency. This symbiotic relationship is critical in systems like DIAMOND, which require a high level of trust and security due to the sensitive nature of the data processed.

Integrating System Design with Mitigation of Security Threats from Human Factors

Integrating the design of the DIAMOND system with the mitigation of security threats from human factors requires a multifaceted approach that prioritises user engagement, education, and system intuitiveness. The cornerstone of this strategy is the development of an interface that is both user-friendly and secure, minimising the potential for user error—a leading cause of security breaches. According to Nielsen (1993), usability is a critical aspect of system design that impacts user performance and satisfaction. Therefore, the DIAMOND system will incorporate features such as error-tolerant design, predictive text input, and logical navigation pathways. These features help prevent errors before they occur and offer corrective suggestions when they do, thereby enhancing the overall security of the system. Additionally, regular training sessions will be conducted to educate users on the importance of security protocols and the role they play in safeguarding the system. These sessions will cover topics such as password security, recognition of phishing attempts, and correct data handling procedures, tailored to accommodate the varying levels of user proficiency (MacKenzie, 2012).

Moreover, to further mitigate risks from human factors, the DIAMOND system will implement a robust feedback mechanism that provides real-time alerts to users about their actions within the system. This instant feedback allows users to quickly identify and rectify mistakes, reinforcing the correct use of the system and preventing potential security issues from escalating. For instance, the system might immediately notify a user if they attempt to input sensitive information into an unsecured field or if they are about to execute an action that could compromise system integrity. Such interactive feedback mechanisms are crucial for maintaining security and have been shown to significantly reduce error rates in complex systems (Shneiderman et al., 2005). By

combining these design principles with an ongoing commitment to user training and support, the DIAMOND system aims to create an environment where security is a shared responsibility, and all users are empowered to contribute to the system's integrity.

User Acceptance and Self-reporting of Risks and Incidents

User acceptance and the acceptable use of the DIAMOND system are crucial aspects that dictate its overall effectiveness and integrity. Achieving user acceptance begins with involving the users in the design and development process. This participatory approach ensures that the system aligns with their practical needs and expectations, thereby fostering a sense of ownership and familiarity with the system from the outset (Nielsen, 1993). For the DIAMOND system, this means engaging with law enforcement officials, who are the primary users, to understand their workflow and incorporate their feedback into the system design. This involvement not only aids in developing a system that is intuitive and efficient for its intended use but also helps in building trust in the system's capabilities. Furthermore, to ensure the system is used acceptably and responsibly, comprehensive training programs will be established, educating users about the system's capabilities and the ethical implications of its use. Such programs are crucial for clarifying the boundaries of acceptable use, particularly in a system handling sensitive data, and they contribute to preventing misuse of the system. Regular refresher courses and updates on new features or security protocols will maintain a high level of competency among users.

For the DIAMOND system to be fully integrated into the daily operations of its users, its acceptance must extend beyond initial training and onboarding. Continuous support and a responsive feedback system are key to sustaining long-term user engagement and acceptance. This can be achieved by establishing a dedicated support team that addresses user queries and concerns promptly, ensuring that users feel supported at all times. Additionally, implementing a feedback mechanism where users can report their experiences and suggest improvements helps in continually refining the system to better suit their needs. By maintaining open channels of communication and demonstrating a commitment to continual improvement, the system can adapt to the evolving requirements of its users, thereby ensuring its sustained acceptance and appropriate use. This iterative process, rooted in user feedback, ensures that the system remains not only functional but also relevant and user-centric in its operations (Shneiderman et al., 2005).

To ensure that users readily report risks and incidents, the DIAMOND system will incorporate an easily accessible and straightforward incident reporting mechanism. Creating a culture that emphasises the importance of security and the value of incident reporting is crucial. Users will be encouraged through incentive programs that reward vigilance and proactive reporting. Providing feedback on the actions taken in response to reports will maintain user engagement and trust in the system's commitment to security.

References:

Nielsen, J. (1993). Usability engineering. Morgan Kaufmann.

MacKenzie, I. S. (2012). Human-computer interaction: An empirical research perspective.

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2005). *Designing the user interface: strategies for effective human-computer interaction*. Pearson.