

D6.4 Social media for Enhanced Situation Awareness



This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 101021274



Protection of Critical Infrastructures from advanced combined cyber and physical threats

Deliverable nº:	D6.4
Deliverable name:	Social media for Enhanced Situation Awareness
Version:	1.0
Release date:	31/03/2022
Type* - Dissemination level**	Report - Public
Status:	Final
Editors	ICCS
Contributing WP	WP6

Abstract

This deliverable describes the design and development of the "Integration with Social Media" component of the PRAETORIAN platform. The component is responsible (i) for detecting social media posts related to security threats, (ii) for providing useful information from social media posts to security officers during incidents and (iii) for recommending relevant posts to social media to guide the public during incidents.

Disclaimer

This document contains material, which is the copyright of certain PRAETORIAN beneficiaries, and may not be reproduced or copied without permission.

The information appearing in this document has been prepared in good faith and represents the views of the authors. Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authors accept no statutory, contractual or other legal liability for any error or omission to the fullest extent that liability can be limited in law.

This document reflects only the view of its authors. Neither the authors nor the Research Executive Agency nor European Commission are responsible for any use that may be made of the information it contains. The use of the content provided is at the sole risk of the user. The reader is encouraged to investigate whether professional advice is necessary in all situations.

No part of this document may be copied, reproduced, disclosed, or distributed by any means whatsoever, including electronic without the express permission of the PRAETORIAN project partners. The same applies for translation, adaptation or transformation, arrangement or reproduction by any method or procedure whatsoever.

PRAETORIAN

PRAETORIAN strategic goal is to increase the security and resilience of European CIs, facilitating the coordinated protection of interrelated CI against combined physical and cyber threats. To that end, the project will provide a multidimensional (economical, technological, policy, societal) yet installation-specific toolset comprising: (i) a Physical Situation Awareness system, (ii) a Cyber Situation Awareness system; (iii) a Hybrid Situation Awareness system, which will include digital twins of the infrastructure under protection; and (iv) a Coordinated Response system. The PRAETORIAN toolset will support the security managers of Critical Infrastructures (CI) in their decision making to anticipate and withstand potential cyber, physical or combined security threats to their own infrastructures and other interrelated CIs that could have a severe impact on their performance and/or the security of the population in their vicinity.

The project will specifically tackle (i.e. prevent, detect, response and, in case of a declared attack, mitigate) human-made cyber and physical attacks or natural disasters affecting CIs. It will also address how an attack or incident in a specific CI can jeopardise the normal operation of other neighbouring/interrelated CIs, and how to make all of them more resilient, by predicting cascading effects and proposing a unified response among CIs and assisting First Responder teams.

PRAETORIAN is a CI-led, user-driven project, which will demonstrate its results in three international pilot clusters, some of them cross border -Spain, France and Croatia-, involving 9 outstanding critical infrastructures: 2 international airports, 2 ports, 3 hospitals and 2 power plants.

Document history:

Version	Date of issue	Content and changes	Partner
0.1	1 Mar. 2022	ToC	ICCS
0.2	15 Mar. 2022	Integrating input by FRs	ICCS, SDMIS, CPBV, CMRS
0.9	18 Mar. 2022	Ready for internal review	ICCS
0.10	25 Mar. 2022	Review	DLR
0.11	28 Mar. 2022	Review	RINI
1.0	31Mar. 2022	Final version	ICCS

List of Authors:

Partner	Author
ICCS	Lazaros Papadopoulos, Georgios Tzanos, Antonios Karteris
CMRS	Zdenko Lovric

Peer reviewed by:

Partner	Reviewer
RINI	Garik Markarian, Jelena Levak
DLR	Andrei-Vlad Predescu, Nils Carstengerdes, Meilin Schaper Tim H. Stelkens-Kobsch

Table of Contents

EXECUTIVE SUMMARY	9
1. INTRODUCTION	10
1.1 PURPOSE OF THE DOCUMENT.....	10
1.2 SCOPE OF THE DOCUMENT.....	11
1.3 STRUCTURE OF THE DOCUMENT	11
2. SOCIAL MEDIA SECURITY THREAT DETECTION	12
2.1 STATE OF THE ART.....	12
2.2 METHODOLOGY AND TECHNICAL IMPLEMENTATION	13
2.3 INTEROPERABILITY WITH THE PRAETORIAN PLATFORM	15
3. CRISIS OBSERVATION: IDENTIFICATION OF INFORMATIVE SOCIAL MEDIA POSTS DURING CRISES	17
3.1 STATE OF THE ART.....	17
3.2 METHODOLOGY & TECHNICAL IMPLEMENTATION	17
3.2.1 Text Classification.....	18
3.2.2 Image Classification	22
3.3 INTEROPERABILITY WITH THE PRAETORIAN PLATFORM	25
4. RECOMMENDATION OF CUSTOMIZABLE SOCIAL MEDIA POSTS TARGETING THE PUBLIC DURING CRISES	27
5. CONCLUSIONS.....	34
6. REFERENCES.....	35
ANNEXES.....	38
I. ANNEX A.....	38

Index of Tables

Table 1: Validation accuracy of text classification models.....	20
Table 2: Confusion matrix for informative tweet classification on the testing set (English)	20
Table 3: Confusion matrix for informative tweet classification on the testing set (multilingual).	21
Table 4: Performance metrics for the English and multilingual datasets.	21
Table 5: Validation accuracy of image classification models	23
Table 6: Confusion matrix for the ResNet50V2 model on the validation dataset	24
Table 7: Confusion matrix for the ResNet50V2 model on the testing dataset	24
Table 8: Performance metrics of ResNet50v2 for image classification on the testing dataset	25
Table 9: Warning message templates available in the PRAETORIAN IOP.	27

Index of Figures

Figure 1: Position of the “Integration with social media” component among the Response Coordination PRAETORIAN components.....	10
Figure 2: Functionality and data flow of the Social Media Security Threat Detection (SMSTD) subcomponent.	13
Figure 3: Normal priority tweet example	14
Figure 4: High-priority tweet example	15
Figure 5: Functionality and data flow of the Crisis Observation subcomponent.....	18
Figure 6: Training progression of LaBSE for 500 Epochs.	20
Figure 7: Text classification performance	21
Figure 8: Training progression of ResNet50V2	24
Figure 9: Performance of ResNet50V2 for image classification.....	25
Figure 10: Functionality and data flow of the social media post recommendation subcomponent	27
Figure 11: Schema for the flood-type warning template.....	28
Figure 12: Indicative schema for a flood-type incident.....	29
Figure 13: Example of a GET request in python using the requests library	30
Figure 14: Indicative GUI for social media post recommendation.....	31
Figure 15: Indicative GUI for generating and storing a new template.....	32
Figure 16: JSON file for new template.....	32
Figure 17: Posting a message generated by a new template.....	33

Abbreviations and Acronyms

AIDR	Artificial Intelligence for Digital Response
API	Application Programming Interface
BERT	Bidirectional Encoder Representations from Transformers
CI	Critical Infrastructure
CNN	Convolutional Neural Network
CPU	Central Processing Unit
DMD	Damage Multimodal Dataset
DSM	Disasters on Social Media
DSS	Decision Support System
FR	First Responder
GPU	Graphics Processing Unit
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
IOP	Interoperability Platform
JSON	JavaScript Object Notation
NLP	Natural Language Processing
NLU	Natural Language Understanding
NVD	National Vulnerability Database
ReLU	Rectified Linear Unit
REST	REpresentational State Transfer
SA	Situation Awareness
SMSTD	Social Media Security Threat Detection
URL	Uniform Resource Locator
VGG16	Visual Geometry Group 16
VLC	Valencia Airport
VRAM	Video Random Access Memory

Executive Summary

This deliverable describes the design and development of the "Integration with Social Media" component of the PRAETORIAN platform. The component is responsible for detecting social media posts related to security threats, such as posts about data leaks and cyber-attacks, which are of interest to the security officers of the Critical Infrastructures. Additionally, it provides useful relevant information from social media posts to security officers during incidents, to increase situation awareness. Finally, it recommends relevant posts to social media to guide the public during incidents. The component interacts with the Interoperability Platform and the Decision Support System of PRAETORIAN through REST API.

1. Introduction

1.1 Purpose of the document

The PRAETORIAN system utilizes social media in different ways. The “Integration with social media” component developed in the context of T6.4 consists of three subcomponents that perform the following:

1. Detection of posts about impending security threats in social media that the end user should be aware of.
2. Identification of useful information in social media, which can be used to increase the Situation Awareness (SA) of the end users during an incident.
3. (Semi-)automation of the posting of information to social media for end users, in order to facilitate the coordination of the public during an incident.

Therefore, social media act both as input of valuable information for the PRAETORIAN system, as well as output, in order to interact with the public during a crisis. Also, they are used both when no crisis is ongoing (by monitoring social media to detect suspicious posts), and during crises (by identifying posts related to the ongoing incident, or by automatically generating social media posts for the security officers).

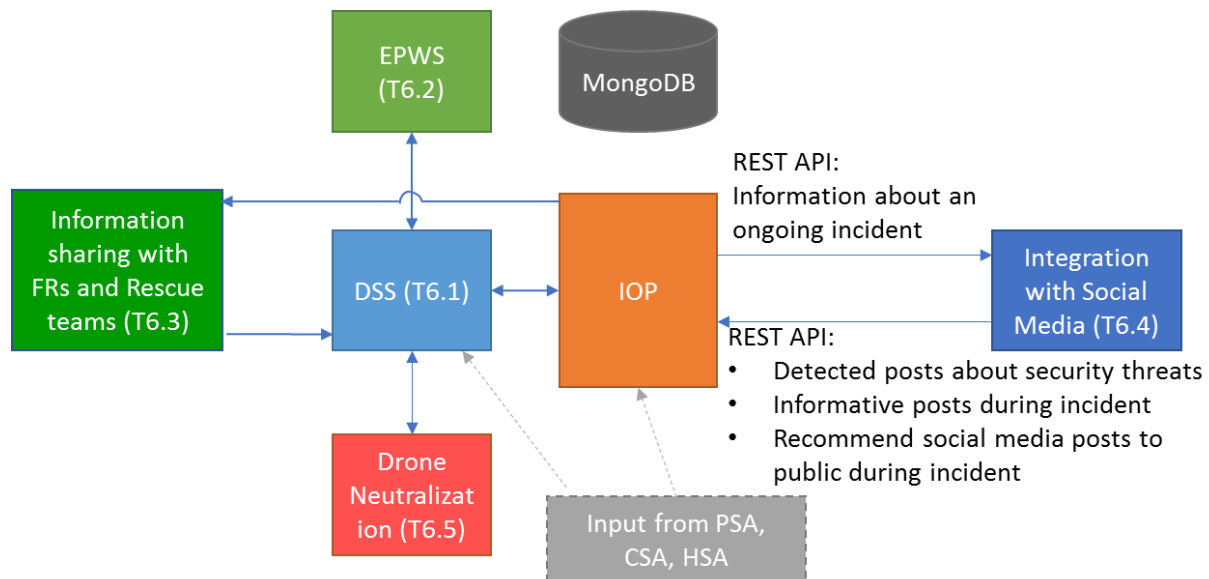


Figure 1: Position of the “Integration with social media” component among the Response Coordination PRAETORIAN components

Figure 1 shows the “Integration with social media” position among the PRAETORIAN Response Coordination components. It exchanges information with the Interoperability Platform (IOP) in both directions: The component retrieves information for a specific ongoing incident, such as the type of incident and the location. On the other hand, the detected suspicious posts, the informative posts by the public during an incident, as well as recommendations to security officers for posting to social

media to guide the public are stored to the IOP through REST API and forwarded to DSS through JSON format. (The inputs/outputs of each subcomponent are explicitly described in the following sections).

1.2 Scope of the document

This document describes the “Integration with social media” component of the PRAETORIAN Coordinated Response, as well as the design and development of its subcomponents.

1.3 Structure of the document

This document is structured as follows:

- Section 2 describes the subcomponent responsible for the detection of social media posts related to security threats.
- Section 3 deals with the subcomponent which identifies informative social media posts during a specific incident.
- Section 4 describes the subcomponent that recommends social media posts during an incident to guide the public, which security officers can optionally customize and post.
- Annex A includes social media post templates provided by PRAETORIAN partners participating as First Responders (FRs) that can be used in PRAETORIAN pilot scenarios.

2. Social Media Security Threat Detection

2.1 State of the Art

Given the meteoric rise of Twitter and other social media platforms in recent years, it is only natural that congregation sites like these would become vehicles for suspicious and malicious activity. With millions of users logging in and sharing their thoughts, opinions and activities every day, social media platforms offer an accessible and centralized way both for security experts and analysts to share their latest findings and provide information on vulnerabilities and data breaches, as well as for malicious agents to coordinate their activities.

On the cybersecurity front, information about security threats and data breaches is often shared on Twitter before it is analysed or even detected by specialized registries, such as the National Vulnerability Database (NVD) [1]. As such, large amounts of research have been put into utilizing Twitter as an alternate source of bleeding edge information on new security threats and vulnerabilities. Sapienza et al. [2] applied text mining techniques on tweets posted by reputable security experts to identify newly detected cybersecurity threats, but the effectiveness of this approach depends on the activity of specific Twitter accounts. Mittal et al. [3] developed CyberTwitter, a threat and vulnerability detection framework that monitors Twitter based on a set of keywords; their methodology focuses on generating alerts with full confidence but limited accuracy. Sceller et al. [4] proposed SONAR, a real-time cybersecurity event detection algorithm with higher accuracy, but their approach requires a preparation period of several months in order to collect a sufficient dataset of keywords. Alves et al. [5] offer SYNAPSE, a highly effective real-time security event identification module; however, their work is confined to monitoring security-related Twitter profiles and overlooks useful information that may emerge from third-party sources. On the subject of data breaches and leaks, most modern approaches require the possession of a detailed list of security-critical files, signatures and digital fingerprints [6], which is unattainable in the case of the PRAETORIAN system.

On the other hand, Twitter has also widely become a hotbed for terrorist and extremist content. Malicious agents have been utilizing Twitter and other social media platforms to propagate their ideology and coordinate their activities [7]. As such, detection of terrorist related activities on social media constitutes an essential tool for law enforcement agencies and security officers. Kaati et al. [8] develop a machine learning algorithm to classify terrorist affiliated content on Twitter, but their approach focuses more on determining terrorist affiliated user profiles, and less on determining their activities. Ahmad et al. [7] and Azizan et al. [9] use sentiment analysis techniques to classify tweets as extremist, but, while producing highly accurate results, their approaches do not focus on detecting and predicting extremist activities.

In the context of PRAETORIAN, the focus was put on creating a real-time security threat detection system that monitors the entirety of Twitter for posts that arouse suspicion regarding data breaches, cybersecurity vulnerabilities and potential terrorist threats on the Critical Infrastructures that pertain

to the PRAETORIAN project. Similarly to [2] and [4], a data mining approach is employed in order to provide the security officers of the CIs with essential information on potential security threats, and a large focus is put on detecting potential data breaches that are announced on Twitter, despite the lack of a centralized database of sensitive documents and files. In response to the limitations of the approaches proposed in [2] and [4], our approach allows Twitter-wide monitoring and offers out-of-the-box functionality and further customizability without requiring preliminary configuration activities.

2.2 Methodology and technical implementation

In this subsection, the Social Media Security Threat Detection (SMSTD) subcomponent of the “Integration with Social Media” component of the PRAETORIAN system is described in detail. SMSTD is a social media post monitoring and annotation application based on text mining techniques, and operates as shown in figure 2.

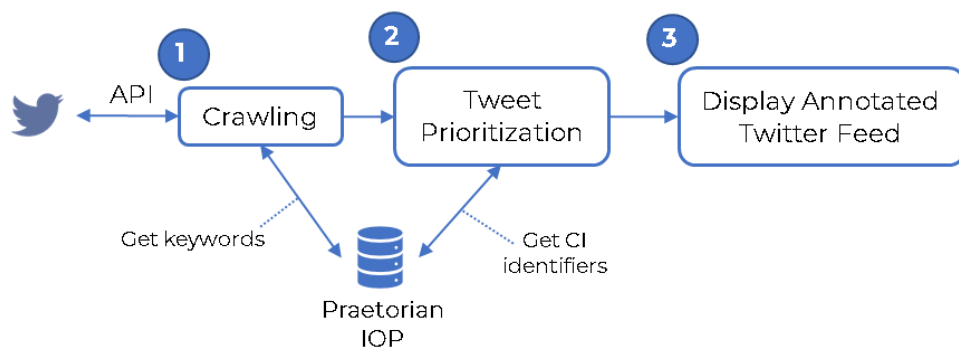


Figure 2: Functionality and data flow of the Social Media Security Threat Detection (SMSTD) subcomponent.

First, the SMSTD is supplied with a curated list of cybersecurity and cyber threat related keywords, originating from a number of different sources ([4] [3]). These keywords are categorized according to the taxonomy defined in [4]:

- Data breaches
- Social engineering
- Vulnerabilities
- Malwares
- Botnets
- Denial of service attacks

Furthermore, the module is supplied with a consolidated list of terrorism and extremism related keywords, composed from multiple sources ([10] [11] [12]). All keywords are supplied in English, Spanish, French and Croatian.

Supplied with the keyword list, the SMSTD composes a set of filtering rules and forwards it to the Twitter streaming service, utilizing the Twitter V2 API. In return, the SMSTD starts receiving a real-time feed of Twitter posts that correspond to the rules in a process also known as *crawling*.

Next, the SMSTD is provided with a list of identifiers related to the Critical Infrastructure in question. These identifiers include:

- CI name (and variants),
- CI location,
- Locations and Landmarks of importance in proximity to the CI,
- Physical assets of the CI (e.g. buildings, terminals on an airport, etc.),
- Digital assets of the CI (e.g. name of cloud or email provider, etc.),
- Usernames of Twitter accounts related to the CI.

The identifiers can be provided in a variety of languages, such as English, Spanish, French and Croatian.

Equipped with the identifiers, the SMSTD monitors the real-time Twitter feed and annotates the tweets that contain one or more of the CI identifiers as high priority, in a process coined *Post Prioritization*.

Once a post is identified as high priority, it is forwarded to the IOP to subsequently alert the responsible security officer through the DSS (Figure 2). An intuitive GUI is also offered as a proof of concept, through which the end-user can view the Twitter feed in real time.

The keyword and identifier lists are stored in the IOP. The SMSTD subcomponent is developed in the Python 3 programming language, and interfaces with the IOP through the REST API.

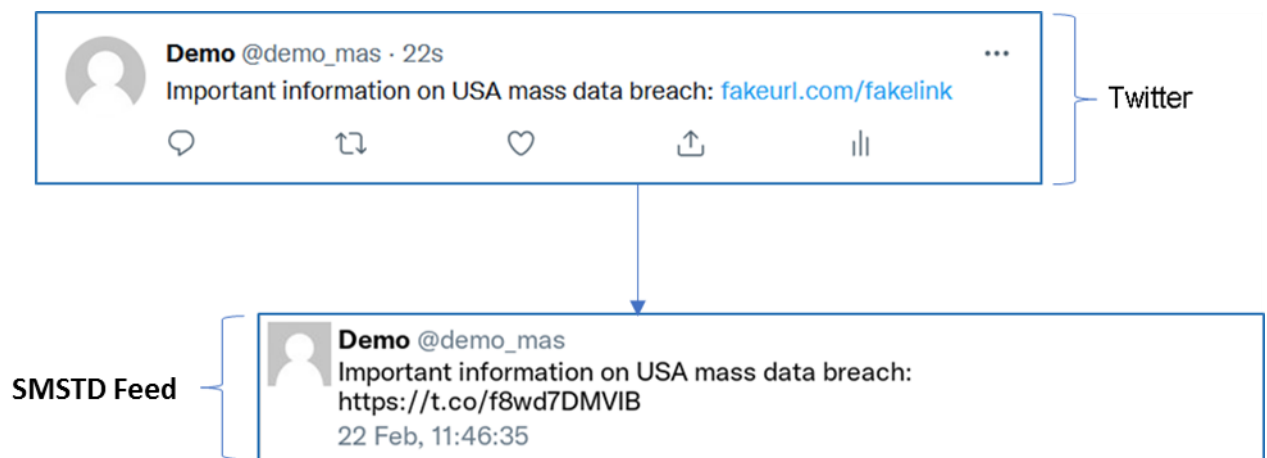


Figure 3: Normal priority tweet example

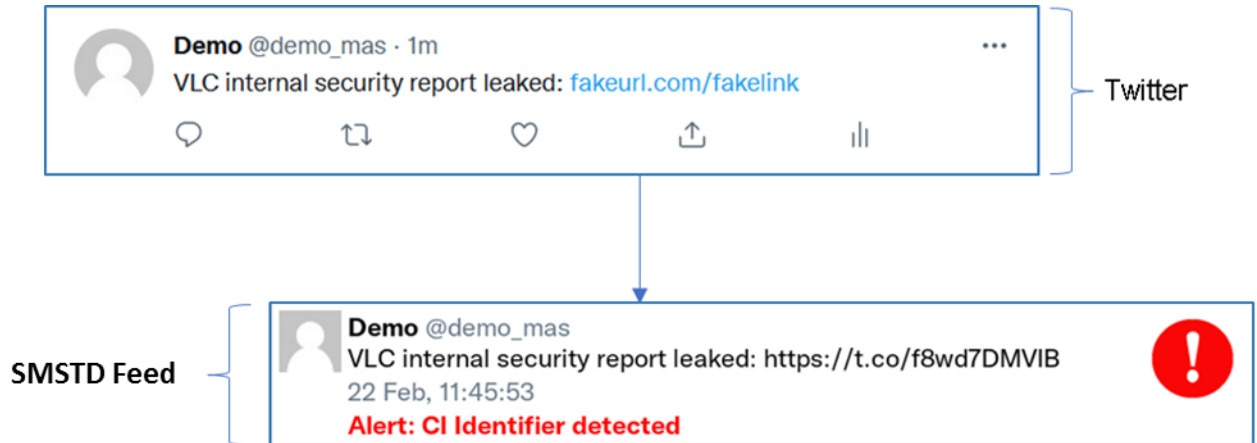


Figure 4: High-priority tweet example

Figure 3 and Figure 4 demonstrate an example of the functionality of the SMSTD, where the Critical Infrastructure is the VLC. In the first example, the tweet contains cybersecurity related keywords ('data breach') but no CI identifiers, so the tweet is detected but not classified as high priority. In the second example, the tweet contains both suspicious keywords ('security report') and a CI identifier ('VLC'), so the tweet is prioritized and annotated, and the security officer is alerted through DSS.

2.3 Interoperability with the PRAETORIAN Platform

This section contains the definitions of the inputs of the SMSTD components and the corresponding outputs, which will be used to enable the integration of the subcomponent into the PRAETORIAN system.

Inputs required at configuration time:

- Critical Infrastructure (CI) related information:
 - CI name (and variations),
 - CI location,
 - Locations and landmarks of importance in proximity to the CI,
 - Physical assets of the CI (e.g. buildings, terminals on an airport, etc.),
 - Digital assets of the CI (e.g. name of cloud or email provider, etc.),
 - Usernames of Twitter accounts related to the CI (e.g. Security officers, administrative staff etc.).

Inputs required at runtime:

- None (Input is provided through the Twitter API)

Outputs produced at runtime:

- Real-time feed of suspicious tweets,
- Notifications of detected suspicious tweets, forwarded to the PRAETORIAN IOP as a JSON file through the REST API.

Keywords and CI identifiers are uploaded to the MongoDB database of the Interoperability Platform in the form of text files and can be easily altered or customized directly through the database.

3. Crisis Observation: Identification of informative social media posts during crises

3.1 State of the Art

During natural and man-made disasters, providing critical information to security officers in order to develop situation awareness is an objective of prime importance to minimize the damage, perform successful evacuation operations and effectively coordinate all personnel activities.

In recent years, social media such as Twitter have become an important, and often overlooked, source of vital information. The role of social media evolved quickly from a congregation site to a real-time source of crowdsourced information during the 2010 Haiti earthquake [13], and Twitter has since largely cemented its place as a prime news source during disasters and crises [14].

As expected, the exhaustive amount of information present in social media has given rise to the question of discerning the informativeness of specific social media messages, especially during events where swiftness and timely responsiveness is imperative. Posts are defined as informative if they provide help to victims of a disaster or assistance to response agents or humanitarian organizations in the form of vital information about the ongoing crises [15].

A lot of research work has gone into automatically discerning such informativeness in social media posts. Imran et al. [16] develop a model based on Conditional Random Fields (CRFs) to extract valuable information, yet they only focus on text posts. Caragea et al. [17] and Madichetty and Sridevi [18] developed Convolutional Neural Network (CNN) models to detect informative tweets; however, their work focuses solely on the text component of tweets too, and the accuracy of their approaches leaves much to be desired. Mozannar et al. [19] offer a multimodal classification solution to identify tweets reporting on damage during disasters with high accuracy; their limited dataset, though, disallows generalizations on the effectiveness of their approach.

In the context of PRAETORIAN, a multimodal classification technique is applied to both image and text elements of a tweet, in order to automatically detect those that contain valuable information quickly and effectively. Through the usage of machine learning techniques and leveraging of multilingual word embeddings, an effective classification algorithm is provided that should prove valuable in enhancing situation awareness as part of the PRAETORIAN system.

3.2 Methodology & Technical Implementation

To achieve the aforementioned goals, a social media monitoring tool based on Machine Learning techniques that operates at times of crisis, coined Crisis Observation, is developed.

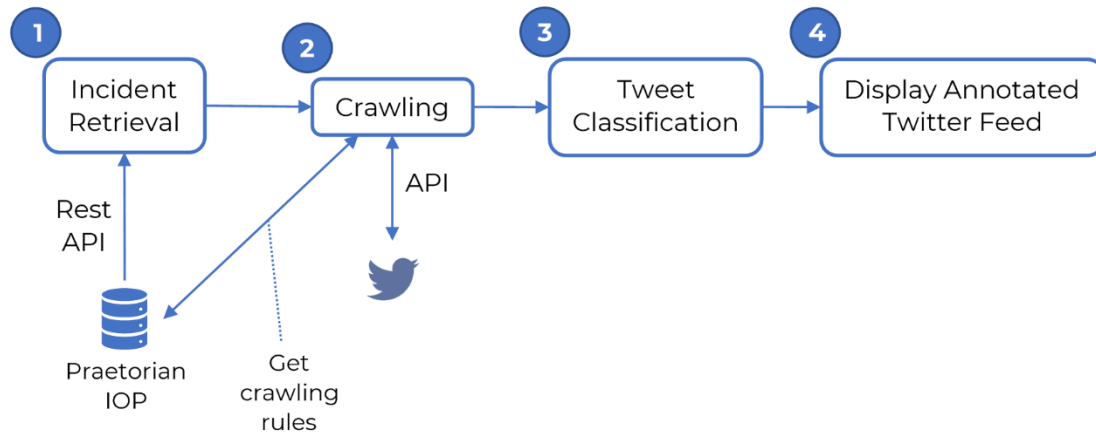


Figure 5: Functionality and data flow of the Crisis Observation subcomponent

First, as seen in Figure 5, the subcomponent receives an incident report from the PRAETORIAN Interoperability Platform through the REST API. This incident report contains essential information about an ongoing crisis at the Critical Infrastructure in question, including the type of crisis (Fire, Earthquake, blackout, etc.), as well as its location and time.

Next, the crisis observation subcomponent queries the Twitter v2 API for posts relevant to the ongoing crisis, using a list of rules that include keywords related to the type and location of the crisis. Similarly to the SMSTD, this process is coined *crawling*. Next, it performs multimodal, binary classification on the filtered posts in order to discern those that contain valuable information for the Security Officers of the Critical Infrastructure. More precisely, it performs binary text classification on the text of the tweet and image classification on the accompanying images, utilizing Natural Language Processing (NLP) and Binary Image Classification techniques, respectively. We elaborate on the classification techniques in the following sections.

Finally, the crisis observation subcomponent forwards the classified posts to the respective Security Officer through an intuitive, minimalistic GUI.

3.2.1 Text Classification

First, the crisis observation subcomponent requires a mechanism that discerns text messages on Twitter that contain useful information. For that reason, a Natural Language Processing (NLP) pipeline is developed, aiming to classify tweets posted during a crisis into two categories, depending on whether the information contained in the tweet in question is potentially informative or not.

Thus, a classification algorithm is developed in the Python 3 Programming Language using the sentiment classifier of the NLU SparkNLP library [20]. All training and validation are carried out on a computing infrastructure, courtesy of ICCS: 20-core Intel Xeon Gold 6138 CPU clocked at 2GHz, an Nvidia Tesla V100S GPU equipped with 32GB of VRAM and 132GB of RAM.

The dataset was created by merging a number of different datasets, containing tweets made during man-made and natural disasters. Particularly, the datasets are:

- CrisisLexT6 [21]
- CrisisLexT26 [22]
- CrisisMMD [23]
- SWDM2013 [16]
- ISCRAM13 [24]
- HumAID [25]
- DSM [26]
- AIDR [27]

and contain tweets made during disasters including:

- Biological Crises
- Cyclones
- Hurricanes
- Typhoons
- Bioterror Attacks
- Earthquakes
- Landslides
- Vehicle Crashes
- Bombings
- Explosions
- Residential Fires
- Volcano Eruptions
- Building Collapses
- Floods
- Tornadoes
- Wildfires

The final dataset contains an array of non-English tweets, which are split into a separate dataset in order to evaluate the model's multilingual performance. This multilingual dataset consists of 9199 tweets.

After data pre-processing, (consolidating, preparing the data, and removing duplicates), the final dataset consists of 156900 tweets, which is split further into three sets:

- Training set, consisting of 110457 tweets (70% of the total dataset)
- Validation set, consisting of 15062 tweets (10% of the total dataset)
- Testing set, consisting of 31381 tweets (20% of the total dataset)

For our sentence embeddings, two different multilingual options are utilized:

- Language-agnostic BERT Sentence Embeddings (LaBSE) [28]
- Multilingual BERT Sentence Embeddings (mBERT) [29]

Then, the two pipelines were trained for 500 epochs using a learning rate of 0.0005 and produced the following results:

Table 1: Validation accuracy of text classification models

Model	LaBSE	mBERT
Validation Accuracy (%)	85.35%	83.91%

The best performing model, LaBSE, was selected for the Crisis Observation implementation with regards to text classification. The training progression of the model through the 500 epochs is shown in Figure 6.



Figure 6: Training progression of LaBSE for 500 Epochs.

Next, we tested the model is evaluated using the testing set.

Table 2: Confusion matrix for informative tweet classification on the testing set (English)

	Informative	Not Informative	True values
Informative	16674	2157	
Not Informative	2748	9801	
Predicted Values			

Table 3: Confusion matrix for informative tweet classification on the testing set (multilingual).

	Informative	Not Informative	True Values
Informative	6693	1020	
Not Informative	762	724	
Predicted Values			

The confusion matrices for the two testing sets (English language and multilingual) are shown in Table 2 and Table 3.

Table 4: Performance metrics for the English and multilingual datasets.

	English dataset	Multilingual dataset
Testing Accuracy	84.37%	80.63%
Testing Precision	85.85%	89.78%
Testing Recall	88.55%	86.78%
Testing F1 Score	87.18%	88.25%

Table 4 summarizes the accuracy results using the English and the multilingual testing datasets.

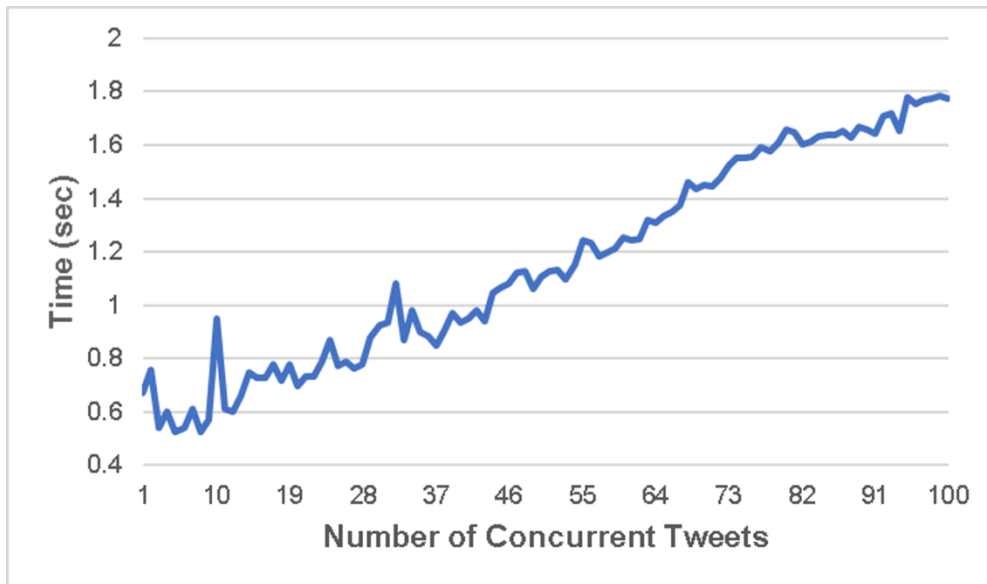


Figure 7: Text classification performance

The loading and initialization of the prediction pipeline takes a considerable amount of time (more than 30 seconds), rendering the hot-starting of the application essential. Once initialized, however, the pipeline exhibits real-time performance, producing predictions on single tweets on an average of 580 milliseconds and classifies clusters of multiple tweets in real time (up to 50 tweets per second), as illustrated in Figure 7.

3.2.2 Image Classification

Another source of potentially useful information through social media are the images that often accompany (or even constitute) users' posts. These pictures often contain information that either supplements or completely replaces the information contained in their text posts. For example, a user might upload an image of an ongoing fire with a non-descriptive caption, making it impossible for the subcomponent to discern the value of the information without assessing the accompanying image. For that reason, a specialized Convolutional Neural Network (CNN) model that aims to classify these pictures as informative or not informative in real-time is developed.

To that end, the transfer learning approach is adopted, where a pre-existing CNN model that has already been trained on a different classification task is configured and retrained. This technique reduces the time required to train the model on new data, and often produces comparable classification results.

A training and validation algorithm was developed in the Python 3 programming language, utilizing the Tensorflow library [30] and the Keras deep learning API [31]. All training and validation were carried out on the computing system described in section 3.2.1.

The dataset used originates from a consolidation of an array of datasets from different sources into a single one. These datasets consist of images taken by real-life users and uploaded to their Twitter accounts during both natural disasters (earthquakes, floods, fires, hurricanes), as well as man-made crises (terrorist attacks, bombing incidents, armed conflicts). More specifically, the datasets are:

- ASONAM17 [32]
- CrisisMMD [23]
- AIDR [27]
- DMD [19]

After consolidating the datasets, the data for the training algorithm was prepared appropriately and duplicate images were removed. The final dataset consists of 59717 annotated images posted on social media during different crisis. Each image is classified as "Informative" or "Not Informative", depending on whether it contains any potentially useful information or not. The dataset was split further into three discrete sets:

- A training set, containing 42040 images (70% of the total dataset)
- A validation set, containing 5733 images (10% of the total dataset)
- A testing set, containing the remaining 11944 images (20% of the total dataset).

For our model, several pretrained classification models were evaluated, focusing on their potential accuracy, their performance impact and their real-time classification potential. The following models were used:

- VGG16 [33]
- ResNet50 [34]

- ResNet50V2 [35]
- InceptionV3 [36]
- MobileNetV2 [37]

To utilize these pretrained models as binary classification models, some changes are performed to their layered structure, and their hyperparameters are configured. This process is as follows:

1. Initialize pretrained models, skipping the pre-existing top layer.
2. Append the following layers on the top for binary classification:
 - a. An Average Pooling Layer,
 - b. A Dense Layer of output size 1024 and a 'ReLU' activator function,
 - c. A Dense Layer of output size 1 and a 'Sigmoid' activator function.
3. Freeze all layers apart from the newly appended ones.
4. Compile the model, using the 'Adam' optimizer and the 'Binary Crossentropy' Loss Function.
5. Train for at least 10 epochs, with Early Stopping and Learning Rate Reduction.

The models were then trained on the training set until the Early Stopping function activated, indicating that the loss performance of our model has reached a plateau. At the end of each epoch, our training algorithm validates our classification model against the validation set of images, and informs us of the current performance of our model.

Table 5: Validation accuracy of image classification models

Model	VGG16	ResNet50	ResNet50V2	InceptionV3	MobileNetV2
Validation Accuracy (%)	81.77%	70.10%	86.13%	83.94%	84.49%

At the end of the training, the accuracy results for the 5 different CNN models were obtained as shown in Table 5. Evidently, the ResNet50v2 model produces the best performance, so it is elected to be used for the image classification task.

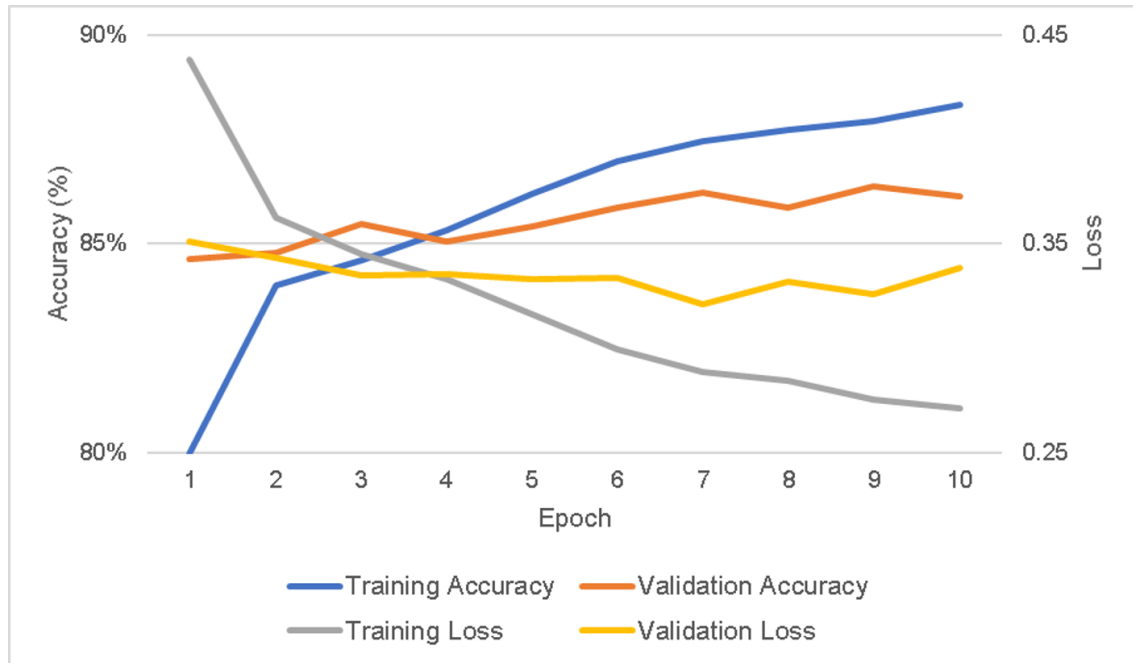


Figure 8: Training progression of ResNet50V2

Figure 8 shows the fluctuation of the accuracy and loss metrics of the model progressively for every training epoch.

In order to further evaluate the performance of our model, the confusion matrix of the model on the validation set was generated (Table 6).

Table 6: Confusion matrix for the ResNet50V2 model on the validation dataset

	Informative	Not Informative	True Values
Informative	2584	411	
Not Informative	384	2354	
Predicted Values			

Next, the model was evaluated against the testing set of the dataset, and the confusion matrix was generated (Table 7):

Table 7: Confusion matrix for the ResNet50V2 model on the testing dataset

	Informative	Not Informative	True Values
Informative	2852	562	
Not Informative	505	4558	
Predicted Values			

Table 8: Performance metrics of ResNet50v2 for image classification on the testing dataset

Testing Accuracy	87.41%
Testing Loss	0.3047
Testing Precision	84.96%
Testing Recall	83.54%
Testing F1 Score	84.24%

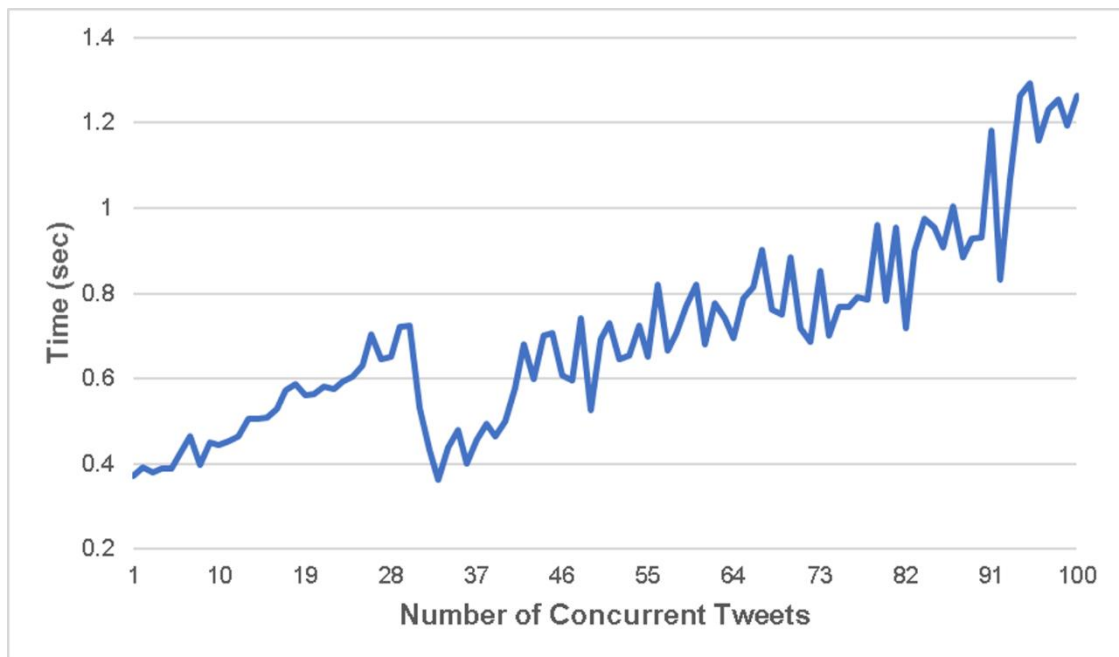


Figure 9: Performance of ResNet50V2 for image classification

The accuracy of the image classification model is summarized on Table 8. As shown, our model makes the correct prediction 87% of the time. Performance wise, our image classification application requires approximately 8 seconds on our server to initialize and load the model, necessitating the hot-start of the application. Once loaded, however, the model exhibits real-time classification performance, making predictions on single images in less than 400ms, and efficiently predicting over larger sets of images in real-time (up to 90 tweets per second), as displayed in Figure 9.

3.3 Interoperability with the PRAETORIAN Platform

This section contains the definitions of the inputs of the Crisis Observation subcomponent and the corresponding outputs, which will be used to enable the integration of the subcomponent into the PRAETORIAN system.

Inputs required for configuration:

- None

Inputs required at runtime:

- Incident Alert in JSON format:
 - Type of Incident (e.g. bomb, fire, earthquake, etc.),
 - Location of Incident,
 - Time of Incident

Outputs generated:

- Real-time feed of relevant tweets

4. Recommendation of customizable social media posts targeting the public during crises

The third subcomponent developed in the context of the “Integration with social media” is used to provide recommendations to security officers of CIs about social media posting in order to coordinate and guide the public during an incident. It is based on a set of template posts, grouped by incident type, which the security officers can edit before posting.

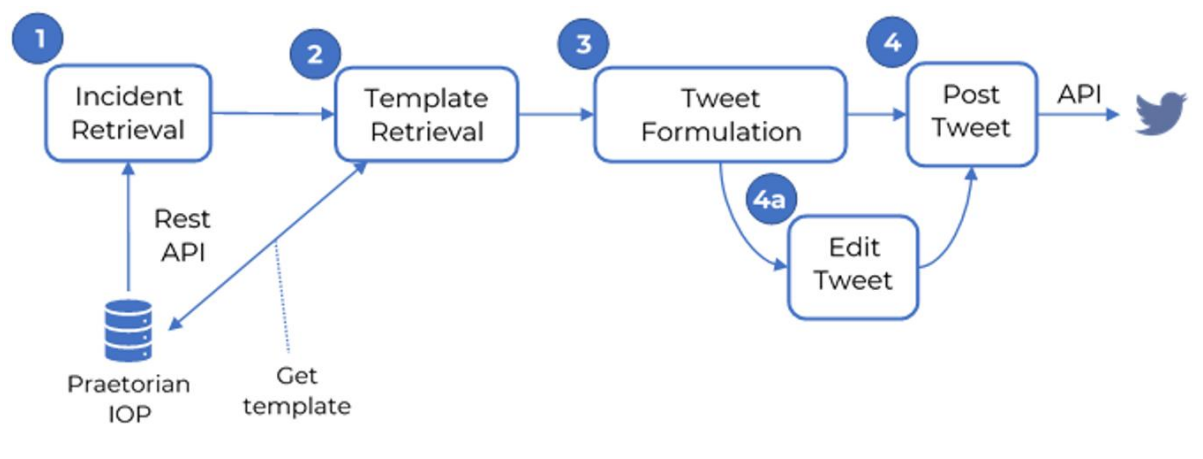


Figure 10: Functionality and data flow of the social media post recommendation subcomponent

The functionality and the data flow of the subcomponent are shown in Figure 10. The social media post templates are stored in the IOP. During an incident, relevant information about the incident, such as the type, the location and the time are retrieved from the IOP. This information is used for two purposes:

1. To select the relevant social media post templates.
2. To customize the templates based on incident-specific information. This is done automatically: for example, the location and/or the time of the incident are filled in automatically in the template based on the information already available for the ongoing incident.

The security officers can then edit and adapt the post and finally post it in the social media to guide the public accordingly.

Table 9: Warning message templates available in the PRAETORIAN IOP.

Type	Warning Message
Flood	Flood Emergency! Flood warning for \$location. Follow instructions from authorities. Avoid the area.
Fire	Fire Emergency! Fire alarm in \$location. Evacuate the area. Follow instructions from authorities.

Building Evacuation	Building Evacuation Emergency! Calmly evacuate the \$facility building using the emergency exits. Follow instructions from authorities.
Explosion	Explosion Emergency! There has been an explosion in \$location. Prepare to evacuate. Follow instructions from authorities.
Power Supply Outage	Power Supply Outage Emergency! \$location is currently experiencing a power outage. Crews are working to restore power. Updates to follow.
Bomb Threat	Bomb Threat Emergency! \$location has received bomb threat. Prepare to evacuate. Follow instructions from authorities.

Table 9 shows examples of templates stored in the IOP and used by the social media post recommendation subcomponent. These templates were verified by the FRs and rescue team members of the PRAETORIAN consortium during the workshop that was held on 7 March 2022. The location field (i.e., \$location) is filled in automatically by the incident-specific information available in the IOP. These warning messages cover a variety of incidents and are relevant with the project pilot scenarios. More messages, in local languages, also tailored to pilot scenarios, are included in Annex A.

This subcomponent is already integrated in the PRAETORIAN system and uses the IOP. The rest of the section focuses on the implementation details.

The schema for a *warning messages template*, in other words the *Fields* contained in each *Document* in the *warningMessagesTempl Collection* is as follows:

- _id
- generated_by
- text_message_template

Then, the following fields are added automatically:

- _updated and
- _expired

Figure 11 shows an example of a schema for a flood-type warning template in JSON format:

```
{
  "status": "success",
  "data": {
    "_id": "flood",
    "text_message_template": "Emergency! Flood warning for
    $location. Follow instructions from authorities. Avoid
    the area. ",
    "generated_by": "Praetorian",
    "_updated": "2022-02-08T09: 37: 14.239Z",
    "_expired": false
  }
}
```

Figure 11: Schema for the flood-type warning template

The schema for an *incident* in the Incidents *Collection* is as follows:

- `_id`
- `incident_type`
- `location`
- `twitter_post`
- `description` (optional)

Then, the following fields are added automatically:

- `_updated` and
- `_expired`

Figure 12 shows an example of a schema for a flood-type incident in JSON format:

```
{
  "status": "success",
  "data": {
    "_id": "e8NFLJPnCJ7eRxbMQ",
    "name": "Town Flooding",
    "incident_type": "flood",
    "description": "Heavy Rain!",
    "location": "Valencia",
    "twitter_post": "Emergency!
    'Flood warning for Valencia. Follow instructions from
    authorities. Avoid the area.'",
    "_updated": "2022-02-08T18:38:03.275Z",
    "_expired": false
  }
}
```

Figure 12: Indicative schema for a flood-type incident

The implementation of the IOP enables the selection of the schema of our preference inside the Documents. This means that the Documents do not have required fields and the new entries can contain whatever type of data is required without restrictions.

A RESTful API is utilized in order to write to the database and enter new entries, as accessing the database directly is prohibited. The fact that the database is, as stated before, agnostic and schema-free aids in handling it using the RESTful API exclusively.

A REST API uses HTTP requests to access and use data. That data can be used to GET, PUT, POST and DELETE data types, which refer to the reading, updating, creating and deleting of operations concerning resources. These operations allow the handling of the data and of the specific operations concerning all the resources in the database.

The HTTP requests that a REST API handles can be sent using any programming language, so the Python language and the Requests library were chosen since the tool that develops and utilizes the data written and read from and to the database is also written in the Python language.

However, to be able to make any request to the database, the URL that the API is hosted on and the necessary credentials must first be declared. These credentials are declared in the request header, an HTTP header that can be used in an HTTP request to provide information about the request context so that the server can tailor the response. For example, the Accept- * headers indicate the allowed and preferred formats of the response, which in our case are headers used to supply authentication credentials.

Afterwards, the operation to be performed is chosen, and the request is sent to the server. Depending on the operation, a GET, a POST or a PATCH request can be sent, in order to retrieve data (Figure 13), add new data or update existing data, respectively. Finally, a response in the form of a dictionary is received, that can subsequently be iterated on to access the data.

```
import requests
from requests import *
import json

url = 'https://praetorian-api.k8s.etra-id.com/api/v2/praetorian/incidents'
headers = {
    X-User-ID: 'USER_ID',
    X-Auth-Token: 'AUTH-TOKEN',
    Content-Type: 'application/json;charset=UTF-8'
}
payload = ""
response = requests.request("GET", url, headers=headers, data=payload)
print(response.text)
```

Figure 13: Example of a GET request in python using the requests library

The need to develop a tool that will integrate all these requests into our post recommendation tool motivated us to the development of a custom library thanks to which, any request can be carried out in the database by defining only the desired parameters. At the same time, some functionalities were added which are not available with simple calls in the API. Such functionalities are the automatic completion of a field in a Document using data from another entry and the ability to search the database for both data and specific fields inside the Collections.

Therefore, in order to generate the recommended Twitter post using the templates stored in the IOP, the REST API and the custom *Library(HandlerDB)*, the steps bellow are followed:

The first step is to create an instance of the custom library. This instance will be initialized with all the necessary data in order to communicate and send requests to the database through the REST API.

```
hdr = HandlerDB("Incidents")
```

Based on the type of the incident, a search is conducted on all the warning message template documents until a relevant one is found. Then, the “generic keywords” contained in the template (e.g. \$location) are replaced with information provided inside the incident Document.

Assuming, for example, a new incident of flood type, an appropriate generic template would be the following:

“Emergency! Flood warning for \$location. Follow instructions from authorities. Avoid the area.”

If the incident was happening in Valencia, the modified message would be:

“Emergency! Flood warning for Valencia. Follow instructions from authorities. Avoid the area.”

Finally, the `get_twitter_post` method is called to retrieve the recommended post of an incident using its `_id`:

```
tweet = hdr.get_twitter_post('e8NFLJPnCj7eRxbMQ')
```

The screenshot displays the PRAETORIAN web interface. At the top is a navigation bar with links: Praetorian, Incidents, Templates, Statistics, Settings, Profile, and Log Out. Below this, a section titled 'NEW INCIDENT' contains a table with four columns: Name, Incident Type, Location, and Description. The table has one row with the values: Town Flooding, Flood, Valencia, and Heavy Rain. Below the table, there are three input fields: 'INCIDENT TYPE' with the value 'FLOOD', 'GENERATED BY' with the value 'PRAETORIAN', and 'RECOMMENDED SOCIAL MEDIA POST (press click to edit)' with the value '“Emergency! Flood warning for Valencia. Follow instructions from authorities. Avoid the area.”'. To the right of these fields is a large box labeled 'Twitter Feed' containing a Twitter logo. At the bottom, there is a 'Social Media' dropdown menu set to 'Twitter' and two buttons: 'Post' and 'Cancel'.

Figure 14: Indicative GUI for social media post recommendation

Figure 14 shows an indicative GUI for social media post recommendation. The type of incident, the field indicating who is posting the template and the recommended message are automatically generated. The security officer can edit the message and select the social media platform in which it will be posted.

Finally, another feature that is available in our tool is the creation of new warning message templates by security officers for types of incidents that lack a template in the PRAETORIAN system. In that case, the Security Officer can register a new template based on this new type of incident.

The steps that the Security officers are expected to follow are:

Firstly, the Security Officer will have to click on the *Templates* tab to register a *New Template* (Figure 15).

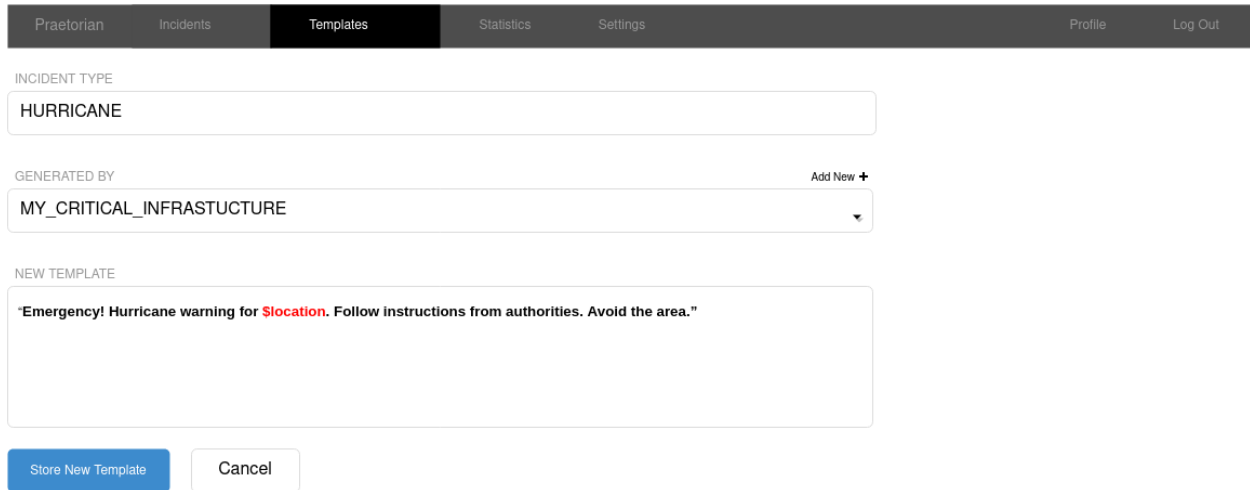


Figure 15: Indicative GUI for generating and storing a new template

In this tab the Security Officer fills:

- The field TYPE OF INCIDENT with the type of the Incident, which will be its unique identifier.
- The field GENERATED BY which will be the name of the Critical Infrastructure.
- The field NEW TEMPLATE where the Security Officer will write a generic new template by using one or more of the following keywords: *\$location*, *\$incident_time*, *\$facility*.

After that, by pressing the button *Store New Template*, this template will be stored in the database.

```
New_template = {"_id": "hurricane",
                "text_message_template": "Emergency! Hurricane warning for $location.
                Follow instructions from authorities. Avoid the area.",
                "generated_by": "CRITICAL_INFRASTRUCTURE"
                }
```

Figure 16: JSON file for new template

Behind the scenes, these fields generate a JSON file like the one in Figure 16. And to insert this new template in the database we will use the custom Library for the REST API:

```
hdr = HandlerDB("warningMessagesTempl")
pst = hdr.post(New_template)
```


Praetorian
Incidents
Templates
Statistics
Settings
Profile
Log Out

NEW INCIDENT

Name	Incident Type	Location	Description(optional)
Dangerous Hurricane	Hurricane	Barcelona	None

INCIDENT TYPE
Add New +
HURRICANE


GENERATED BY
More
MY_CRITICAL_INFRASTRUCTURE

RECOMMENDED SOCIAL MEDIA POST (press click to edit)

"Emergency! Hurricane warning for **Barcelona**. Follow instructions from authorities. Avoid the area."

Social Media
Twitter

Post
Cancel



Twitter Feed

Figure 17: Posting a message generated by a new template

After the Security Officer registers the new template, they can go back to the *Incidents* tab and post the social media message, as shown in Figure 17.

5. Conclusions

The design and the development of the "Integration with social media" component has been completed and the current focus is on the integration with the IOP and the interoperability with the other PRAETORIAN components. However, several possible extensions with significant interest are considered. More specifically, while the current implementation focuses on the Twitter social media platform, the possibility of extending the "Integration with social media" component to other platforms, such as LinkedIn or Telegram, is certainly worthy of investigation. Concerning the Crisis Observation subcomponent, it would be useful to investigate the possibility of training multiple discrete text or image classification models (one on each type of incident), and the impact this would produce on the classification accuracy of the module. Finally, another extension under consideration is the detection of fake social media posts, or posts that spread "fake news". There is a lot of existing work in this area and such a component would add useful functionality to the "integration with social media" PRAETORIAN component.

6. References

- [1] R. Campiolo, L. A. F. Santos, D. M. Batista and M. A. Gerosa, "Evaluating the utilization of Twitter messages as a source of security alerts," in *28th Annual ACM Symposium on Applied Computing (SAC '13)*, Coimbra, Portugal, 2013.
- [2] A. Sapienza, A. Bessi, S. Damodaran, P. Shakarian, K. Lerman and E. Ferrara, "Early Warnings of Cyber Threats in Online Discussions," in *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*, New Orleans, LA, USA, 2017.
- [3] S. Mittal, P. K. Das, V. Mulwad, A. Joshi and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," in *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, San Francisco, CA, USA, 2016.
- [4] Q. L. Sceller, E. Karbab, M. Debbabi and F. Iqbal, "SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream," in *ARES '17: International Conference on Availability, Reliability and Security*, Reggio Calabria, Italy, 2017.
- [5] F. Alves, A. Bettini, P. M. Ferreira and A. Bessani, "Processing tweets for cybersecurity threat awareness," *Information Systems*, vol. 95, 2021.
- [6] L. Cheng, F. Liu and D. Yao, "Enterprise data breach: causes, challenges, prevention, and future directions," *WIREs Data Mining and Knowledge Discovery*, vol. 7, no. 5, 2017.
- [7] S. Ahmad, M. Z. Asghar, F. M. Alotaibi and I. Awan, "Detection and classification of social media-based extremist affiliations using sentiment analysis techniques," *Human-centric Computing and Information Sciences*, vol. 24, no. 9, 2019.
- [8] L. Kaati, E. Omer, N. Prucha and A. Shrestha, "Detecting Multipliers of Jihadism on Twitter," in *2015 IEEE International Conference on Data Mining Workshop (ICDMW)*, Washington DC, USA, 2015.
- [9] S. A. Azizan and I. A. Aziz, "Terrorism Detection Based on Sentiment Analysis Using Machine Learning," *Journal of Engineering and Applied Sciences*, vol. 12, no. 3, pp. 691 - 698, 2017.
- [10] K. Al-Rowaily, A. Muhammad, N. A.-H. Haldar and A.-R. Majed, "BiSAL- A Bilingual Sentiment Analysis Lexicon to Analyze Dark Web Forums for Cyber Security," *Digital Investigation - The International Journal of Digital Forensics and Incident Response*, vol. 14, pp. 53-62, 2015.
- [11] S. Kramer, "Anomaly detection in extremist web forums using a dynamical systems approach," in *ISI-KDD '10: ACM SIGKDD Workshop on Intelligence and Security Informatics*, Washington DC, USA, 2010.
- [12] Department of Homeland Security and Federal Government of the United States, "Analyst's Desktop Binder," 2011. [Online]. Available: <https://epic.org/foia/epic-v-dhs-media-monitoring/Analyst-Desktop-Binder-REDACTED.pdf>.

- [13] M. Keim and E. Noji, "Emergent Use of Social Media: A New Age of Opportunity for Disaster Resilience," *American Journal of Disaster Medicine*, vol. 6, pp. 47-54, 2011.
- [14] D. E. Alexander, "Social Media in Disaster Risk Reduction and Crisis Management," *Science and Engineering Ethics*, vol. 20, no. 3, p. 717–733, 2014.
- [15] J. Houston, J. Hawthorne, M. F. Perreault, E. H. Park, M. G. Hode, M. R. Halliwell, S. E. McGowen, R. Davis, S. Vaid, J. A. McElderry and S. A. Griffith, "Social media and disasters: a functional framework for social media use in disaster planning, response, and research," *Disasters*, vol. 39, no. 1, pp. 1-22, 2015.
- [16] M. Imran, S. Elbassuoni, C. Castillo, F. Diaz and P. Meier, "Practical Extraction of Disaster- Relevant Information from Social Media," in *2nd International Workshop on Social Web for Disaster Management (SWDM'13)*, Rio De Janeiro, Brazil, 2013.
- [17] C. Caragea, A. Silvescu and A. H. Tapia, "Identifying informative messages in disaster events using Convolutional Neural Networks," in *13th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*, Rio de Janeiro, Brazil, 2016.
- [18] S. Madichetty and M. Sridevi, "Detecting Informative Tweets during Disaster using Deep Neural Networks," in *11th International Conference on Communication Systems Networks (COMSNETS)*, Bangalore, India, 2019.
- [19] H. Mozannar, Y. Rizk and M. Awad, "Damage Identification in Social Media Posts using Multimodal Deep Learning," in *15th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*, Rochester, NY, USA, 2018.
- [20] V. Kocaman and D. Talby, "Spark NLP: Natural language understanding at scale," *Software Impacts*, vol. 8, p. 100058, 2021.
- [21] A. Olteanu, C. Castillo, F. Diaz and S. Vieweg, "CrisisLex: A Lexicon for Collecting and Filtering Microblogged Communications in Crises," in *AAAI Conference on Weblogs and Social Media (ICWSM'14)*, Ann Arbor, MI, USA, 2014.
- [22] A. Olteanu, S. Vieweg and C. Castillo, "What to Expect When the Unexpected Happens: Social Media Communications Across Crises," in *ACM 2015 Conference on Computer Supported Cooperative Work and Social Computing (CSCW '15)*, Vancouver, BC, Canada, 2015.
- [23] F. Alam, F. Ofli and M. Imran, "CrisisMMD: Multimodal Twitter Datasets from Natural Disasters," in *12th International AAAI Conference on Web and Social Media (ICWSM)*, Palo Alto, CA, USA, 2018.
- [24] M. Imran, S. Elbassuoni, C. Castillo, F. Diaz and P. Meier, "Extracting Information Nuggets from Disaster- Related Messages in Social Media," in *10th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*, Baden-Baden, Germany, 2013.
- [25] F. Alam, U. Qazi, M. Imran and F. Ofli, "HumAID: Human-Annotated Disaster Incidents Data from Twitter," in *15th International Conference on Web and Social Media (ICWSM)*, Online, 2021.

- [26] CrowdFlower, “Disasters on Social Media,” [Online]. Available: <https://data.world/crowdflower/disasters-on-social-media>. [Accessed 10 January 2022].
- [27] M. Imran, C. Castillo, J. Lucas, P. Meier and S. Vieweg, “AIDR: Artificial Intelligence for Digital Response,” in *23rd International Conference on World Wide Web*, New York, NY, USA, 2014.
- [28] F. Feng, Y. Yang, D. Cer, N. Arivazhagan and W. Wang, *Language-agnostic BERT Sentence Embedding*, arXiv:2007.01852, 2020.
- [29] J. Devlin, M.-W. Chang, K. Lee and K. Toutanova, “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding,” in *2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, Minneapolis, MN, USA, 2019.
- [30] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, M. Devin, S. Ghemawat, I. Goodfellow, A. Harp, G. Irving, M. Isard and R. Jozefowicz, “TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems,” 2015. [Online]. Available: <https://www.tensorflow.org/>.
- [31] F. Chollet and others, “Keras,” 2015. [Online]. Available: <https://keras.io>.
- [32] F. Alam, F. Ofli, M. Imran, T. Alam and U. Qazi, “Deep Learning Benchmarks and Datasets for Social Media Image Classification for Disaster Response,” in *2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, The Hague, Netherlands, 2020.
- [33] K. Simonyan and A. Zisserman, *Very Deep Convolutional Networks for Large-Scale Image Recognition*, arXiv:1409.1556, 2015.
- [34] K. He, X. Zhang, S. Ren and J. Sun, *Deep Residual Learning for Image Recognition*, arXiv:1512.03385, 2015.
- [35] K. He, X. Zhang, S. Ren and J. Sun, *Identity Mappings in Deep Residual Networks*, arXiv:1603.05027, 2016.
- [36] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto and H. Adam, *Rethinking the Inception Architecture for Computer Vision*, arXiv:1704.04861, 2016.
- [37] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov and C. Liang-Chieh, *MobileNetV2: Inverted Residuals and Linear Bottlenecks*, arXiv:1801.04381, 2018.

Annexes

I. ANNEX A

This appendix includes templates of warning messages both in Croatian and in English, oriented to the PRAETORIAN pilot scenarios. These messages will be used by the subcomponent that recommends posts for social media to the security officers and will be integrated in the IOP, along with the more generic and short messages of Table 9.

EVAKUACIJA PODRUČJA HIDROELEKTRANE

TEKST ZA WEB/EMAIL/GLASOVNU PORUKU: Potrebna je trenutna evakuacija stanovnika naselja _____ nizvodno od brane HE _____ zbog _____ (navedite razloge za evakuaciju). Ostanite mirni. Slijedite upute žurnih službi i krenite prema mjestima za organizirani prijevoz ili krenite osobnim vozilima. Nakon što napustite područje, idite na zborna mjesta okupljanja evakuiranih osoba svoga mjesta. Obavezno se evidentirajte u službi traženja kako bi se pouzdano znalo da ste na sigurnom. Molimo ograničite korištenje telefona kako bi telefonske linije bile slobodne za poruke žurnih službi. Ostanite u pripravnosti za dodatne poruke i pratite informacije koje ćemo dostaviti putem HEP web stranice _____ ili broja 112. Osobe iz područja koja nisu na popisu za evakuaciju trebaju ostati na svojim mjestima i biti spremne za promjenu uvjeta.

TEKST SMS PORUKE: Potreba je evakuacija stanovnika naselja _____. Idite na evakuacijsko zborna mjesto gdje ćete dobiti informacije o područjima koja trebaju biti evakuirana.

PREKID UZBUNE

TEKST ZA WEB/EMAIL/GLASOVNU PORUKU: Opasnost od puknuća brane HE _____ je završila. Stanovnici evakuiranih naselja _____ mogu krenuti na zborna mjesta za organizirani povratak i prijevoz u naselja _____. Molimo budite u pripravnosti za daljnje upute.

TEKST SMS PORUKE: Opasnost je završila. Možete krenuti na zborna mjesta zbog organiziranog povratka ili ukoliko imate osobni automobil, možete se vratiti u naselja _____. Molimo budite u pripravnosti za daljnje upute.

HITNA SITUACIJA U ZGRADI AERODROMA

TEKST ZA WEB/EMAIL/GLASOVNU PORUKU: Hitna situacija u prostorima aerodroma: _____ u _____ (mjesto). Prostor aerodroma _____ je potencijalno ugrožen biološkim agensom opasnim za ljudsko zdravlje. Molimo, uzmite svoje osobne stvari i napustite zatvoreni prostor aerodromske zgrade i izađite na otvoreni prostor na parkiralištu ispred zgrade aerodroma slijedeći oznake za evakuaciju. Slušajte upute tehničkog osoblja i pratite informacije koje ćemo dostavljati putem razglasa i/ili posjetite web stranicu aerodroma _____ www. xxxxxxxxxxxx za više informacija i nove podatke o incidentu.

TEKST SMS PORUKE: Započela je evakuacija putnika i svog osoblja aerodroma _____.Krenite prema izlazu i pratite upute tehničkog osoblja aerodroma.

PREKID UZBUNE

TEKST ZA WEB/EMAIL/GLASOVNU PORUKU: Opasnost od ugroze biološkim agensom na aerodromu _____ je završila. Možete krenuti u aerodromsku zgradu bez straha za svoju sigurnost. Informacije o nastavku vašeg putovanja naći ćete na informacijskim punktovima i/ili na ekranima sustava za informacije o letovima aerodroma _____.

TEKST SMS PORUKE: Opasnost je završila. Možete krenuti u aerodromsku zgradu kako biste nastavili svoje putovanje.

HYDROELECTRIC POWER PLANT AREA EVACUATION

WEB/EMAIL/VOICE MAIL TEXT: Immediate evacuation of the residents of _____ (name of place) down the river from HPP dam _____ is necessary due to _____ (reason for evacuation). Remain calm. Follow the instructions issued by first responders and go to the stations where organized transportation is waiting or use your own vehicles. After you leave the area, go to the assembly point for the people evacuated from your area. It is required that you register with the tracking service so that it can be noted that you are safe. Please limit the use of phones so that phone lines can stay open for emergency messages. Standby for updates and keep apprised of any information that we will deliver via HEP website _____ or number 112. Persons from areas not listed for evacuation should remain in place and be alert to changing conditions.

TEXT MESSAGE: Evacuation of residents of _____ (name of place) is necessary. Go to the evacuation assembly point where you will receive information about the areas to be evacuated.

ALL CLEAR

WEB/EMAIL/VOICEMAIL TEXT: The danger caused by the HPP dam _____ has ended. Residents of the evacuated places _____ can start moving toward the assembly points for the organized return and transportation to _____. Please standby for further instructions.

TEXT MESSAGE: The danger has ended. You can start moving toward the assembly points for the organized return or if you have a personal vehicle, you can return to _____. Please standby for further instructions.

AIRPORT EMERGENCY

WEB/EMAIL/VOICEMAIL TEXT: An emergency situation in the airport area: _____ in _____ (place). The area of _____ airport is potentially endangered by a biological agent dangerous for human health. Please take your belongings and leave the indoor spaces of the airport and go out into the outdoor spaces on the parking lot in front of the airport building following the emergency exit lights. Follow the instructions given by the technical staff and keep apprised of any information that we will deliver via public address system and/or go to the airport website _____ for more information and updates on the incident.

TEXT MESSAGE: Evacuation of passengers and all _____ airport staff has begun. Go to the exit and follow instructions given by technical staff.

ALL CLEAR

WEB/EMAIL/VOICE MAIL TEXT: The danger caused by the biological agent at the _____ airport has ended. You can go into the airport building without fear for your safety. The information on the continuance of your journey can be found at the info-points and/or flight information display screens of the _____ airport.

TEXT MESSAGE: The danger has ended. You can return to the airport building so you can carry on your way.