République Algérienne Démocratique et Populaire Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Université A/Mira Bejaia
Faculté des Sciences Exactes
Département Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme Master professionnel en Informatique

Spécialité : Administration et sécurité des réseaux

Thème

Amélioration du système de vidéosurveillance par l'intégration du deep learning au sein de BMT

Réalisé par :
Ouchaoua Nihal
Oudai Melissa

Encadré par :
Mme.BATTAT Nadia
M.MADAOUI Madjid

Devant le jury composés de :

Présidente : Mme. HAMZA Lamia	M.C.B	U.A/Mira , Bejaia.
Examinateur : M. AKILAL Karim	M.C.B	U.A/Mira, Bejaia.
Examinatrice: Mme.YESSAD Nawal	M.C.B	U.A/Mira, Bejaia.
Examinatrice : Mme.TASOULT Nadia	M.C.A	U.A/Mira, Bejaia.

Année universitaire 2024/2025

Remerciement

Avant tout , nous exprimons notre profonde gratitude à DIEU TOUT-PUISSSANT , qui nous a donné la santé , la patience et la volonté nécessaires pour mener à bien ce travail.

Nous tenons à remercier chaleureusement notre encadrante , Mme N.Battat pour ses conseils précieux , son accompagnement constant et sa disponibilité tout au long de ce projet.

Nos sincères remerciements vont également à notre encadrant , M M.Madaoui au sein de l'entreprise BMT , pour son soutien technique , sa confiance et son encadrement professionnel.

Nous exprimons également notre reconnaissance aux membres de jury, pour le temps qu'ils ont consacré à évaluer notre travail , ainsi qu'à l'ensemble du département pour les connaissances et les compétences transmises au cours de notre parcours.

Nos pensées les plus sincères vont à nos familles, pour leur amour , leur patience et leur soutien indéfectible.

Et enfin , un grand merci à nous deux , pour l'esprit d'équipe, l'entraide, la détermination et le travail acharné qui ont fait de ce projet une réussite partagée.

Dédicace

Je dédie ce travail à ma chère famille, pour leur innombrables sacrifices , leur amour inconditionnel et leur encouragement constant , qui m'ont porté tout au long de ce parcours.

A mon frère et ma soeur , pour leur précieux conseils et leur présence bienveillante.

A mes amies, pour leur soutien fidèle, et leurs mots qui ont toujours su m'encourager même dans les moments difficiles.

A ma binôme Melissa, avec qui j'ai partagé chaque étape de ce projet, chaque doute et chaque victoire.Merci pour ta confiance, ta force et ta complicité.

Et enfin, à toute ma promotion une génération inoubliable avec qui j'ai grandi , appris, ri, pleuré et évolué durant cette belle aventure humaine. Vous resterez à jamais gravés dans ma mémoire.

Nihal.

Dédicace

Je dédie ce mémoire, fruit de longs mois de travail, de persévérance et de dévouement, à toutes les personnes qui ont été à mes côtés tout au long de cette aventure.

Tout d'abord, je rends un hommage sincère à mes chers parents. Leur amour inconditionnel, leur patience et leurs innombrables sacrifices ont toujours été la source de ma motivation. Qu'Allah les protège et leur accorde santé, bonheur et longue vie.

Je dédie également ce travail à toute ma famille, à ma sœur ,mon frère et à ma tante , pour leur soutien moral et leurs encouragements permanents.

Je pense aussi à mes meilleures amies , qui ont toujours su m'apporter leur soutien, leur bonne humeur et leurs précieux conseils dans les moments difficiles.

Une dédicace toute particulière à ma binôme Nihal, une personne formidable avec qui j'ai partagé cette aventure.
Je te remercie sincèrement pour ton sérieux, ta patience, ton implication et ton esprit d'équipe. Ton soutien et ta collaboration ont grandement facilité la réalisation de ce projet. Ce fut un véritable plaisir et un honneur de travailler à tes côtés.

Je tiens également à remercier mes enseignants et mon encadrant pour leur disponibilité, leur encadrement et leurs conseils avisés qui ont permis l'aboutissement de ce travail.

Merci infiniment à vous tous.

Melissa.

Résumé

La vidéosurveillance joue aujourd'hui un rôle essentiel dans la protection des personnes et des biens, que ce soit dans les espaces publics ou privés. Toutefois, les systèmes traditionnels de vidéosurveillance présentent des limites importantes, notamment la nécessité d'une surveillance humaine continue et leur exposition croissante aux cybermenaces. Dans ce contexte, ce mémoire s'inscrit dans une démarche d'amélioration du système de vidéosurveillance de l'entreprise Béjaïa Méditerranéen Terminal (BMT), en proposant une solution basée sur l'utilisation des techniques d'apprentissage profond (deep learning). L'objectif de ce travail est : d'une part, automatiser la détection des comportements anormaux dans les flux vidéo afin de réduire la dépendance à l'intervention humaine et d'améliorer la réactivité face aux événements critiques ; d'autre part, renforcer la détection des logiciels malveillants (malwares) susceptibles d'échapper aux outils de sécurité traditionnels, contribuant ainsi à une meilleure protection du système d'information de l'entreprise.

Les résultats obtenus ont permis de démontrer l'efficacité de la solution proposée. Grâce à l'intelligence artificielle, le système peut détecter automatiquement des comportements suspects et des malwares, ce qui améliore la sécurité globale de l'entreprise tout en réduisant la charge humaine.

Mots clés : Vidéosurveillance, Sécurité, Cybersécurité, Deep learning, Malwares, Comportements anormaux, Intelligence artificielle, Détection automatique, Système d'information, Analyse vidéo.

Abstract

Video surveillance today plays an essential role in the protection of people and property, whether in public or private spaces. However, traditional video surveillance systems have significant limitations, particularly the need for continuous human monitoring and their increasing exposure to cyber threats. In this context, this thesis is part of an effort to improve the video surveillance system of the company Béjaïa Méditerranéen Terminal (BMT), by proposing a solution based on the use of deep learning techniques. The objective of this work is: on the one hand, to automate the detection of abnormal behaviors in video streams in order to reduce reliance on human intervention and improve responsiveness to critical events; on the other hand, to enhance the detection of malware that may evade traditional security tools, thereby contributing to better protection of the company's information system.

The results obtained have demonstrated the effectiveness of the proposed solution. Thanks to artificial intelligence, the system can automatically detect suspicious behaviors and malware, which improves the overall security of the company while reducing the human workload.

Keywords: Video surveillance, Security, Cybersecurity, Deep learning, Malware, Abnormal behaviors, Artificial intelligence, Automatic detection, Information system, Video analysis.

Table de matières

Table des figures

Liste des tableaux

Liste des abréviations

CCTV : Closed Circuit Television.

EMI : Electromagnetic Interference.

DVR : Digital Video Recorder.

NVR : Network Video Recorder

PTZ : Pan-Tilt-Zoom.

TCP/IP : Transmission Control Protocol / Internet Protocol.

IP : Internet Protocol.

IoT : Internet of Things (Internet des objets).

WLAN : Wireless Local Area Network.

LCD : Liquid Crystal Display

LED : Light Emitting Diode

GSM : Global System for Mobile Communications.

DDOS : Distributed Denial of Service (attaque par déni de service distribué).

BMT : Béjaia Mediterranean Terminal.

DCSASS : Dataset for Complex Scene Abnormality in Surveillance Systems.

CNN : Convolutional Neural Network (réseau de neurones convolutif).

RNN : Recurrent Neural Network (réseau de neurones récurrent).

LSTM : Long Short-Term Memory (mémoire à long terme et court terme).

ConvLSTM : Convolutional long Short-term Memory.

FC : Fully Connected (couche entièrement connectée dans les CNN).

ReLU : Rectified Linear Unit (fonction d'activation dans les réseaux de neurones).

LOSS : Loss Function (fonction de perte).

POOL : Pooling Layer (couche de sous-échantillonnage).

Conv 2d : 2D Convolutional Layer.

IA : Intelligence Artificielle.

4G : 4th Generation (Mobile Network).

Introduction générale

Dans le but de renforcer la sécurité des personnes et des biens publics, les systèmes de vidéosurveillance sont aujourd'hui largement déployés dans divers espaces publics et privés tels que les entreprises, les gares, les aéroports , les hôpitaux, les marchés, les établissements scolaires et les centres résidentiels. L'objectif principal de ces systèmes est de prévenir et de contrôler les risques liés à la sécurité publique en détectant, de manière rapide et précise, les événements anormaux.

L'une des entreprises ayant adopté ce type de système de surveillance est BMT : Béjaïa Méditerranéen Terminal SPA, au sein de laquelle nous avons effectué notre stage de fin d'études. Cette expérience nous a permis d'identifier deux problématiques majeures.

La première est directement liée aux limites des systèmes de surveillance traditionnels. En effet, la surveillance continue des flux vidéo représente une tâche fastidieuse et difficilement soutenable à long terme, notamment à un rythme soutenu. Cela conduit à une utilisation inefficace des caméras de surveillance et impose une présence humaine constante. Ce type de tâche requiert non seulement un temps considérable, mais aussi une vigilance et une concentration permanentes de la part des agents de sécurité, ce qui n'est pas toujours réalisable.

La seconde problématique concerne la cybersécurité. Le système de vidéosurveillance déployé au sein de cette entreprise peut être exposé à des menaces croissantes liées aux attaques de logiciels malveillants (malwares). Ces attaques exploitent des techniques avancées telles que l'injection de code, le débordement de mémoire tampon, la réutilisation de ports ou encore les attaques collaboratives. De plus, les attaquants utilisent des méthodes d'obfuscation sophistiquées, telles que la permutation ou la réorganisation de code, afin d'échapper aux outils de sécurité classiques. Ces malwares peuvent non seulement perturber le bon fonctionnement des systèmes de vidéosurveillance, mais également compromettre les trois piliers fondamentaux de la sécurité informatique :

- **La disponibilité** : par la suppression des vidéos stockées.
- **L'intégrité :** par la modification des enregistrements vidéo.

- **La confidentialité :** en portant atteinte à la vie privée et à la protection des données sensibles.

Dans le cadre de notre projet de fin d'études, et afin d'apporter une solution d'amélioration pour l'entreprise BMT, notre contribution consiste à :

- Automatiser la détection des comportements anormaux dans les vidéos de surveillance à l'aide de techniques d'apprentissage profond (deep learning).
- Renforcer la détection des malwares qui échappent aux outils de sécurité conventionnels tels que les antivirus classiques.

La solution proposée vise à améliorer la qualité et la rapidité de détection, à réduire la dépendance à l'intervention humaine, et à limiter l'impact des malwares sur l'ensemble du système.

Pour évaluer l'efficacité de notre approche, nous avons utilisé deux classifieurs de deep learning, chacun appliqué à un jeu de données (dataset) adapté à la problématique traitée. Les résultats de simulation ont montré une amélioration significative en termes de précision et de temps de détection, tout en contribuant à une meilleure résilience face aux menaces informatiques.Le travail est decomposé en 4 chapitres :Généralités sur les systèmes de vidéosurveillance, Présentation de l'entreprise d'accueil BMT, Détection des malwares et des comportements anormaux basée sur le deep learning et finalement la Mise en œuvre de l'approche, expérimentation et analyse des résultats obtenus.

CHAPITRE 01

Généralités sur les systèmes de vidéosurveillance

1.1 Introduction

À l'heure actuelle, le monde se révèle être de plus en plus complexe dans ses structures et ses interactions. Cela entraîne une hausse du nombre d'incidents tragiques, qu'ils soient accidentels ou intentionnels. En revanche, les entreprises sont également plus strictes en matière de sécurité et de prévention, utilisant les progrès technologiques pour satisfaire ces exigences de la manière la plus efficace possible.

Ainsi, la vidéosurveillance s'est imposée de façon omniprésente et connaît actuellement une importante progression, à la fois d'un point de vue technologique et économique. Elle s'est imposée comme un aspect essentiel des stratégies de sécurité gouvernementales, on l'observe dans une multitude de domaines (secteur bancaire, transport, industrie, grande surface, etc.) ou espaces de vie (villes, bâtiments professionnels, infrastructures publiques, etc.) pour satisfaire les demandes et les nécessités de l'utilisateur.

Dans ce chapitre, nous définirons le système de vidéo surveillance, expliquerons certains concepts utilisés dans ce domaine, et présenterons les avantages de ce système dans notre vie quotidienne, son évolution et les différents domaines d’application.

1.2 Le système de la vidéo-surveillance

1.2.1 Définition

La vidéosurveillance consiste à placer des caméras dans un lieu public ou privé et implique l'utilisation d'un ensemble de caméras, d'écrans et d'interfaces vidéo pour surveiller une ou plusieurs scènes et détecter des comportements particuliers jugés inappropriés ou susceptibles de signaler la présence ou l'existence de comportements indésirables .[1]

1.2.2 Evolution de la vidéosurveillance

Les systèmes de vidéosurveillance sont en place depuis approximativement un quart de siècle. À leurs débuts, ils étaient complètement analogiques, mais ils se dirigent

progressivement vers l'adoption de la technologie numérique. Les systèmes modernes ont peu de similitudes avec les anciennes caméras analogiques connectées à des magnétoscopes classiques. Actuellement, ils se servent de caméras IP et de serveurs informatiques pour l'enregistrement vidéo dans un système entièrement numérique. Cependant, il reste une gamme de solutions partiellement numériques qui intègrent divers composants digitaux en quantité variable .[2]

L'évolution a connue 3 principales périodes :

1.2.2.1 Systèmes de vidéosurveillance classique CCTV

Un système traditionnel de vidéosurveillance CCTV, basé sur des caméras analogiques dotées de sorties coaxiales, est connecté au moniteur.Un opérateur doit constamment être devant l'écran pour la supervision et l'intervention en cas d'anomalies, Comme illustré à la figure 1.1.[2]

Avantages :

- Installation très facile et non professionnelle.
- La manipulation des données est assez facile et accessible à toute personne.

Inconvénients :

- Cette surveillance a un champ d'action très restreint.
- Il est nécessaire de programmer un opérateur pour effectuer le contrôle.
- Pas de déclenchement de surveillance.

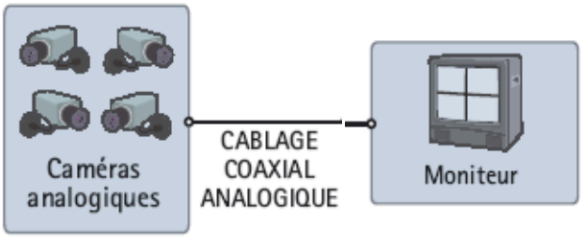


Figure 1.1 : Systèmes de vidéosurveillance classique CCTV.

1.2.2.2 Systèmes de vidéosurveillance analogique avec magnétoscopes traditionnels

Un système de vidéosurveillance analogique, intégrant un magnétoscope classique , est un dispositif entièrement analogique où les caméras analogiques dotées de sorties coaxiales sont connectées au magnétoscope pour effectuer l'enregistrement .[2]

Comme illustré à la figure 1.2.[2]

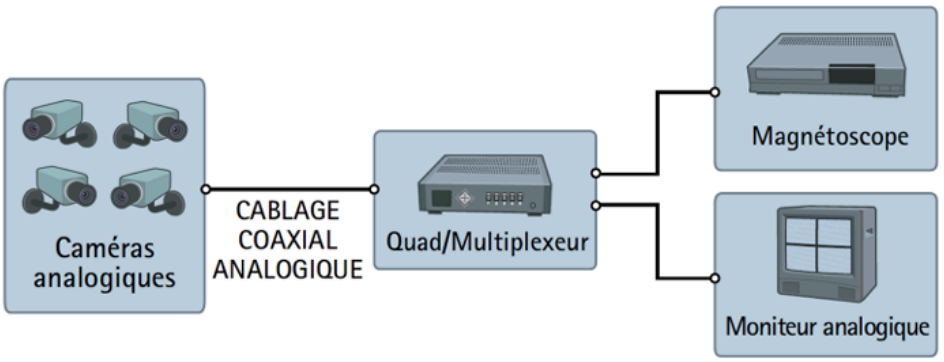


Figure 1.2 : Systèmes de vidéosurveillance analogique avec magnétoscopes traditionnels

1.2.2.3 Systèmes de vidéosurveillance analogique avec enregistreurs numériques

De nos jours encore, le système de vidéosurveillance analogique demeure le plus répandu dans les entreprises, boutiques et résidences privées. Il est doté de caméras analogiques qui ont pour seule fonction de prendre des images et de les transmettre à un enregistreur à durée limitée via un signal analogique. Cela exige des liaisons par câble coaxial à l'enregistreur digital pour chaque caméra et des connexions distinctes par câble pour l'alimentation .[3]

Comme illustré à la figure 1.3.[2]

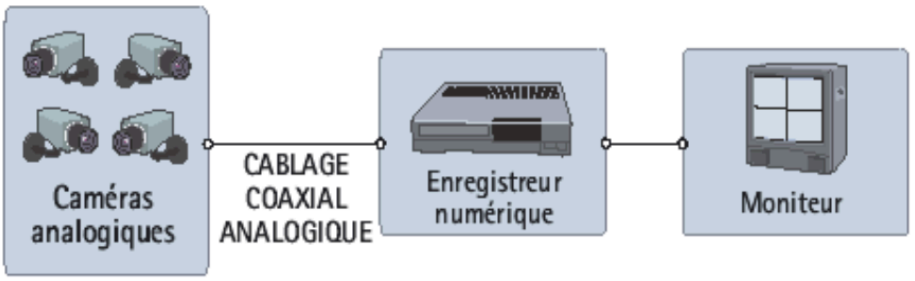


Figure 1.3 : Système de vidéosurveillance analogique avec enregistreur numerique

1.2.2.4 Systèmes de vidéosurveillance analogique avec enregistreurs numériques réseau

Un dispositif de vidéosurveillance analogique qui utilise un enregistreur numérique réseau (DVR) constitue un système partiellement numérique intégrant un enregistreur numérique réseau, connecté par l'intermédiaire d'un port Ethernet.Après avoir été numérisée et compressée sur l'appareil d'enregistrement

numérique, les séquences peuvent être transférées via un réseau informatique pour une surveillance à distance sur PC.[3]

Comme illustré à la figure 1.4.[2]

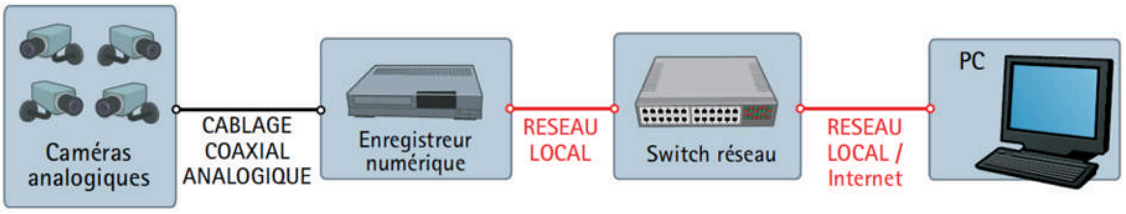


Figure 1.4 : Système de vidéosurveillance analogique avec enregistreur numérique réseau

Certains enregistreurs numériques possèdent un port RG45, ce qui lui permet de transmettre les images directement sur un réseau informatique et de les visualiser sur un ordinateur.

1.2.2.5 Système de vidéosurveillance IP

C'est le système de vidéosurveillance en vigueur actuellement. Contrairement aux systèmes de vidéosurveillance analogiques, la vidéosurveillance IP, entièrement numérique, utilise des caméras réseau qui peuvent convertir les signaux électriques en séquences binaires et les transmettre via le réseau informatique à l'aide du protocole TCP/IP.

La vidéosurveillance IP permet aux utilisateurs d'obtenir à tout instant et en tout lieu des informations sur une opération en cours, et de la suivre en temps réel.

1.2.3 Avantages et inconvénients d'un système de vidéosurveillance

L'usage des systèmes de vidéosurveillance s'est progressivement élargi dans différents environnements, y compris les lieux publics, les sociétés et les domiciles. Bien qu'ils aient de nombreux atouts, ils comportent également certains désavantages. Voici une énumération des avantages et des inconvénients de la vidéosurveillance :

1.2.3.1 Avantages

- Dissuasion des malfaiteurs potentiels afin qu'ils réfléchissent à deux fois avant de s'engager dans des actions illégales.
- Contrôle en temps réel.
- Renforcer la sécurité de vos biens.
- Collecte de preuves dans le cadre de procédures judiciaires ou d'enquêtes.
- Accès à distance.
- Amélioration de l'efficacité opérationnelle (contrôler la productivité des employés).
- Intégration à d'autres systèmes de sécurité.

1.2.3.2 Inconvénients

- Porter atteinte à la vie privée.
- Considérations d'ordre juridique et éthique.
- l'installation et l'entretien d'un système de vidéosurveillance peuvent engendrer des frais importants.
- Risques de cybersécurité et de fiabilité.
- Mauvaise utilisation potentielle.

1.3 Architecture d'installation de vidéosurveillance

1.3.1 Vidéosurveillance en circuit fermé et circuit ouvert

- **Vidéosurveillance en circuit fermé ou CCTV :**

  Dans un dispositif de vidéosurveillance en circuit fermé (aussi connu sous le nom de CCTV ou Closed Circuit Television), le système se compose d'un ensemble de caméras et de moniteurs qui appartiennent à une entité ou une organisation dont l'objectif n'est pas de partager les images en dehors de ses locaux. Seul celui qui est connecté au réseau s'intéresse à l'émission et la réception.[2]

  Comme illustré à la figure 1.5.[2]

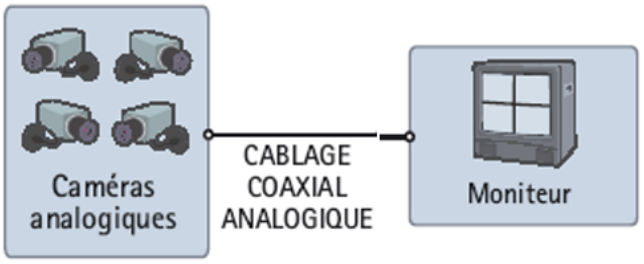


Figure 1.5 : Vidéosurveillance en circuit fermé ou CCTV

- **Vidéosurveillance en circuit ouvert ou OCCTV :**

  Un système de vidéosurveillance a pour fonction précise d'assurer la sécurité d'un lieu spécifique. Il est tout à fait justifié que l'utilisateur puisse accéder à son système de manière sécurisée, surtout s'il désire une gestion multi-site. Dans ce domaine, des avancées ont été réalisées grâce aux technologies en matière d'électronique, d'informatique et de télécommunications. L'expression OCCTV (Télévision en circuit ouvert et fermé) a été inventée pour caractériser ce genre d'application. L'émergence de ce genre d'installation est liée à l'avènement de l'internet, et plus particulièrement de l'internet haut débit.[2]

1.3.2 Les fonctions d'une installation

Dans un système de vidéosurveillance, on retrouve constamment trois fonctions essentielles et liées entre elles : réception, gestion, visualisation .[4]

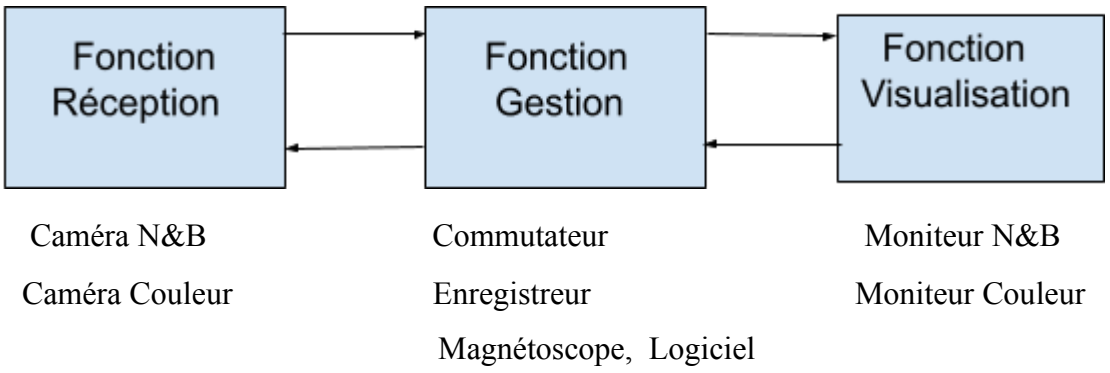


Figure 1.6 : Synoptique d'une installation de vidéosurveillance

1.3.2.1 Fonction de réception

La caméra constitue l'élément essentiel du système de vidéosurveillance. Selon le contexte et les exigences de l'utilisateur, il sera nécessaire de sélectionner l'équipement approprié parmi une vaste sélection de caméras :

- ➢ des caméras couleur ou noir et blanc
- ➢ des caméras haute définition
- ➢ des caméras fixes, mobiles, discrètes
- ➢ des caméras intérieures ou extérieures et de l'environnement (éclairage, champ électrique, etc.)

1.3.2.2 Fonction de gestion

Les dispositifs de gestion offrent la possibilité, selon les exigences d'utilisation, de projeter une ou plusieurs images sur un ou plusieurs écrans.Ce genre de présentation s'effectuera en utilisant divers équipements préétablis lors de l'analyse et répondra aux exigences spécifiées par le client.C'est ici que le tableau de bord pour les caméras mobiles sera incorporé.Dans cette fonction on retrouve les services stockage et traitement des flux vidéo.

1.3.2.3 Fonction de visualisation

Cette fonction est fréquemment combinée avec le rôle de gardien ou au centre de sécurité. Elle s'effectue sur un écran qui constitue le dispositif permettant d'afficher les images obtenues par les caméras de sécurité ou stockées par l'enregistreur de vidéosurveillance. Il est aussi possible de visualiser les données à distance en utilisant un smartphone ou un ordinateur, pour une surveillance sereine.

1.4 Analyse des vulnérabilités des caméras de surveillance

Les caméras de surveillance jouent un rôle important dans la sécurité moderne, mais il n'y a pas d'erreur. Entre le matériel, les logiciels et les faiblesses du réseau, ces appareils peuvent devenir des destinations privilégiées pour les cyberattaques.

1.4.1 Vulnérabilités matérielles

1.4.1.1 Accès physique

- **Manutention directe :** Les caméras peuvent être facilement détruites, séparées ou traitées lorsqu'elles sont installées à une hauteur accessible ou à un emplacement non garanti.
- **Substitution par un appareil malveillant:** L'attaquant remplace les caméras légitimes par des appareils malins et crée des points d'accès secrets pour le réseau.
- **Blocage de la vision :** Parfois - les gens AB peuvent interférer avec l'objectif de la caméra avec des autocollants, de la peinture ou d'autres objets pour le rendre inefficace.

1.4.1.2 Composants obsolètes

- **Technologie dépassée :** Les caméras plus anciennes ne peuvent pas intégrer le chiffrement des matériaux ou les invités Sabota.
- **Durabilité limitée :** Les composants moins résistants au vieillissement, à l'humidité ou aux environnements extrêmes peuvent s'arrêter prématurément.
- **Absence de mises à jour :** Les caméras souvent obsolètes sont abandonnées par les fabricants. Cela signifie que des mises à jour sûres ne sont pas disponibles.

1.4.1.3 Interférences

- **Interférences électromagnétiques (EMI)**: L'EMI est une perturbation causée par des champs électromagnétiques externes qui peuvent affecter les circuits de caméra électronique. Il peut provenir de la nature (foudre, perte de soleil) ou artificiel (moteurs électriques, appareils sans fil).
- **Climats extrêmes:** La température extrême, l'humidité et le mauvais temps peuvent affecter la caméra:
  - ➢ Chaleur excessive : Risque de surchauffe des composants internes
  - ➢ Froid intense : Congélation des circuits ou formation de buée.
  - ➢ Pluie et vent : Risques de court-circuit ou de dommages physiques.
- **Jamming de fréquence:** Le brouillage de fréquence est la perturbation des communications sans fil des caméras connectées (Wi-Fi ou GSM). Cela empêche d'envoyer des vidéos et des avertissements.

1.4.2 Vulnérabilités logicielles

1.4.2.1 Micrologiciel non mis à jour

Le firmware (ou le micrologiciel) est un logiciel embarqué qui contrôle les principales fonctions d'une caméra. S'il n'est pas mis à jour régulièrement, cela peut conduire à

- **Exploitation de failles connues** :Les fabricants publient souvent des mises à jour pour réparer les faiblesses. Si ces mises à jour ne sont pas installées, les pirates ne pourront pas utiliser les défauts qu'ils ont atteints.
- **Backdoors non intentionnelles** : Certaines traces originales contiennent des "portes volées" qui permettent un accès administratif caché.
- **Non-conformité avec les normes récentes** : Les anciens micrologues ne prennent pas en charge les protocoles de sécurité modernes, tels que les algorithmes de chiffrement avancés .[5]

1.4.2.2 Authentification faible

- **Accès non autorisé**

  Si la caméra utilise un mot de passe inférieur ou un mot de passe par défaut, le système de l'attaquant sera facilement accessible.

  - ➢ **Recherche automatisée** : Les pirates utilisent l'outil de numérisation pour trouver des caméras connectées à Internet qui sont connectées à des mots de passe connus ou bas.
  - ➢ **Contrôle complet des caméras** : Une fois l'accès obtenu, les intrus peuvent
    - Voir les flux vidéo en direct et accéder aux archives.
    - Désactiver ou détourner les caméras pour supprimer toute preuve de leurs actions.
    - Modifier les paramètres réseau pour aggraver la vulnérabilité.

- **Utilisation dans des botnets**

  Un botnet est un réseau de dispositifs de compromis utilisés pour effectuer des cyberattaques à grande échelle. Les caméras de surveillance protégées sont les objectifs privilégiés de ces réseaux

- ➢ **Botnet Mirai** :En 2016, Botnet Mirai a été infecté par des millions d'appareils IoT, y compris des caméras qui utilisent des mots de passe standard. Il est utilisé pour effectuer l'une des plus grandes attaques de services distribuées non enregistrées (DDOS), perturbant l'accès à des services critiques tels que Twitter et Netflix.
- ➢ **Propagation rapide** :Dès que la caméra est infectée, le malware scanne et infecte d'autres appareils connectés au réseau, créant une chaîne d'attaque.[6]

1.4.3 Vulnérabilités réseau

1.4.3.1 Transmission non sécurisée

Lorsqu'un le flux vidéo est envoyé sans cryptage, il peut être intercepté par un tiers malveillant.

- **Espionnage:** Les attaquants peuvent visualiser les flux vidéo et affecter la confidentialité de leurs données.
- **Falsification des données:** Le flux vidéo peut changer avec la désinformation et masquer l'activité malveillante.
- **Collecte de données sensibles:** Les images immédiates contiennent des informations sensibles telles que les modèles de sécurité et l'identité de la personne surveillée.[5]

1.4.3.2 Propagation sur le réseau

Une fois qu'une caméra est compromise, elle peut être utilisée comme point d'entrée pour attaquer d'autres appareils dans le même réseau. C'est une formation :

- **Déploiement de logiciels malveillants:** Un malware peut infecter différents systèmes connectés, comme des serveurs ou des ordinateurs
- **Interception des données réseau:** En accédant à la caméra, les intrus peuvent utiliser des données sensibles qui traversent le réseau.
- **Perturbation des opérations:** Les écarts peuvent ralentir ou paralyser l'ensemble du réseau.[6]

1.5 environnement matériel

1.5.1 Dispositifs de vidéosurveillance

- **Caméras de sécurité**
  - ➢ **Caméras analogiques** : Utilisez un câble coaxial pour transférer le signal analogique dans un enregistreur vidéo (DVR).
  - ➢ **Caméras IP** :La connexion à un réseau informatique permet une surveillance à distance sur Internet.
  - ➢ **Caméras HD analogiques** :Développement de caméras analogiques qui offrent une meilleure qualité d'image.
  - ➢ **Caméras thermiques** : Captent la chaleur des objets et des personnes pour une surveillance efficace même dans l'obscurité totale.
  - ➢ **Caméras infrarouges** : Il est équipé d'une Infralot LED pour le tournage avec de mauvaises conditions d'éclairage .
  - ➢ **Caméras motorisées (PTZ)** : Permettent de pivoter, zoomer et suivre des mouvements à distance.
  - ➢ **Caméras dôme** : Protégées par un boîtier en forme de dôme, elles sont discrètes et difficiles à orienter visuellement.
  - ➢ **Caméras bullet** : elles sont cylindriques, souvent utilisées en extérieur pour leur portée étendue.

Selon le mode de connexion et d'alimentation, ces caméras peuvent être filaires , sans fil ou WLAN. Le modèle câblé fournit une connexion stable, tandis que la caméra sans fil fonctionne avec une batterie et est facile à installer. Les caméras WLAN permettent un accès et une gestion à distance via des applications mobiles.[7]

- **Enregistreurs vidéo**
  - ➢ **DVR (Digital Video Recorder) :** Économique,Il utilise souvent des caméras analogiques pour fournir une qualité standard
  - ➢ **NVR (Network Video Recorder)** : Développé pour les dernières caméras IP, il propose des fonctionnalités haute résolution et avancées telles que la détection intelligente.
  - ➢ **Stockage** : Peut inclure des disques durs de grande capacité et des options de sauvegarde sur le cloud.[8]

- **Détecteurs de mouvement**
  - ➢ **Fonctionnement :** Activez l'enregistrement uniquement si le mouvement est reconnu. Cela économise l'espace de stockage.
  - ➢ **Alertes :** Peuvent envoyer des notifications en temps réel via des applications mobiles ou par e-mail.
  - ➢ **Zones de détection** : Des appareils spécifiques vous permettent de configurer des zones spécifiques pour surveiller et éviter les déclencheurs inutiles.[8]

- **Support de transmission**

Pour transmettre le signal vidéo de la caméra vers les dispositifs d'utilisation (comme le moniteur ou le magnétoscope), l'usage du câble coaxial, qui est actuellement le plus couramment utilisé, s'avère indispensable. Cependant Il existe également d'autres méthodes : la fibre optique, les ondes radio, le câble torsadé, etc.

Ainsi, les divers genres de connecteurs employés en vidéosurveillance ont un impact essentiel sur la performance et la fiabilité des systèmes de sécurité. De la prise RJ45, cruciale pour le transfert de données et l'alimentation par PoE, au connecteur en fibre optique, essentiel pour les installations à grande échelle, chaque type de connecteur présente des caractéristiques distinctes conçues pour répondre à des exigences particulières. Une connaissance approfondie de ces connecteurs vous aide à sélectionner les options les plus appropriées pour améliorer votre système de vidéosurveillance IP, en tenant compte des besoins de votre environnement et de vos matériels.

1.5.2 Équipements de visionnage

1.5.2.1 Moniteurs

- **Types de moniteurs**
  - ➢ **Moniteurs LCD ou LED** : Offre une haute résolution pour des images nettes et claires.
  - ➢ **Moniteurs 4K** : Idéal pour les systèmes de caméras haute résolution où on peut voir les plus petits détails.

➢ **Moniteurs tactiles** : utilisé pour interagir directement avec le logiciel de gestion vidéo.

- **Caractéristiques essentielles**
  - ➢ **Taille d'écran** : Les moniteurs de 20 à 32 pouces sont les plus utilisés dans les systèmes de surveillance.
  - ➢ **Multivision** : Ces moniteurs peuvent afficher simultanément plusieurs flux vidéo (mode mosaïque).
  - ➢ **Montage** : Options pour être fixés au mur ou sur des supports ergonomiques pour une meilleure visibilité.

1.5.2.2 Logiciels de gestion vidéo

- **Fonctionnalités principales**
  - ➢ **Lecture en direct et en différé** : Permet de visualiser les images en direct ou de revoir les enregistrements.
  - ➢ **Analyse vidéo intelligente** : Détection de mouvements, reconnaissance faciale ou d'objets.
  - ➢ **Notifications en temps réel** : Alertes envoyées en cas d'événement suspect.
  - ➢ **Gestion des caméras** : Configuration des zones de détection et paramétrage des caméras.
- **Compatibilité**
  - ➢ Compatible avec les systèmes d'exploitation courants (Windows, macOS, Linux).
  - ➢ Accessible via des applications mobiles pour une surveillance à distance.
- **Stockage et sauvegarde**
  - ➢ Fonctionnalités de sauvegarde automatique sur des disques locaux ou dans le cloud.
  - ➢ Options de recherche avancée pour trouver rapidement des séquences spécifiques.[9]

1.5.3 Exemples existants de systèmes de vidéosurveillance

1.5.3.1 Systèmes intelligents

Ces systèmes exploitent l'intelligence artificielle (IA) et des algorithmes avancés pour améliorer la sécurité

- **Détection des comportements suspects** : L'IA peut analyser les flux vidéo pour identifier des activités inhabituelles, comme des mouvements erratiques, des attroupements anormaux ou des comportements potentiellement menaçants.
- **Reconnaissance faciale** : Permet d'identifier des individus spécifiques (par exemple, les employés autorisés ou les personnes figurant sur une liste noire).
- **Suivi automatique** : Les caméras dotées d'IA peuvent suivre un individu ou un objet en mouvement dans un espace donné.
- **Alertes intelligentes** : Notifications en temps réel envoyées au personnel de sécurité lorsqu'une situation anormale est détectée.[9]

1.5.3.2 Systèmes mobiles

Les systèmes mobiles sont conçus pour leur flexibilité et leur adaptabilité.

- **Caractéristiques**
  - ➢ Caméras portables ou déployables rapidement.
  - ➢ Alimentés par batteries ou panneaux solaires pour des environnements sans infrastructure électrique.
- **Utilisations courantes**
  - ➢ Surveillance temporaire lors d'événements, chantiers ou installations temporaires.
  - ➢ Surveillance dans des zones isolées ou difficiles d'accès.
- **Connectivité**
  - ➢ Équipés de connexions sans fil (Wi-Fi ou 4G/5G) pour un accès à distance en temps réel.
  - ➢ Options de stockage local ou cloud pour enregistrer les vidéos.[10]

1.6 conclusion

La vidéosurveillance s'impose comme une réponse stratégique à la complexité croissante de notre monde et à l'augmentation des besoins en sécurité. Grâce à son évolution constante, elle intègre des technologies avancées, permettant d'améliorer son efficacité et son accessibilité dans divers secteurs tels que les banques, les transports, l'industrie, et les espaces publics.

En dépit des défis liés à sa mise en œuvre, notamment les vulnérabilités matérielles, logicielles et réseaux, ainsi que les questions éthiques entourant la vie privée, la vidéosurveillance reste un outil incontournable pour prévenir les incidents et protéger les infrastructures critiques.

Ce chapitre a permis d'explorer ses concepts fondamentaux, son évolution, ses domaines d'application variés, tout en soulignant ses avantages significatifs dans notre quotidien. À l'avenir, avec des technologies en plein essor comme l'intelligence artificielle, la vidéosurveillance promet de s'adapter encore davantage aux exigences croissantes de la sécurité moderne.

CHAPITRE 02

Présentation de l’entreprise d’accueil, BMT.

2.1 Introduction

Ce chapitre se focalise sur la présentation de l'organisme d'accueil BMT , en soulignant sa structure globale et ses objectifs primordiaux. Nous mettrons un accent particulier sur l'architecture réseau existante, où plusieurs enjeux ont été identifiés, surtout en ce qui concerne la performance et la sécurité.Pour finir, des mesures techniques et organisationnelles seront suggérées pour optimiser la performance et la fiabilité de l'infrastructure réseau du BMT.

2.2 Historique de la BMT

Dans son plan de développement 2004-2006, l'entreprise portuaire de Bejaia (EPB) avait inscrit à l'ordre du jour le besoin d'établir un partenariat pour la conception, le financement, l'exploitation et l'entretien d'un terminal à conteneurs au port de Bejaia.Dès lors, l'EPB s'est lancé dans la tâche d'identifier les partenaires potentiels et a arrêté son choix sur le groupe PORTEK qui est spécialisé dans le domaine de la gestion des terminaux à conteneurs. Le projet a été présenté au conseil de participation de l'État (CPE) en février 2004. Le CPE a donné son accord au projet en mai 2004.

Sur accord du gouvernement, Bejaia Méditerranéen Terminal Spa « BMT Spa » a vu le jour avec la jointe venture de l'entreprise portuaire de Bejaia (EPB) à 51% et PORTEK une société Singapourienne à 49%.

En 2011 PORTEK Systems and Equipment, a été racheté par le groupe Japonais MITSUI.

Figure 2.1 : Les partenaires de la BMT

2.3 Présentation de BMT

BMT (Béjaia Mediterranean Terminal) est une jointe venture entre l'entreprise Portuaire de Bejaia et Portek Systems & Equipment. EPB est l'autorité portuaire qui gère le port de Béjaïa. PORTEK Systems and Equipment, c'est une filiale du groupe PORTEK qui est un opérateur de terminaux à conteneurs présent dans plusieurs ports dans le monde et également spécialisé dans les équipements portuaires.

BMT Spa « société par actions », c'est une entreprise prestataire de services spécialisée dans le fonctionnement, l'exploitation, et la gestion du terminal à conteneurs du port de Bejaia. Pour atteindre son objectif, elle s'est dotée d'un personnel compétent particulièrement formé dans l'opération de gestion des terminaux à conteneurs. Elle dispose d'équipements d'exploitation des plus perfectionnés pour les opérations de manutention et d'acconage afin d'offrir des prestations de services de qualité, d'efficacité et de fiabilité en des temps records et a des coûts compétitifs. BMT Spa offre ses prestations sur la base 24H/7j.

Le niveau technique mis en place et la qualité des infrastructures et équipements performants (portiques de quai, portiques gerbeurs) font aujourd'hui du port de Bejaia et de BMT Spa, le premier terminal moderne d'Algérie avec une plate- forme portuaire très performante.

2.4 Situation géographique

La BMT est localisée au nouveau quai, dans le bassin sud du port de Béjaïa, cette dernière fournit des services vastes et importants par des infrastructures routières reliant l'ensemble des villes du pays, des voies ferroviaires et d'un aéroport international.

Au niveau national, BMT est située au centre du Nord-est de l'Algérie, sa position géographique est privilégiée, car elle bénéficie de l'une des baies les plus importantes en méditerranée.

BMT SPA se trouve à proximité de la gare ferroviaire, à quelques minutes de l'aéroport de Béjaïa, reliée à la route nationale ce qui facilite le transport de

marchandises conteneurisées de toute nature vers l'arrière-pays et vers d'autres destinations telles que la banlieue d'Alger.

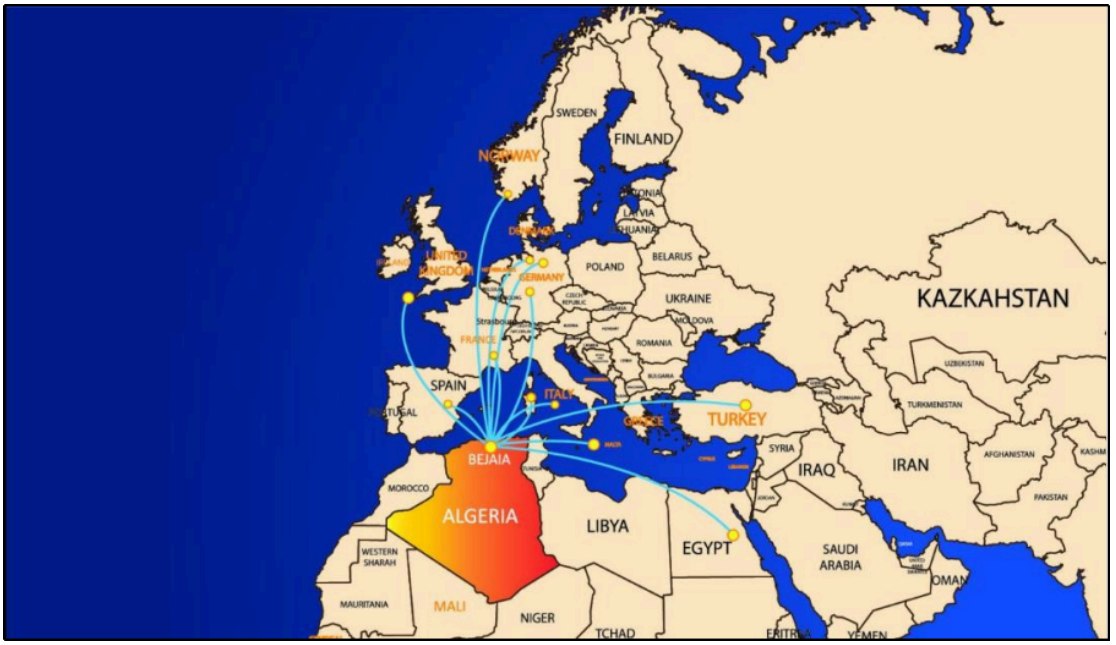


Figure 2.2 : La localisation de l'entreprise BMT

2.5 Structure et organigramme de la BMT

Comme toutes les entreprises, Béjaïa Méditerranéen Terminal dispose un organigramme bien structuré composé d'une direction générale qui se divise en plusieurs sous-directions de différents services comme illustré par Figure 2.3 :

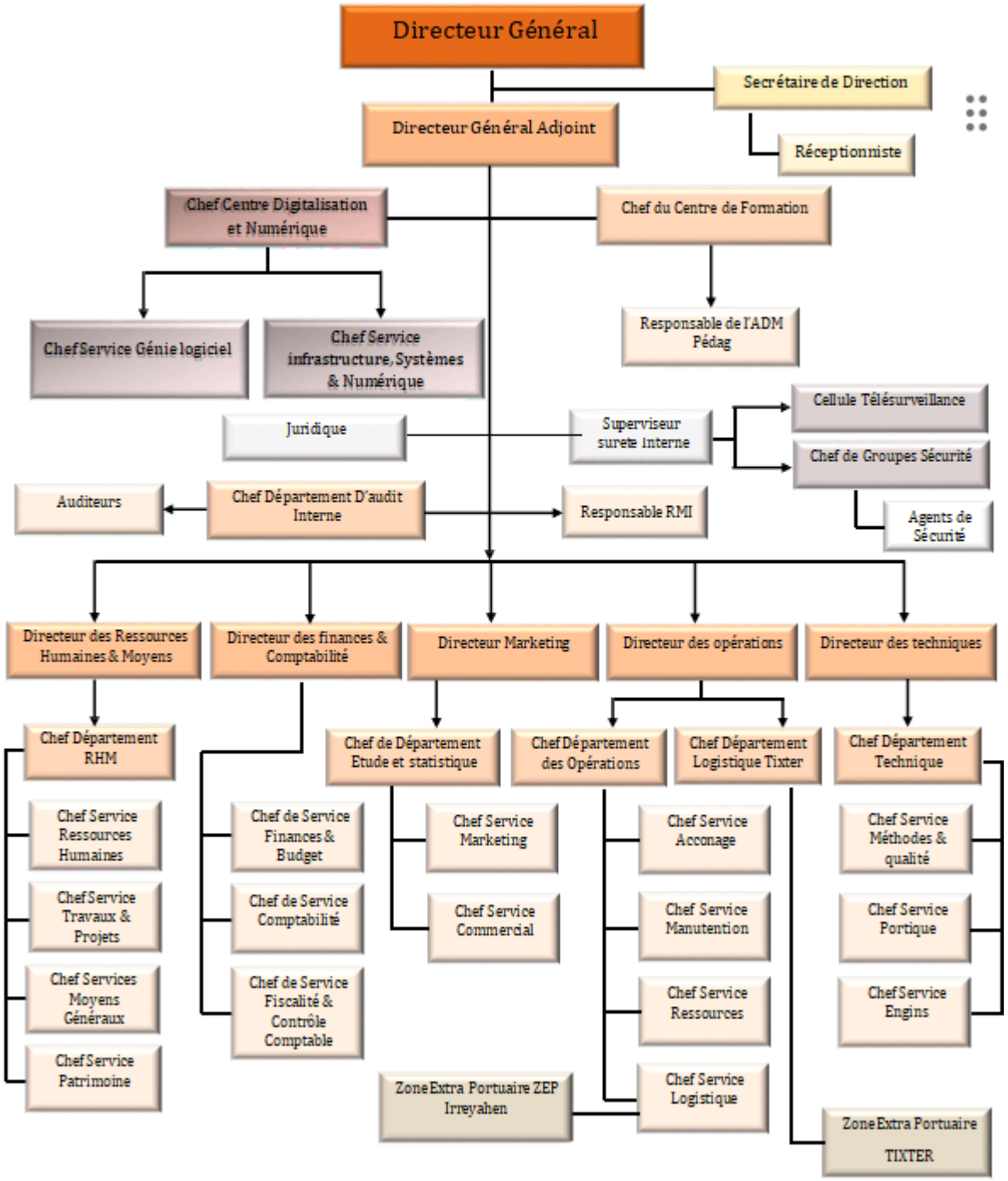


Figure 2.3 : L'organigramme de la BMT

- **Direction générale (DG)**

À sa tête le Directeur Général qui gère la société « BMT-spa », il a pour rôle de définir et de piloter la stratégie globale de l'entreprise et il assigne des directives au Directeur Général Adjoint qui fait la liaison et coordonne entre les différentes directions de l'entreprise.

Les deux éléments suivants font partie à la direction générale :

❖ **Le département audit interne :** Assure l'audit des procédures et mesure leur efficacité.
❖ **Le centre de digitalisation et numérique (CDN) :** Mettre en place un schéma directeur informatique et uniformiser les processus en termes de digitalisation, d'automatisation d'infrastructures informatiques.

➢ **Direction des ressources humaines et moyens (DRHM)**

Elle est directement rattachée à la direction générale, sa mission est de mettre en œuvre des systèmes de gestion intégrés à la stratégie de BMT pour atteindre ses objectifs et qui traduisent une adéquation entre les impératifs économiques et les attentes du personnel. L'importance de cette structure réside dans la recherche de meilleurs potentiels, les conserver en leur offrant les meilleures conditions (climat de travail, environnement, développement des compétences et formations adéquates).

Cette direction se compose de quatre principaux services qui sont :

- **Le Service Ressources Humaines :** Assure la gestion administrative du personnel et le développement des compétences.
- **Le Service Projet et Travaux :** Assure la réalisation et la gestion des travaux et le suivi des projets.
- **Le Service Moyens Généraux :** Satisfaire les besoins des différentes structures en produits et prestations de services.
- **Le Service de Patrimoine :** Assure la gestion des stocks et des immobilisations.

➢ Direction des finances et comptabilité (DFC)

La direction des finances et de la comptabilité est le domaine de la finance relatif aux décisions financières d'une entreprise. Elle a pour principal rôle : établir et suivre les budgets et les plans de financement. Déterminer, rechercher et négocier les financements les plus appropriés en relation avec les établissements concernés. Élaborer le bilan et autres états financiers et comptables et établir et analyser le bilan de fin d'année.

Cette direction est composée de deux services essentiels :

- **Le Service chargé des Finances et Budget :** Assure la gestion de la trésorerie et le suivi de l'exécution du budget de la société et de la comptabilité analytique.
- **Le Service chargé de la comptabilité :** Procède au contrôle et à l'enregistrement de toutes les opérations de la société (achat, vente, investissement, etc.).

➢ Direction marketing (DM)

La direction Marketing est restructurée récemment après la jonction des trois départements (commercial + Marketing + Informatique). Elle a pour rôle, l'analyse du marché, les produits et le service demandé par les clients. Cette direction est chargée d'étudier, d'analyser et d'évaluer les offres de la concurrence et de la date de l'arrivée des nouveaux produits sur le marché. Cependant, la direction marketing se compose de :

- **Service Marketing :** assure la promotion de l'image de marque de l'entreprise et la mise en œuvre du plan marketing et commercial.
- **Service Commercial :** procède à la facturation des prestations fournies et le recouvrement des créances.

➢ Direction des opérations (DO)

Appelée aussi direction du management des activités. Elle assure la planification des escales, du parc à conteneurs et la planification des ressources et des équipements. Elle prend en charge les opérations de manutention, comme la réception des navires porte-conteneurs, leurs chargements et déchargements. De plus, elle suit les opérations de l'acconage tel que : le suivi des livraisons, dépotages, restitutions du vide et le traitement des conteneurs frigorifiques.

Elle se compose de quatre services :

- **Le Service Ressources :** Assure une meilleure affectation des ressources humaines et matérielles.
- **Le Service Logistique :** Assure le suivi des moyens logistiques ainsi que la prestation logistique globale.
- **Le Service Acconage :** Assure la gestion des opérations au niveau du terminal.
- **Le Service Manutention :** Assure la gestion des opérations aux navires.

➢ Direction des techniques (DT)

C'est la direction qui s'occupe de la stratégie industrielle, sa mission principale est la programmation des équipements. La mise en place des programmes sur un plan technique. La recherche et l'amélioration de qualité de travail et d'exploitation des équipements.

Elle se compose de :

- **Service Portique :** assure la maintenance des portiques de quai et des grues mobiles.
- **Service Méthodes et Qualité :** assure la mise en œuvre du plan de maintenance des équipements.

2.6 Objectifs de la BMT

- ➢ Faire du terminal à conteneur de BMT une infrastructure moderne et de répondre aux exigences les plus sévères en matière de qualité dans le traitement du conteneur.
- ➢ La mise à disposition d'une nouvelle technique dans le traitement du conteneur pour :
  - Un gain de productivité.
  - Une réduction du coût d'escale.
  - Une fiabilité de l'information.
  - Un meilleur service des clients.
  - Faire face aux concurrences nationales et internationales.
  - Gagner des parts de marché.
- ➢ Sauvegarder la marchandise des clients.
- ➢ Faire face à la concurrence nationale et internationale.
- ➢ Gagner des parts de marché.

2.7 Les opérations de la BMT

L'activité principale de la BMT est la gestion et l'exploitation du terminal à conteneurs. Sa mission principale est de traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des opérations qui ont un rapport avec le conteneur. Pour ce faire, elle s'est dotée d'équipements performants et de systèmes informatiques pour le support de la logistique du conteneur afin d'offrir des services de qualité, efficaces et fiables pour assurer une satisfaction totale des clients.

Bejaia Méditerranéen Terminal reçoit annuellement un grand nombre de navires pour lesquels elle assure les opérations de planification, de manutention et d'acconage avec un suivi et une traçabilité des opérations.

2.7.1 Opérations de planification

- Planification des escales.
- Planification déchargement/chargement.
- Planification du parc à conteneurs.
- Planification des ressources : équipes et moyens matériels.

2.7.2 Opérations de manutention

- La réception des navires porte-conteneurs.
- Le déchargement des conteneurs du navire.
- La préparation des conteneurs à embarquer.
- Le chargement des conteneurs du navire.

2.7.3 Opérations d'acconage

- Transfert des conteneurs vers les zones d'entreposage.
- Transfert des conteneurs frigorifiques vers la zone « reefers ».
- Mise à disposition des conteneurs aux services de contrôle aux frontières.
- Mise à disposition des conteneurs vides.
- Suivi des livraisons et des dépotages.
- Suivi des restitutions et des mises à quai pour embarquement.
- Gestion des conteneurs dans les zones de stockage.
- Sécurité absolue sur le terminal.

2.8 Présentation du service d'accueil (Centre Digitalisation et Numérique)

2.8.1 Présentation et organisation

Lors de la création de l'entreprise, le service informatique faisait partie de la direction marketing. Quelques années plus tard, l'entreprise a créé un département d'informatique indépendant de la direction marketing et composé de deux sections : section d'étude et développement et section d'exploitation.

En 2021, le département informatique a été remplacé par le centre digitalisation et numérique qui est composé de deux services :

- Service génie logiciel.
- Service infrastructure, système et numérique.

Le centre digitalisation et numérique est un service qui appartient à la direction générale, il met à la disposition des acteurs de BMT les moyens informatiques (matériels, logiciels) permettant la mise en œuvre du système d'information et la gestion des ressources informatique de l'entreprise. De plus, il assure la maintenance

du parc informatique et le développement de nouvelles applications aux différentes structures.

2.8.2 Missions et objectives de centre digitalisation et numérique

Parmi les principales missions et fonctions des deux services, nous citons :

➢ **Service génie logiciel**

- Étude, conception et développement des applications informatiques.
- Suivi des évolutions des applications de gestion existantes.
- Maintenance des logiciels de gestion existante.
- Sécurité des systèmes d'information de l'entreprise.
- Assurer l'évolution du système d'information.
- Sauvegarde et contrôle des données de l'entreprise.
- Administration des serveurs de messagerie et du site web.

➢ **Service infrastructure Systèmes et Numériques**

- Installation et la mise à niveau des systèmes d'exploitation des équipements informatiques.
- Assure l'implémentation des nouveaux systèmes ou des nouvelles versions.
- Garantit le bon fonctionnement des systèmes informatiques et assure la maintenance des équipements.
- Gère le réseau informatique et veille à son évolution et à son optimisation.
- Offre les éléments nécessaires à la sécurité pour l'accès aux données de l'entreprise.
- Garantit la qualité de service (optimisation des performances informatiques, haut taux de disponibilité des applications et systèmes d'exploitation).
- Gère l'administration de l'infrastructure logicielle en surveillant les performances et en apportant les solutions correctives nécessaires.

2.9 Etude de l'existant

2.9.1 Présentation du réseau de la BMT

Le réseau de la BMTspa est un réseau Ethernet qui relie les différents équipements d'un réseau LAN en se basant sur la topologie étoile. La norme de câblage utilisée est T568B selon les types de périphériques à connecter.

Afin de se connecter au réseau Internet, la BMT s'appuie sur le standard de transmission de données sans fil WIMAX (Worldwide Interoperability for Microware Access) pour assurer la transmission des données à haut débit (70Mbit/s) par voie hertzienne en utilisant une fréquence radio privée et sécurisée.

2.9.2 Infrastructure réseau

L'entreprise générale possède deux sites physiques : la BMT qui se trouve au niveau du port de Bejaia et la ZEP (zone extra-portuaire) sur la rue d'Irriyahen Bejaia.

La BMT possède un grand parc informatique composé de trois (03) réseaux :

A. **Réseau local (LAN) :** c'est un réseau Wi-fi et filaire reliant les sites distants par une fibre optique. Il est composé par :
   - **Un serveur de fichier :** Assure le transfert des données à travers un réseau.
   - **Un serveur d'intranet:** Gère les applications de messagerie et d'internet.
   - **Un serveur de caméra :** Gère les caméras de surveillance de l'entreprise.
   - **Un serveur NAS :** Contient plusieurs baies de stockage accessible depuis les postes clients pour le stockage des données.
   - Les postes de travail.
   - **Un switch à 24 ports :** Les serveurs web sont reliés à un Switch auquel sont branchés les postes de travail.

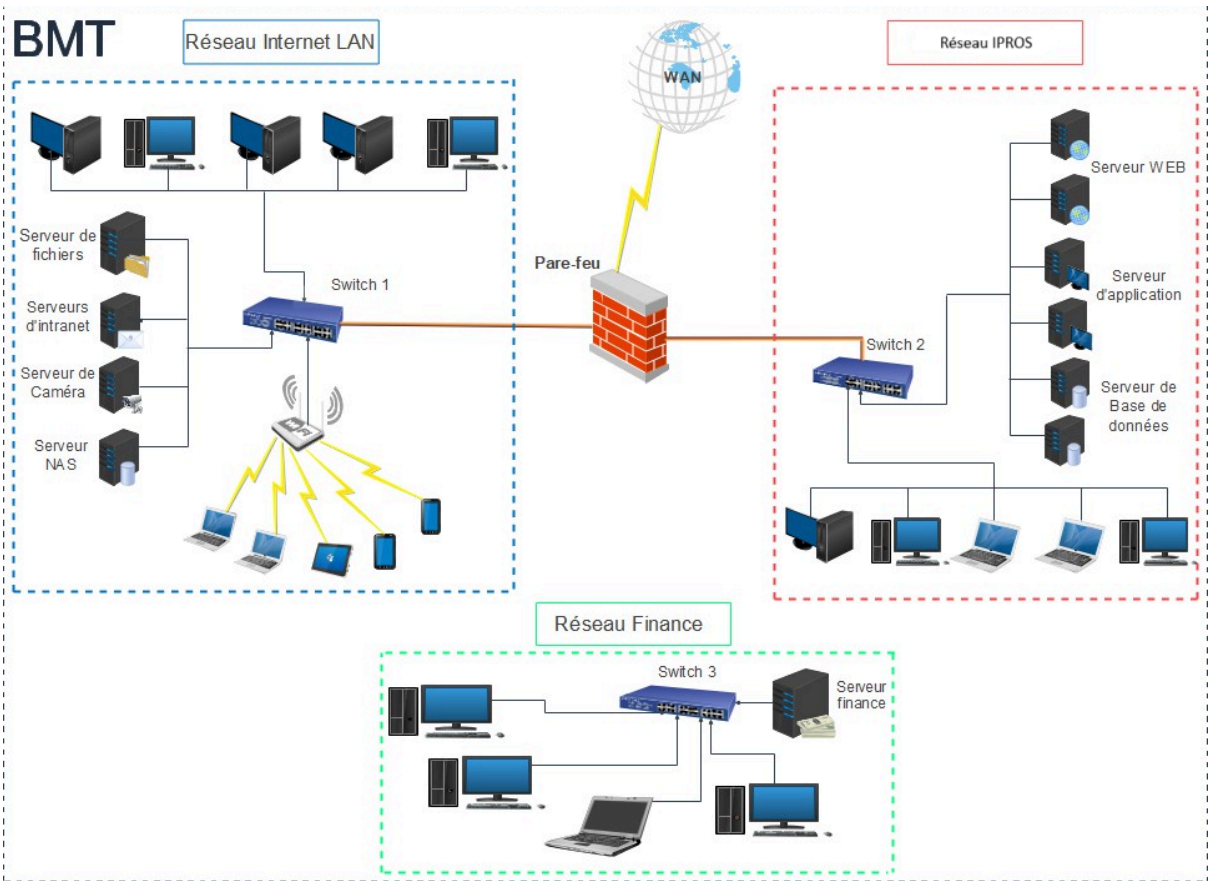
B. **Résseau de production IPROS :** c'est un système de gestion du terminal à conteneurs développé par un prestataire de services.Ce réseau est basé sur l'architecture client-serveur qui assure la gestion des activités opérationnelles (regroupe les domaines navires, conteneurs, etc.) et fonctionnelles (tout ce qui concerne la gestion des ressources humaines, et du parc auto).

   Ce réseau principal de l'entreprise est composé de :

- Deux serveurs de bases de données Oracle.
- Deux serveurs d'applications TOMCAT.
- Deux serveurs web Apache.
- Les postes de travail.
- Un Switch : auxquels sont branchés les postes de travail et les serveurs.

C. **Réseau finance :** c'est un réseau privé et sensible pour cela, il est complètement isolé de l'internet, et utilisé que pour le service finance et comptabilité. Ce réseau offre l'accès à une dizaine de personnes uniquement pour garantir la confidentialité des données. Il est composé de :
   - Un switch.
   - Un serveur des finances.
   - Les Postes de travail.

La figure 2.4 ci-dessous montre l'architecture réseau de la BMT :



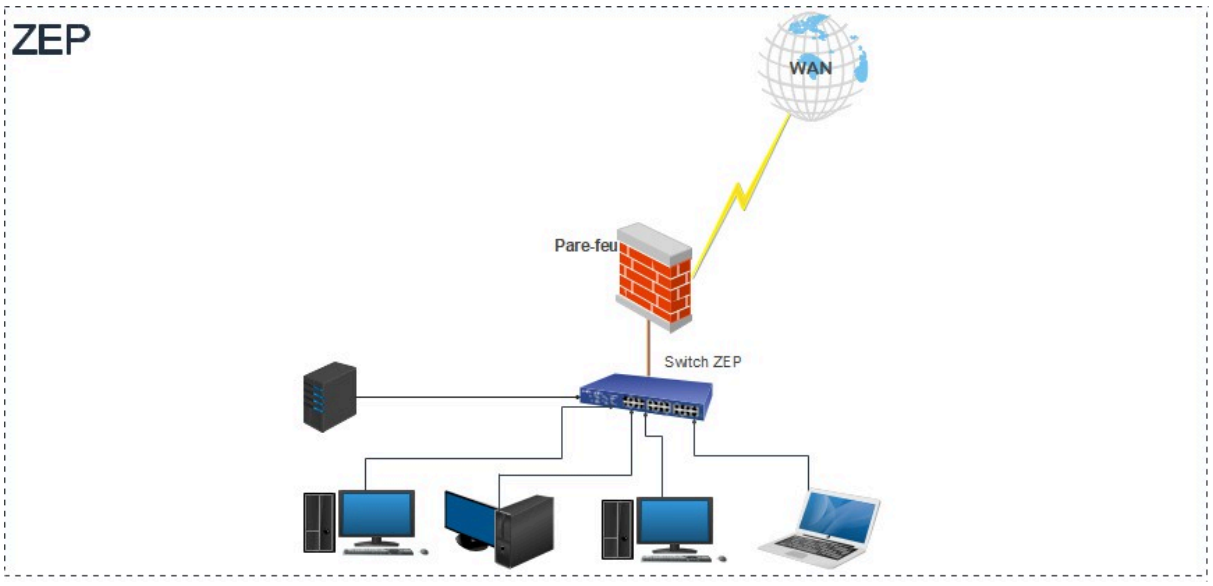


Figure 2.4 : Architecture réseau de la BMT

2.10 Problématique

2.10.1 Description de la problématique

Avec l'essor des systèmes de vidéosurveillance, il devient impératif d'intégrer des techniques capables d'assister efficacement les opérateurs humains. Les systèmes traditionnels présentent en effet des limites notables, notamment en termes de charge cognitive et de temps de réaction. La détection manuelle des comportements anormaux peut s'avérer insuffisante face à la quantité croissante de flux vidéo à analyser en temps réel, nécessitant une concentration élevée et soutenue de la part des agents. Cette situation peut entraîner des retards dans la prise de décision et une inefficacité dans la prévention des incidents critiques.

Au sein de l'entreprise Béjaïa Méditerranéen Terminal (BMT), il apparaît donc nécessaire de déployer des solutions avancées capables d'améliorer le système de surveillance existant. Ces solutions devraient permettre de détecter de manière automatique les comportements suspects ou dangereux, tout en réduisant les délais de détection et le taux d'erreurs humaines.

Parallèlement à ces défis opérationnels, l'architecture actuelle du réseau présente également des vulnérabilités importantes face aux logiciels malveillants, qu'ils soient introduits intentionnellement ou non. En effet, l'accès distant au serveur central de vidéosurveillance, mis en place pour des raisons de continuité de service et de gestion centralisée des flux provenant de plusieurs points de contrôle, constitue une faille de sécurité si cet accès n'est pas strictement sécurisé. De plus, cette vulnérabilité est aggravée par l'incapacité des outils de sécurité traditionnels, tels que les antivirus classiques, à détecter des malwares de plus en plus sophistiqués, utilisant des techniques de camouflage avancées, telles que l'obfuscation et la permutation de code, afin d'échapper aux systèmes de détection conventionnels.

Ces malwares peuvent gravement compromettre la sécurité du système : atteinte à la confidentialité des vidéos enregistrées, altération ou suppression de données critiques, dysfonctionnements des serveurs, et exploitation des serveurs de vidéosurveillance comme points d'entrée pour infiltrer des systèmes internes sensibles. Dans des environnements

interconnectés, où plusieurs réseaux locaux sont liés sans cloisonnement adapté, la menace devient encore plus grave et expose l'intégralité du système d'information à des attaques majeures.

L'absence de mécanismes avancés et robustes de détection des intrusions, ainsi que le manque de segmentation du réseau, augmentent considérablement la surface d'attaque et diminuent la résilience des systèmes face aux cybermenaces modernes. Il ne s'agit donc pas de simples défauts de configuration, mais bien d'une problématique structurelle qui remet en question la sécurité globale des infrastructures.

Par ailleurs, ces défis techniques s'accompagnent de contraintes juridiques et éthiques incontournables :

- **Sur le plan juridique :** Les réglementations en vigueur, notamment le Règlement Général sur la Protection des Données (RGPD) et les lois locales applicables, imposent une protection rigoureuse des données personnelles capturées par les systèmes de vidéosurveillance, telles que les visages et les plaques d'immatriculation. Toute faille susceptible de permettre un accès non autorisé à ces données constitue une violation des droits des personnes concernées et expose l'entreprise à des sanctions légales. Les organisations ont également l'obligation légale de sécuriser l'accès à leurs systèmes critiques.
- **Sur le plan éthique :** Les entreprises doivent veiller à ce que l'utilisation des données issues de la vidéosurveillance respecte strictement la vie privée et soit limitée à des finalités légitimes. Un système vulnérable, mal configuré ou détourné de son usage initial peut entraîner des abus de surveillance, compromettant la confiance des parties prenantes. Les organisations portent ainsi une responsabilité morale dans la protection des données sensibles et dans la prévention de leur exploitation malveillante.

Face à ces défis techniques, juridiques et éthiques, il devient indispensable de mettre en place des solutions avancées capables de :

- Détecter automatiquement les comportements humains anormaux dans les flux vidéo, avec précision et rapidité.

- Identifier les malwares sophistiqués, souvent indétectables par les outils de sécurité traditionnels.

2.11 Contribution

Dans le cadre de ce projet, notre contribution principale consiste à améliorer le système de vidéosurveillance de l'entreprise BMT en développant un système de détection automatique des comportements anormaux et des malwares, reposant sur les techniques avancées de deep learning.

Premièrement, nous avons conçu un système de détection automatique des malwares basé sur les techniques de visualisation et de classification d'images. Le système de deep learning est alors entraîné pour classifier ces images afin d' identifier des codes malveillants, y compris ceux qui échappent aux antivirus traditionnels grâce à des techniques de camouflage sophistiquées. Ce système peut être utilisé à différentes étapes : lors de la réception de nouveaux fichiers ou flux vidéo, ou après toute manipulation des vidéos stockées.

Deuxièmement, nous proposons la mise en place d'un système de détection automatique des comportements anormaux dans les flux vidéo de surveillance. Ce système vise à surmonter les limites des solutions traditionnelles, notamment la nécessité d'une surveillance humaine continue, qui peut être affectée par la fatigue et l'inattention. L'objectif est d'analyser, en temps réel ou en différé, les séquences vidéo issues des caméras pour détecter automatiquement les comportements suspects ou dangereux. Ce système d'intelligence artificielle peut agir comme un support efficace aux opérateurs en améliorant la rapidité et la fiabilité de la détection, tout en réduisant la charge cognitive.

L'approche proposée contribue à renforcer la sécurité globale du système d'information de BMT à deux niveaux complémentaires :

- Sur le plan informatique, avec une détection avancée des malwares, difficilement identifiables par les solutions classiques.
- Sur le plan visuel, avec une détection efficace des comportements anormaux dans les vidéos.

Ainsi, notre solution permet non seulement d'améliorer la qualité de la surveillance, mais aussi de renforcer la résilience de l'infrastructure face aux menaces cybernétiques modernes,

tout en réduisant la dépendance à la surveillance humaine et aux outils de sécurité traditionnels.

2.12 Conclusion

Ce chapitre a mis en évidence la présentation de Béjaïa Mediterranean Terminal (BMT), soulignant aussi l'importance stratégique de cette infrastructure portuaire et la structuration de ses services d'accueil. Toutefois, l'étude a aussi mis en évidence certaines vulnérabilités au niveau du serveur des caméras de surveillance, exposé à des menaces de cyberattaques et d'intrusions non repérées. Pour résoudre ce problème, une approche axée sur l'incorporation de dispositifs pour détecter les logiciels malveillants et les comportements atypiques apparaît comme une stratégie efficace pour prévenir et contrer les menaces potentielles garantissant par conséquent une protection optimale des données et une surveillance en temps réel.

Cette démarche anticipée a pour objectif d'accroître la robustesse et la sécurité de l'infrastructure, tout en assurant la pérennité des opérations de BMT.

CHAPITRE 03

Détection des malwares et des comportements anormaux basée sur le deep learning

3.1 Introduction

Face à l'augmentation constante des cybermenaces et l'évolution constante de la complexité des attaques, il est devenu crucial de développer des systèmes de sécurité intelligents qui vont au-delà des méthodes traditionnelles fondées uniquement sur la détection par signatures.

Les tâches de sécurité prioritaires pour les utilisateurs individuels et les entreprises. Même une unique attaque peut conduire à une compromission des données et à une perte considérable. Pour améliorer la sécurité de notre infrastructure et minimiser les dangers d'une attaque, nous mettons en place des méthodes de détection d'anomalies en vidéosurveillance basées sur le deep learning .

Ce chapitre expose la démarche de création de la solution suggérée pour l'identification simultanée des comportements anormaux et des malwares et décrit les diverses phases de la création de la solution, qui vont de la sélection des outils et des technologies, à l'élaboration du modèle de détection, en incluant la collecte et le traitement des données, l'entraînement du modèle, l'appréciation de son efficacité, jusqu'à l'intégration finale de l'outil dans un environnement fonctionnel.

3.2 Détection des malwares à l'aide du Deep learning

3.2.1 Introduction à la détection des malwares

Le terme «malicious software», ou logiciels malveillants en français, désigne tout programme ou code nuisible qui peut affecter les systèmes.Les malwares sont employés aussi bien par les hackers que par les gouvernements dans le but de dérober des informations personnelles, financières ou commerciales.[11]

Les cybercriminels exploitent et créent des programmes malveillants à caractère offensif afin de pénétrer les systèmes informatiques visés et réaliser leurs objectifs.A l'inverse ,l'identification des logiciels malveillants repose sur une variété de méthodes et de technologies défensives indispensables pour détecter, interdire et éviter les

conséquences nuisibles liées aux logiciels malveillants. Ces actions de protection couvrent une variété de tactiques, soutenues par une sélection d'instruments ajustés au genre de malware qui a contaminé l'appareil concerné.

3.2.1.1 Typologie des malwares

- **Spyware :** se défini comme un programme conçu dans le but de collecter des données personnelles et de les envoyer à son concepteur ou à un tiers via Internet sans avoir obtenu au préalable une autorisation explicite et éclairée des utilisateurs.[12]

- **Cheval de Troie (trojan) :** est un petit programme malveillant d'apparence anodine qui peut causer des dégâts une fois installé, et permet de surveiller ou de prendre le contrôle d'un ordinateur à distance grâce à des portes derobées.[12]

- **Ransomware :** Un programme malveillant qui a le but d'interdire les utilisateurs d'utiliser leur système soit en bloquant l'accès au système soit en chiffrant les données en demandant une rançon.[12]

- **Botnet malware :** un botnet se définit comme un ensemble d'ordinateurs interconnectés par un logiciel malveillant, c'est-à-dire un programme nuisible, qui vise à contaminer des appareils connectés, tels que les caméras de surveillance IP, dans le but de les incorporer à un réseau d'appareils zombifiés nommé botnet. Une fois compromises, ces caméras peuvent être manipulées à distance par un cybercriminel sans que l'utilisateur ne s'en aperçoive.[12]

3.2.1.2 Techniques de détection

Différentes méthodes peuvent être employées par les entreprises pour repérer et examiner les logiciels malveillants au sein de leurs systèmes. On compte parmi les exemples les plus fréquents :

1. **Détection basée sur la signature :** l'identification par signature repose sur des propriétés spécifiques d'un variant de malware pour le reconnaître, comme le

hachage du fichier, les domaines et les IP qu'il sollicite ou encore les séquences de caractères de l'exécutable.Malgré un faible niveau de faux positifs dans la détection des signatures, elle ne parvient pas à repérer les menaces zero-day ni les nouvelles variantes de malwares.

2. **Détection heuristique :** les heuristiques constituent un ensemble de directives permettant de détecter un logiciel malveillant en fonction de son comportement. Une fois ces règles définies, on peut alors identifier un logiciel malveillant qui n'a jamais été observé auparavant, ce qui rend cette méthode plus flexible que la détection par signature.
3. **Détection comportementale :** les malwares ont souvent une conduite atypique, telle que l'ouverture et le cryptage de plusieurs fichiers simultanément. La détection comportementale scrute ces comportements atypiques pour repérer l'existence de malwares sur un système.
4. **Détection basée sur l'intelligence artficielle :** plus précisément l'apprentissage automatique (ML) et profond (DL), bouleverse la méthode conventionnelle de détection des logiciels malveillants. Plutôt que de s'appuyer uniquement sur des signatures statiques, les systèmes d'IA examinent le comportement des fichiers et des processus en temps réel. Cette méthode dynamique facilite l'identification de modèles suspects, même face à des menaces inédites.

3.2.1.3 Pourquoi le Deep Learning ?

L'apprentissage profond, qui s'inscrit dans une catégorie d'approches d'apprentissage machine(ML), a démontré son efficacité dans de nombreuses tâches d'intelligence artificielle par rapport aux méthodes traditionnelles d'apprentissage machine .

Il modifie la manière dont les machines appréhendent, acquièrent des connaissances et interagissent avec des données complexes, il reproduit le fonctionnement des réseaux neuronaux présents dans le cerveau humain.

Dans un réseau de neurones profond totalement connecté, l'information traverse diverses couches, la couche d'entrée est alimentée avec des données qui sont traitées par des couches intermédiaires. Ces dernières opèrent des transformations sur les données à l'aide de fonctions non linéaires et la prédiction du modèle est produite par la couche de

sortie finale.Ceci permet au modèle d'assimiler des représentations complexes des données.[13]

Comme illustré à la figure 3.1.[13]

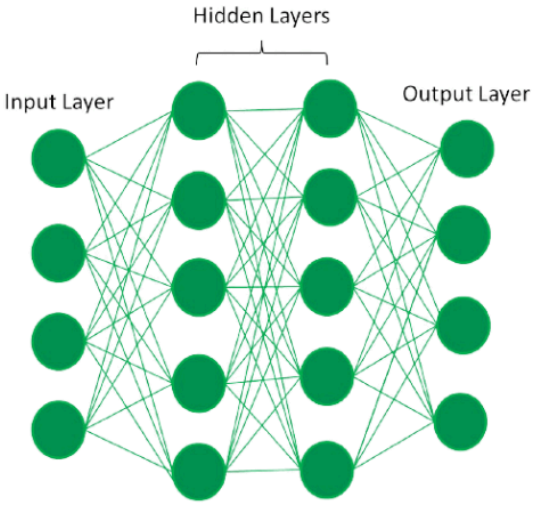


Figure 3.1: Architecture d'un modèle deep learning

3.2.2 Application du Deep Learning en détection de malwares

Il existe de nombreuses applications du Deep Learning que l'on trouve dans divers secteurs :

3.2.2.1 Détection à partir de fichiers binaires

L'analyse binaire pourrait révolutionner la détection des logiciels malveillants en la convertissant en un problème de vision par ordinateur. Dans cette approche, les fichiers sont traités par des algorithmes qui convertissent les valeurs binaires et ASCII en codes couleurs pour la classification malware ou bénin.

3.2.2.2 le traitement automatique de langage naturel

Le traitement automatique du langage naturel est une autre utilisation du DL. Son objectif est d'extraire le sens des mots, voire des phrases, afin de procéder à une analyse de sentiments. Par exemple, l'algorithme sera capable de comprendre le contenu d'un commentaire Google ou d'échanger avec des individus par le biais de chatbots. Le

traitement et l'étude automatisée de textes représentent également une des applications du DL.

3.2.2.3 Détection de malwares à partir d'images

Un des buts de la détection des malwares est d'assurer une lecture, une recherche et une analyse des données de façon efficace et efficiente, et l'identification de malwares à travers des images repose sur l'utilisation de jeux de données qui proposent des représentations visuelles des logiciels malveillants.

Cette méthode se base sur la transformation des fichiers exécutables nuisibles en images en transformant le binaire, octal, hexadécimal ou le décimal en une grille de pixels à deux dimensions. L'image peut être en monochrome (en niveaux de gris) dont les pixels sont des valeurs allant du noir au blanc dans l'intervalle [0-255], où 0 indique le noir et 255 indique le blanc ou bien en couleur RGB.

Comme illustré à la figure 3.2.[14]

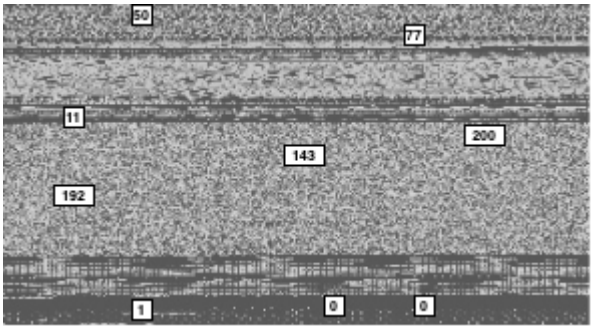


Figure 3.2 : Représentation des fonctionnalités du logiciel malveillant image en niveaux de gris

Ces images sont analysées par des modèles de deep learning,qui est capable de traiter différents types de problèmes liés à la « vision », y compris les tâches de classification d'images de logiciels malveillants .Parmi ces modèles,le CNN proposé par Yuan et al est particulièrement efficace pour catégoriser les malwares en fonction de leurs caractéristiques ou de leurs familles.

3.2.2.3 Métriques d'évaluation et de classification

L'évaluation constitue un aspect crucial de la formation d'un modèle.Selon la problématique à traiter, on dispose de diverses métriques pour juger différentes facettes de notre modèle :

1. Matrice de confusion

Une matrice de confusion, aussi appelée matrice d'erreurs, est un tableau illustrant le nombre de prédictions correctes et incorrectes réalisées par le modèle en comparaison avec les classifications réelles dans l'échantillon test, ainsi que la nature des erreurs commises.

Dans un contexte de classification binaire, on peut visualiser les prédictions du modèle et définir les termes de base de cette façon :

- **Faux positif (fp) :** L'élément a été classé comme positif alors qu'il est négatif.
- **Vrai positif (vp) :** L'élément a été classé comme positif et il est réellement positif.
- **Faux négatif (fn) :** L'élément a été classé comme négatif alors qu'il est positif.
- **Vrai négatif (vn) :** L'élément a été classé comme négatif et il est réellement négatif.

Positif et Négatif fait référence à la prédiction elle-même. Vrai et Faux fait référence à l'exactitude de la prédiction.

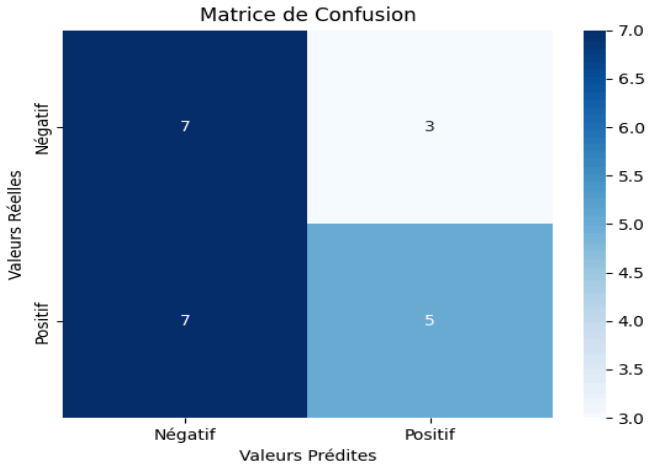


Figure 3.3: Matrice de confusion

2. Accuracy (Précision)

La métrique la plus élémentaire pour l'évaluation du modèle est la précision. Il s'agit du rapport entre le nombre de prédictions justes et le total des prédictions réalisées sur un certain ensemble de données.

Son équation est la suivante :

$$\text{Accuracy} = \frac{vp + vn}{vp + vn + fp + fn}$$

Ou bien :

$$\text{Accuracy} = \frac{\text{Nombre de prédictions correctes}}{\text{Nombre total de prédictions}}$$

La précision est appropriée quand les classes cibles sont équilibrées, mais ce n'est pas un choix judicieux en présence de classes déséquilibrées.Par exemple, un jeu de données qui comporte deux classes cibles de 100 échantillons.

Sur nos données d'entraînement, 98 échantillons sont classés sous la classe A et 2 sous la classe B. Ainsi, notre modèle nous donnerait une précision de 98%. C'est pourquoi il nous faut analyser plus de métriques pour obtenir une meilleure performance.

3. Recall (Rappel)

La proportion de tous les résultats positifs réels qui ont été correctement classés comme tels, est également appelée rappel, il évalue l'aptitude du modèle à identifier les échantillons positifs.

Mathématiquement, le rappel est défini comme suit:

$$\text{Recall} = \frac{TP}{TP + FN}$$

4. F1-score

C'est un indicateur fréquemment utilisé pour évaluer l'efficacité du modèle : il s'agit en fait de la moyenne pondérée de la précision et du rappel. Le score F du classificateur sera élevé uniquement si la précision et le rappel sont aussi élevés. Cette mesure ne privilégie que les classificateurs présentant une précision et un rappel comparables.

Son équation est la suivante :

$$F1 = 2 \times \frac{\text{Précision x Rappel}}{\text{Précision + rappel}}$$

5. Courbe AUC et ROC

La courbe ROC (Receiver Operating Characteristic) est un outil graphique utilisé pour mesurer l'efficacité d'un modèle de classification binaire. Elle représente le taux de vrais positifs (sensibilité) par rapport au taux de faux positifs, pour divers seuils de prise de décision. Plus la courbe tend vers le coin supérieur gauche, meilleure est la performance du modèle.

L'AUC(Area Under the Curve), représente l'espace sous la courbe ROC. Elle offre une mesure globale de performance, indépendante du critère de classification. Un modèle parfait se caractérise par une AUC de 1, alors qu'un modèle aléatoire aurait une AUC de 0,5. Par conséquent, une valeur AUC plus élevée indique une meilleure performance du modèle dans la distinction entre les classes positives et négatives.

Cette métrique est particulièrement pertinente pour effectuer des comparaisons entre plusieurs modèles ou pour juger des modèles sur des jeux de données déséquilibrés.

3.2.3 Réseaux de Deep learning pour la détection des malwares

Le deep learning fait appel à plusieurs types de réseaux, parmi lesquels on distingue les principaux suivants :

3.2.3.1 Les réseaux de neurone convolutif (CNN)

Les réseaux de neurones convolutifs sont des modèles d'apprentissage profond tirés du cortex visuel [Hubel & Wiesel 1962], et sont spécifiquement élaborés pour gérer des données organisées en grille.Ils réalisent une convolution des caractéristiques acquises avec les données d'entrée et font appel à des couches convolutives en 2D, ce qui rend cette structure particulièrement appropriée pour le traitement de données en 2D, comme les images et opèrent en tirant des caractéristiques directement des images.[15]

Un réseau CNN est généralement composé de plusieurs types de couches:

- la couche de convolution (conv).
- la couche de pooling (POOL).
- la couche de correction (ReLU).
- la couche entièrement connectée (FC).
- la couche de perte (LOSS).

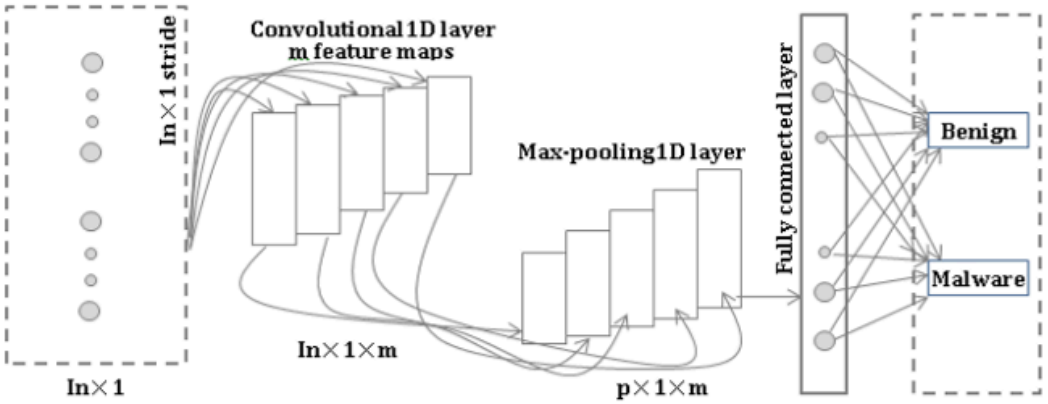


Figure 3.4: Architecture et couches du CNN

3.2.3.2 Réseaux de neurones récurrents (RNN)

On utilise les RNN pour gérer des séries de données, comme les séquences temporelles ou les suites de mots dans un texte et pour traiter des enjeux comme la catégorisation des signaux naturels, le traitement du langage naturel ou l'analyse de vidéos.Ils ont la capacité de maintenir une mémoire interne, ce qui les rend aptes à accomplir des missions telles que la traduction automatique ou la création de contenu textuel.[15][13]

3.2.3.3 Les Autoencoders

Les autoencodeurs constituent une catégorie spécifique de réseau neuronal non supervisé (pas besoin d'étiquette). Le but principal des autoencodeurs est de saisir fidèlement les éléments essentiels des données présentées afin de produire une version condensée des données initiales, créer des données synthétiques crédibles ou détecter des anomalies.[13]

3.2.3.4 Transformers

Les architectures de réseaux de neurones appelées transformateurs ont radicalement modifié l'approche du traitement du langage naturel. Ils sont utilisés pour des missions comme la traduction automatique, la production de texte et la compréhension du langage naturel.[13]

3.3 Détection du comportement humain anormal par Deep learning

3.3.1 Introduction à la détection des comportements anormaux

L'observation des actions d'entités similaires à l'homme et la détection de comportements atypiques qui diffèrent de la norme font partie des anomalies de comportement humain (AHB). Dans le domaine de la vidéosurveillance, les séquences filmées par les caméras fixes sont examinées afin d'identifier de tels comportements et leur détection se focalise majoritairement sur la sûreté et la sécurité publique, en privilégiant le bien-être communautaire. La vidéo de surveillance apporte des éléments visuels essentiels dans un périmètre de vue spécifique pour identifier les comportements humains atypiques.

3.3.1.1 Types de comportements

L'identification de l'AHB est généralement divisée en deux catégories : les comportements anormaux à court terme et les comportements anormaux à long terme, selon la période.

1. **Comportements anormaux à court terme :** désigne des agissements qui dévient de la norme et peuvent être repérés en scrutant une période restreinte d'images vidéo. Des décisions relatives à de tels comportements (la détection d'incendie, la course , la chute, l'encombrement, intrusion et déplacement dans des directions opposées) peuvent être prises sur-le-champ dès que leurs impacts deviennent manifestes en temps réel.
2. **Comportements anormaux à long terme :** L'anomalie du comportement humain sur le long terme désigne des schémas de conduite inhabituelle persistante observés sur une durée prolongée. À l'inverse des comportements atypiques à court terme, il demande une surveillance étendue pour identifier des déviations marquantes par rapport aux modèles de comportement attendus (l'attitude de traîner, l'abandon de sacs

sans surveillance et le manque prolongé d'activité dans certaines zones). Ces derniers peuvent évoluer progressivement avec le temps, exigeant une observation et une étude constantes pour saisir leur impact total.

3.3.1.2 Pourquoi le Deep Learning ?

Au cours des dernières années, l'analyse prédictive du comportement anormal a recours à une diversité d'algorithmes d'apprentissage profond (deep learning) qui présente des bénéfices car il requiert un faible niveau d'ingénierie manuelle, surtout avec l'augmentation de la disponibilité des capacités de traitement et des données, Il offre la possibilité d'extraire de manière automatique des attributs complexes à partir de données non traitées, y compris des vidéos de surveillance. À la différence des techniques classiques qui reposent sur des règles établies manuellement, les réseaux de neurones profonds sont capables d'apprendre à déceler des motifs délicats et temporels dans les gestes ou les positions humaines, même en cas de changements d'éclairage, d'angles de vue ou de perturbations.

Toutefois, un défi majeur réside dans la contrainte liée à la disponibilité des données, communément désignée sous le terme de rareté des données.

3.3.2 Application du Deep Learning

3.3.2.1 Méthodes d'apprentissage

Les méthodes de détection du comportement humain anormal basées sur l'apprentissage profond peuvent être divisées en trois approches : l'apprentissage non supervisé, l'apprentissage partiellement supervisé(faiblement supervisé et semi-supervisé) et l'apprentissage entièrement non supervisé.[14]

1. **Approche non supervisée :** La détection non supervisée se réfère à des méthodes qui reconnaissent des motifs, des irrégularités ou des configurations dans les données sans nécessiter d'échantillons labellisés.Cette méthode est d'une grande valeur, car il est généralement ardu et peu efficace d'obtenir des étiquettes pour divers comportements anormaux. Dans cette catégorie, deux approches largement utilisées sont les techniques fondées sur la reconstruction qui tirent des motifs à partir d'images en

entrée, et les techniques génératives qui s'efforcent de créer une image synthétique et artificielle qu'ils ont assimilée.

2. **Approche partiellement supervisée :** a lieu lorsqu'on dispose de données étiquetées et non étiquetées.Les données étiquetées servent de points d'ancrage pour les phases d'entraînement et de prédiction avec les données non étiquetées.

   Deux approches majeures se dessinent :

   - **La détection semi-supervisée :** Insiste sur la croissance des données étiquetées restreintes accompagnées de données non étiquetées . Le modèle est d'abord entraîné avec des données étiquetées afin de saisir les modèles sous-jacents. Il s'appuie par la suite sur des prédictions de données non étiquetées pour générer des pseudo-étiquettes. On procède ensuite à un nouvel entraînement du modèle en utilisant ce mélange de données étiquetées et pseudo-étiquetées, dans le but d'améliorer la généralisation. On utilise aussi des méthodes comme la régularisation de cohérence et les approches basées sur des graphes pour garantir que le modèle génère des prédictions uniformes et transmet les informations d'étiquette des données étiquetées vers les données non étiquetées.
   - **La détection faiblement supervisée :** Le modèle se base sur des étiquettes moins exactes, plus vagues ou plus sujettes au bruit que les étiquettes entièrement supervisées. On utilise des méthodes comme l'apprentissage d'exemples multiples, où les ensembles d'exemples sont annotés plutôt que les exemples individuels. et les algorithmes de maximisation des attentes qui évaluent les annotations les plus probables tout en optimisant les paramètres du modèle.Des recherches récentes concernant la détection faiblement supervisée de l'AHB ont employé aussi bien des données au niveau vidéo que des données au niveau image.

3. **La détection entièrement non supervisée :** C'est un paradigme dans lequel le modèle est formé pour générer des résultats de détection précis à partir de données d'entrée, il se sert de la précision comme critère principal pour juger l'efficacité du modèle.Généralement, le modèle utilise des couches CNN pour identifier les

caractéristiques locales, qui sont ensuite intégrées dans la couche LSTM afin d'apprendre les relations temporelles entre celles-ci et pour aborder des défis dans le but de capter les caractéristiques temporelles des séquences vidéo.

3.3.3 Réseaux de Deep learning pour la détection des comportements anormaux

En vidéosurveillance, en plus des modèles définis précédemetns des architectures telles que les ConvLSTM sont utilisées pour détecter les mouvements inhabituels :

3.3.3.1 ConvLSTM

Sont des réseaux de mémoire convolutive à long terme composites capables de prévoir la progression d'une séquence vidéo à partir d'un nombre restreint de trames d'entrée(frames).Les scores de régularité sont calculés à partir des erreurs de reconstruction d'un ensemble de prédictions liées à des séquences vidéo anormales, générant ainsi des scores de régularité plus bas étant donné qu'elles s'écartent davantage de la séquence réelle au fil du temps. On effectue une évaluation à la fois qualitative et quantitative des modèles Conv-LSTM, qui montrent des performances concurrentielles sur les jeux de données pour la détection d'anomalies. Les unités Conv-LSTM se sont révélées être un moyen performant pour la modélisation et la prédiction de séquences vidéo.

Le modèle Convolutif LSTM (ConvLSTM) fusionne les potentialités des réseaux convolutifs (CNN), aptes à saisir les liens spatiaux dans les images, et les réseaux LSTM,capables d'assimiler les relations temporelles dans les séquences vidéo.[15]

3.4 Les Data-sets d'évaluation basé sur Deep learning

Un dataset est une collection organisée de données employée pour former, vérifier ou évaluer un modèle d'intelligence artificielle. Selon le secteur d'application, il peut être composé de textes, d'images, de sons, de vidéos ou de données numériques.

L'ensemble de données choisi pour cette étude c'est Malware Detection with images et DCSASS Dataset for Complex Scene Abnormality in Surveillance Systems.

3.5 Conclusion

Dans ce chapitre, nous avons examiné les contributions du deep learning pour l'identification de logiciels malveillants et de comportements humains anormaux dans la vidéosurveillance. Différentes méthodes et structures d'apprentissage approfondi ont été mises en œuvre. Le deep learning, grâce à sa capacité à déduire automatiquement des caractéristiques pertinentes à partir de données complexes telles que les fichiers binaires, les images ou les séquences vidéo, est désormais incontournable dans le secteur de la cybersécurité et de la vidéosurveillance.

CHAPITRE 04

Mise en œuvre de l'approche, expérimentation et analyse des résultats obtenus

4.1 Introduction

Dans ce chapitre, nous traitons la phase expérimentale de cette recherche et détaillons l'application des méthodes de détection dans la vidéosurveillance.

Ce dernier expose minutieusement les jeux de données employés, les phases de préparation des données, les modèles mis en œuvre, ainsi que les résultats obtenus via diverses expérimentations. L'objectif de cette section est d'examiner la pertinence des méthodes précédemment exposées, en se fondant sur des exemples pratiques dans un contexte local.

4.2 Environnement de développement

Dans le domaine de l'apprentissage profond, il est impératif de disposer d'outils puissants et flexibles pour la conception, l'entraînement et le test des modèles. Ce qui nous a conduit vers:

- **Python :** est un langage de programmation interprété, multiparadigue et compatible avec plusieurs plateformes. Il privilégie la programmation structurée impérative, fonctionnelle et orientée objet. Python peut s'utiliser dans de nombreux contextes et s'adapter à tout type d'utilisation grâce à des bibliothèques spécialisées .[16]

- **PyTorch :** est une bibliothèque open-source, robuste et adaptable, qui a conquis les chercheurs et les développeurs pour leurs projets en intelligence artificielle et en science des données.Propose des instruments pour élaborer des architectures sophistiquées de réseaux neuronaux, tels que les réseaux convolutifs (CNN) et récurrents (RNN).[17]

- **TensorFlow :** est un framework open source développé par les chercheurs de Google pour exécuter l'apprentissage automatique et l'apprentissage profond et d'autres charges de travail d'analyse statistique et prédictive sur plusieurs plateformes comme les GPU et les CPU.[18]

- **Keras :** est une API de réseau de neurones développée en Python. C'est une bibliothèque Open Source qui fonctionne au-dessus de frameworks comme Theano et TensorFlow.Destinée à être modulaire, rapide et facile à utiliser, elle propose une méthode simple et intuitive pour la création de modèles de Deep Learning .[19]

- **Sklearn :** est une bibliothèque open-source d'apprentissage automatique offrant des instruments performants et accessibles pour l'analyse et la modélisation des données. C'est un outil puissant pour des tâches comme la classification, la régression, le regroupement et la réduction de dimensionnalité, basé sur NumPy, SciPy et Matplotlib .[20]

- **OpenCV :** constitue une vaste bibliothèque open source dédiée à la vision par ordinateur, l'apprentissage automatique et le traitement d'images. Aujourd'hui, il occupe une position cruciale dans le fonctionnement en temps réel, ce qui est essentiel pour les systèmes contemporains. Grâce à son utilisation, il est possible de traiter des images et des vidéos afin de reconnaître des objets, des visages ou même l'écriture d'une personne, et est constitué d'un module cv2.[21]

- **Numpy :** NumPy, une bibliothèque Python dédiée à la manipulation de tableaux, a été développée par Travis Oliphant en 2005. C'est un projet open source et son utilisation est totalement libre. En Python, les listes peuvent être utilisées comme des tableaux, cependant leur traitement peut s'avérer lent.
  NumPy est conçu pour offrir un objet de tableau qui est jusqu'à 50 fois plus rapide que les listes traditionnelles de Python.[21]

- **Tkinter :** Tool kit interface, également connue sous le nom de Tkinter en anglais, est la bibliothèque graphique open source native pour le langage Python, permettant la conception d'interfaces graphiques sans avoir besoin d'installations ou de bibliothèques additionnelles.[22]

4.3 Implémentations et tests

4.3.1 Détection des malwares

4.3.1.1 Dataset

Le data-set Malware Detection with images correspond à la sélection de données choisie pour détecter les logiciels malveillants à l'aide d'images bénignes, rassemblées depuis différentes sources (Kaggle, Github), ainsi que des images de logiciels malveillants tirées du référentiel Fusion Malware.

Ce jeu de données est organisé en deux sections majeures :

1. Jeu de données : comprend deux répertoires :

- **Bénin :** rassemble les images illustrant les fichiers bénins (non malveillants).
- **Malware :** inclut les images associées à des fichiers malveillants.

Cette section s'agit de l'ensemble complet avant la séparation.

2.SplittedDataset : elle est structurée conformément aux normes d'apprentissage supervisé :

- **Train :** données utilisées pour entrainer le modele
- **Val :** données de validation utilisées pour ajuster les hyperparametres et eviter l'overfitting
- **Test :** données réservées à l'evaluation finale des performances du modèle.

Cette configuration facilite l'implémentation efficace d'un flux de travail d'apprentissage profond pour la classification des malwares basés sur les images.

4.3.1.2 Etapes d'implémentations

Cette partie expose les phases essentielles de l'implémentation du dataset Malware Detection with images pour la détection des malwares via l'analyse d'images , elle s'appuie sur la transformation de fichiers nuisibles en représentations visuelles, facilitant ainsi l'utilisation de méthodes d'apprentissage profond. Chaque échantillon de logiciel malveillant est converti automatiquement en une image RGB lors du traitement , représentant sa structure interne d'une manière qui peut être utilisée par des modèles de classification d'images.

Deux alternatives sont à notre disposition pour la réalisation : développer un réseau de neurones convolutif personnalisé que nous avons entraîné sur notre jeu de données, soit d'utiliser un modèle pré-entraîné(comme MobileNetV2) et poursuivre son apprentissage à l'aide d'images similaires à celles utilisées dans notre application.Afin de tirer parti des avantages de chaque méthode,nous avons choisi de mettre en œuvre les deux alternatives.Cette démarche comparative nous permet d'analyser et d'évaluer les performances respectives d'un modèle personnalisé face à un modèle pré-entraîné,en termes de précision et de capacité de généralisation .

Pour notre réseau de neurones convolutif personnalisé,nous avons implémenté un programme en quatre sections clés :

- Pré-traitement des données.
- Chargement des données.
- Création et entraînement du modèle.
- Évaluation et classification du modèle.

1. Pré-traitement des données

L'étape de prétraitement des données est essentielle dans le processus de classification d'images, puisqu'elle sert à standardiser les données et à les adapter à l'entraînement du modèle. Pour notre projet de détection des malwares à l'aide d'images, les images générées sont redimensionnées à une taille uniforme de (224 x 224 pixels). Cette dimension est choisie pour correspondre à l'architecture de notre réseau de neurones, et chaque pixel de l'image est divisé par 255 pour normaliser les pixels et ramener les valeurs dans une plage entre 0 et 1.

```
model = Sequential([
    Input(shape=(224, 224, 3)),
    Conv2D( filters: 32,  kernel_size: (3, 3), activation='relu'),
    MaxPooling2D( pool_size: 2,  strides: 2),
    BatchNormalization(),
```

Figure 4.1 : Code de redimensionnement des images

```
train_datagen = ImageDataGenerator(
    rescale=1./255,
    rotation_range=20,
    zoom_range=0.2,
    horizontal_flip=True,
    width_shift_range=0.1,
    height_shift_range=0.1
)
```

Figure 4.2 : Code de normalisation des pixels

2. Chargement des données

Pour poursuivre l'apprentissage du modèle sélectionné, il faut lui procurer une base de données d'images bien organisée avec les étiquettes correspondantes (Bénin,Malware) ,par le biais d'images et l'entraînement de modèles d'apprentissage profond pour la classification binaire.

Il est organisé dans un format structuré, divisant les images en trois groupes distincts : train, val et test, chaque groupe contenant deux sous-dossiers qui illustrent les classes malware et benign.pour charger les données nous faisons appel à un générateur de données (ImageDataGenerator) de Keras,qui permet de générer des lots d'images , avec des options de pré-traitement.

3. Création et entraînement du modèle

On a utiliser Un modèle de réseau de neurones convolutionnel (CNN) personnalisé en exploitant l'API Sequential de Keras dans le but d'identifier les malwares à partir d'images.Le modèle se compose de plusieurs couches :

➢ **Convolution et Pooling :** deux couches de convolution (Conv2D) sont employées pour identifier les traits essentiels des images, tels que les textures, les contours, les motifs,etc. nous avons utilisé successivement deux couches convolutifs, la première avec 64 filtres de taille 3×3, et la seconde avec 128 filtres de taille 3×3, permettant au modèle d'extraire progressivement des caractéristiques de plus en plus complexes.

```
Conv2D( filters: 64,  kernel_size: (3, 3), activation='relu'),
MaxPooling2D( pool_size: 2,  strides: 2),
BatchNormalization(),

Conv2D( filters: 128,  kernel_size: (3, 3), activation='relu'),
MaxPooling2D( pool_size: 2,  strides: 2),
BatchNormalization(),
```

Figure 4.3: Code des couches de convolution (Conv2D) utilisé

➢ **Flattening et Couches Denses :**Après l'extraction des caractéristiques à l'aide de plusieurs couches convolutives et de pooling, les données sont aplaties via une couche Flatten, puis transmises à une couche dense de 128 neurones activés par ReLU. Enfin, une dernière couche dense avec un seul neurone et une activation sigmoid effectue la classification binaire entre Malware et Benign**.**

```
Flatten(),
Dense( units: 128, activation='relu'),
Dropout(0.5),
Dense( units: 1, activation='sigmoid')  #
```

Figure 4.4: Code d'aplatissement et de transmission de données

La formation est réalisée sur les données d'entraînement sur une durée de 30 époques, avec un contrôle continu sur les données de validation pour surveiller l'efficacité du

modèle. Cela offre au réseau la possibilité de progresser graduellement et d'améliorer sa capacité à différencier les malwares des fichiers bénins.

```
history = model.fit(
    train,
    validation_data=val,
    epochs=30,
    class_weight={0: 1.0, 1: 2.0},
    callbacks=[early_stop]
)
```

Figure 4.5: Code d'entraînement sur les données avec 30 époques

4. Évaluation et classification du modèle

Le modèle de classification d'images que nous avons construit est un réseau de neurones convolutifs (CNN) qui est adapté à la détection binaire, en particulier pour distinguer les images malveillantes (malware) d'images saines (benign).

Après son entraînement sur un jeu de données étiqueté, nous avons évalué ses performances à l'aide d'un jeu de validation indépendant. Les principales métriques utilisées sont l'Accuracy, Recall ,F1-score et la Matrice de confusion.

4.3.1.3 Présentation de l'interface

Nous avons développé une interface graphique interactive pour ce projet en faisant appel à Tkinter (une librairie Python standard dédiée aux interfaces GUI). Cette interface permet aux utilisateurs d'interagir aisément avec des modèles d'intelligence artificielle sans avoir besoin de compétences techniques en programmation. Elle comprend une interface principale appelée SecureVision, qui est une fenêtre Tkinter servant de point d'accès central vers deux modules essentiels : la détection de malwares et la détection de comportements anormaux.

Figure 4.6: Interface d'accueil

Dans cette section, nous allons présenter l'interface dédiée à la détection de malwares ainsi que ses fonctionnalités :

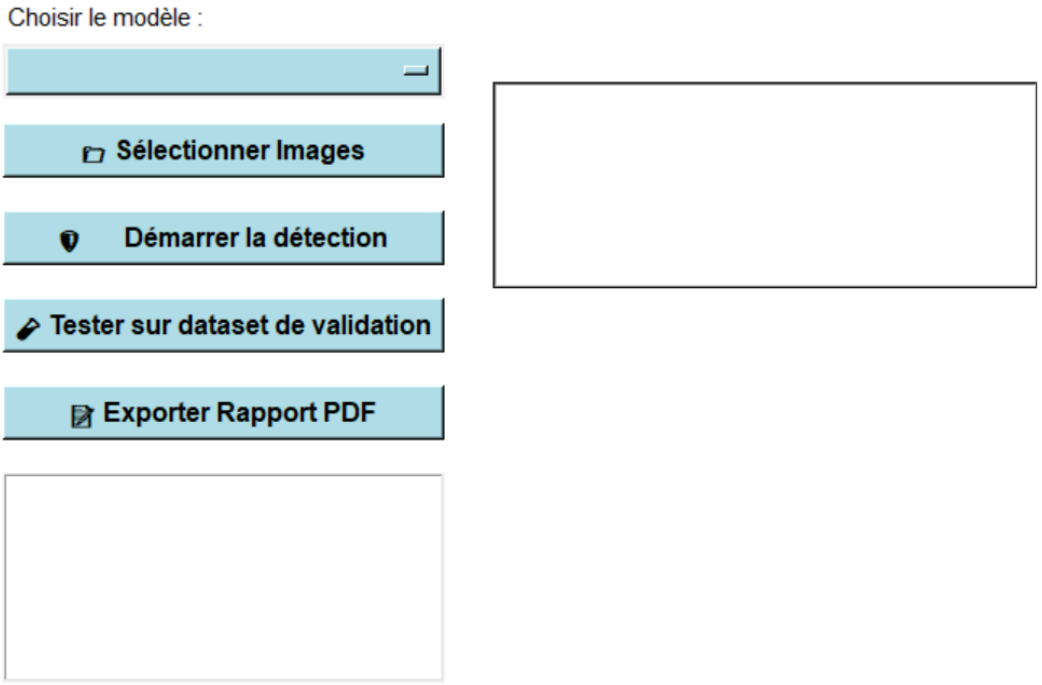


Figure 4.7: Interface de détection de malwares

- **Choix du modèle**

  on peut choisir le modèle à utiliser pour notre détection grâce au bouton « choisir le modèle » ou on peut sélectionner soit Custom qui est notre modèle CNN ou bien MobileNetV2

- **Chargement des images depuis l'ordinateur**

  On peut importer des images depuis notre système local grâce au un bouton « sélectionner images », l'image est automatiquement affichée dans l'interface afin de vérifier qu'il s'agit bien du fichier souhaité.

- **Prédiction de la nature du fichier**

  Le bouton «Démarrer la détection » permet de lancer la prédiction sur l'image chargée. Le modèle de classification, basé sur le réseau de neurones convolutif (CNN), détermine si l'image représente un malware ou un fichier bénin. Le résultat est ensuite affiché clairement dans l'interface, avec un score de confiance (probabilité).

- **Évaluation globale du modèle**

  Notre interface propose également la fonctionnalité d'évaluer automatiquement un jeu de validation contenant des images étiquetées .Lors de cette évaluation,plusieurs métriques de performance sont calculées comme la précision, l'accuracy,le Recall et le F1-score.

- **Export des résultats en PDF**

  L'interface permet d'exporter un rapport au format PDF contenant les résultats de prédiction , les métriques d'évaluation ainsi que la courbe de précision.

4.3.1.4 Résultats

Dans le but de mesurer l'efficacité de chaque approche, nous avons réalisé des tests en utilisant la même image comme référence :

1. **Performances du modèle**

   Après l'entraînement des modèles sur le jeu de données Malware Detection with Images, nous allons évaluer leurs performances sur un ensemble de validation.

   les résultats sont les suivant:

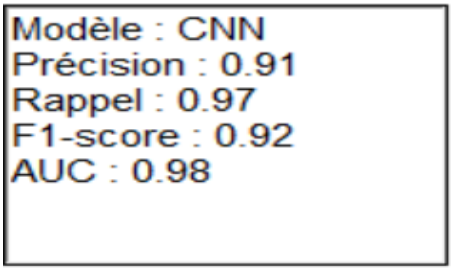


Figure 4.8 : Résultats de performance du modèle CNN

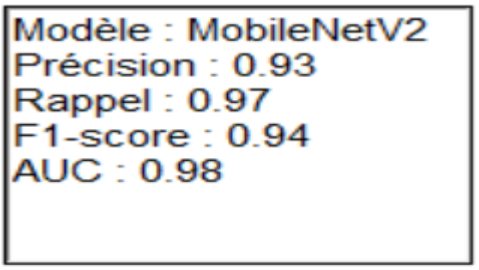


Figure 4.9 : Résultats de performance du modèle MobileNet

2. Matrice de confusion

Les matrices de confusion ont été générées afin de mieux visualiser les performances des modèles et comprendre le taux d'erreurs des modèles selon le type de fichier.

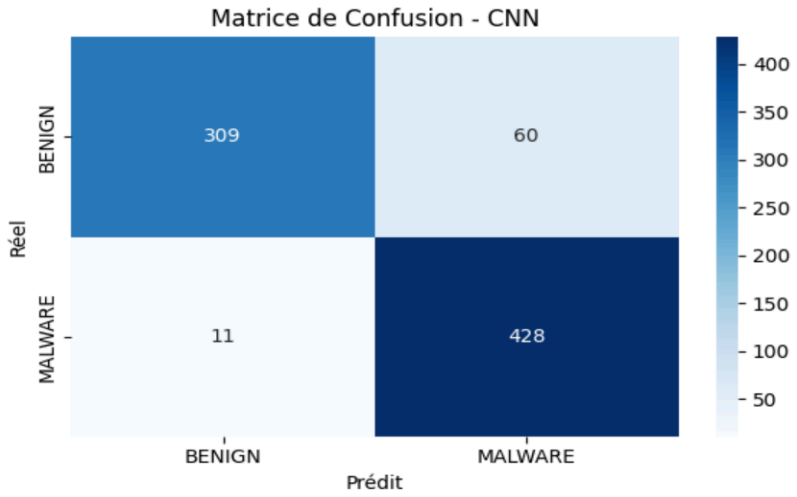


Figure 4.10: Résultats de la matrice de confusion du modèle CNN

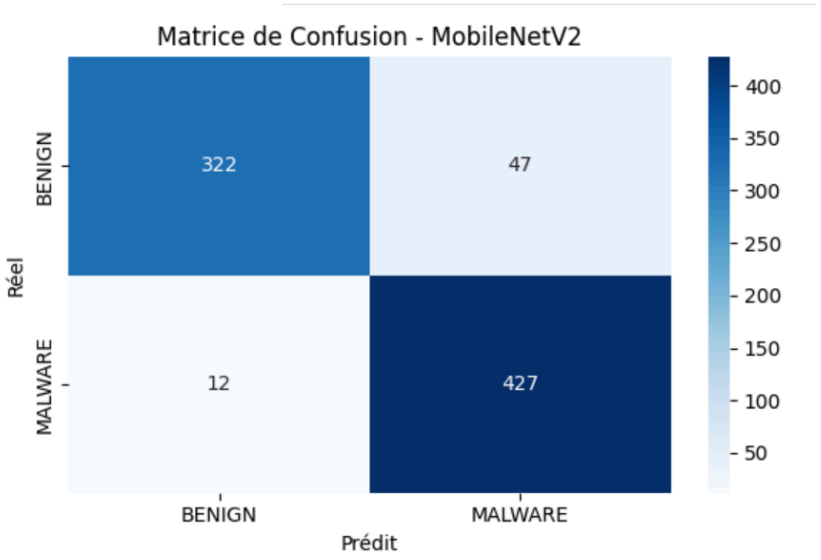
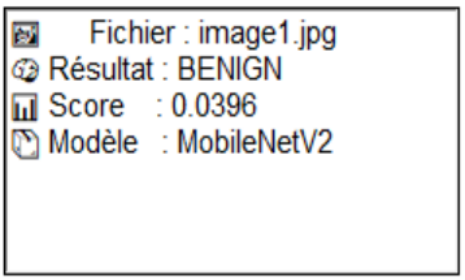
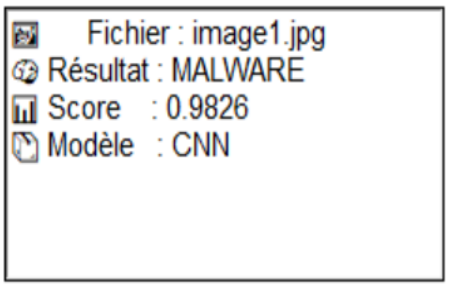


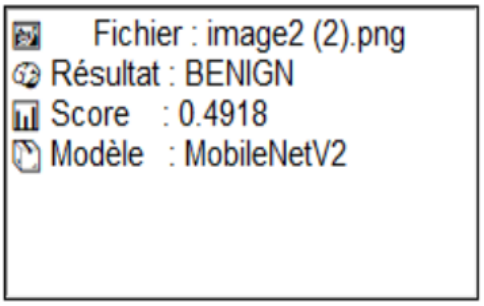
Figure 4.11: Résultats de la matrice de confusion du modèle MobileNet

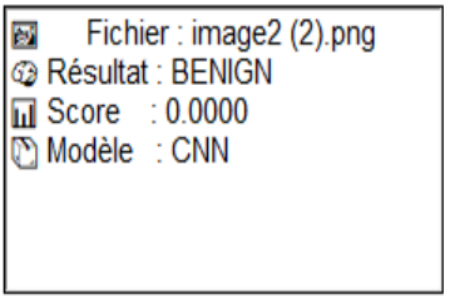
3. Résultats de la classification d'images

Voici quelques exemples de prédictions réalisées par notre interface :









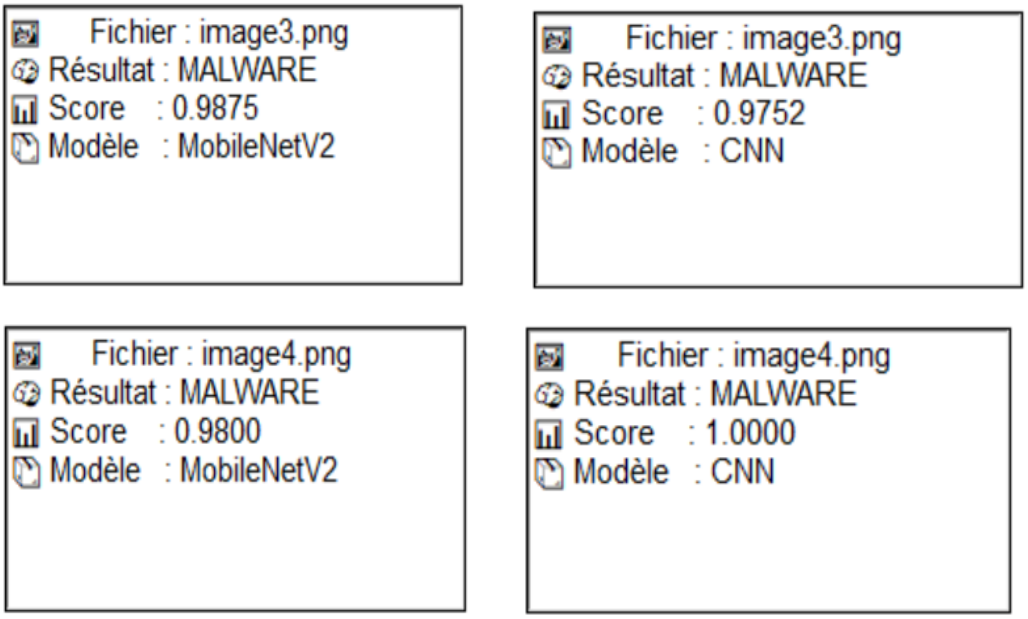


Figure 4.12: Résultats de la classification d'images

4. Rapport

Le rapport a bien été exporté sous forme de PDF contenant les résultats de prédiction des deux modèles ainsi que les courbes de précision.

Rapport de Détection de Malware

Date : 2025-06-19 13:14:21

Fichier : image1.jpg - Résultat : MALWARE - Score : 0.9826 - Modèle : CNN

Fichier : image1.jpg - Résultat : BENIGN - Score : 0.0396 - Modèle : MobileNetV2

Fichier : image2 (2).png - Résultat : BENIGN - Score : 0.0000 - Modèle : CNN

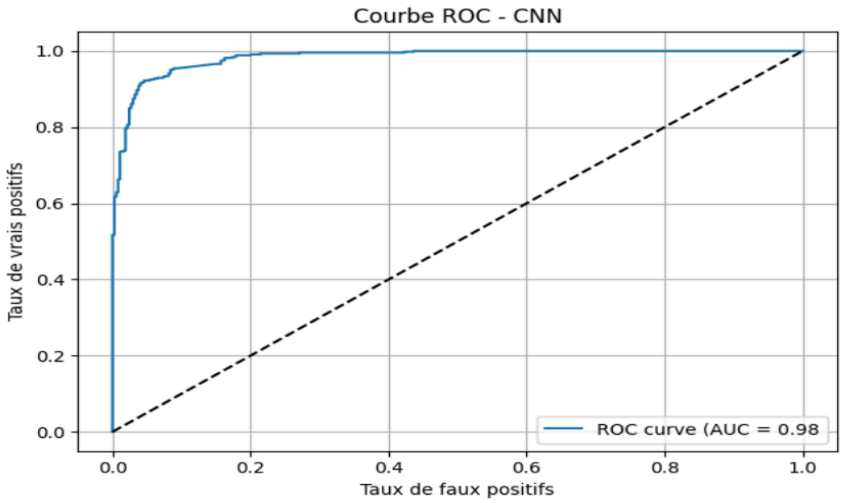
Fichier : image2 (2).png - Résultat : BENIGN - Score : 0.4918 - Modèle : MobileNetV2

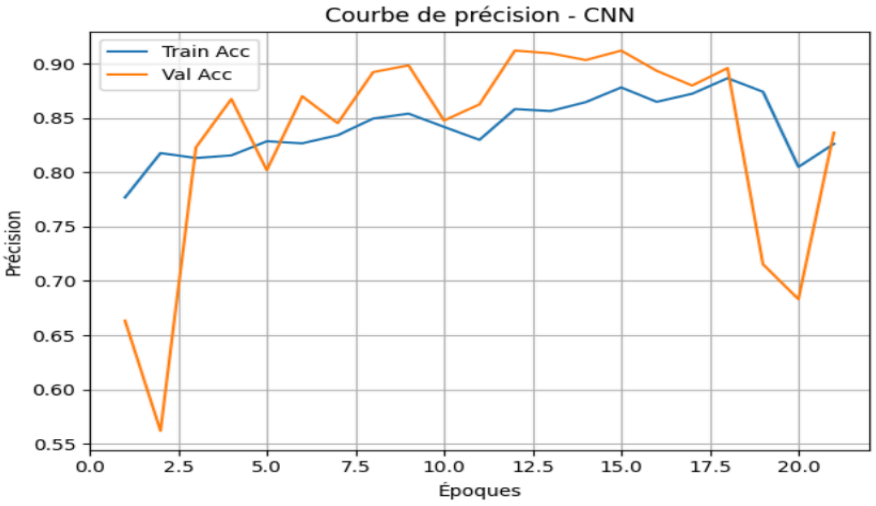
Fichier : image3.png - Résultat : MALWARE - Score : 0.9752 - Modèle : CNN

Fichier : image3.png - Résultat : MALWARE - Score : 0.9875 - Modèle : MobileNetV2

Fichier : image4.png - Résultat : MALWARE - Score : 1.0000 - Modèle : CNN

Fichier : image4.png - Résultat : MALWARE - Score : 0.9800 - Modèle : MobileNetV2





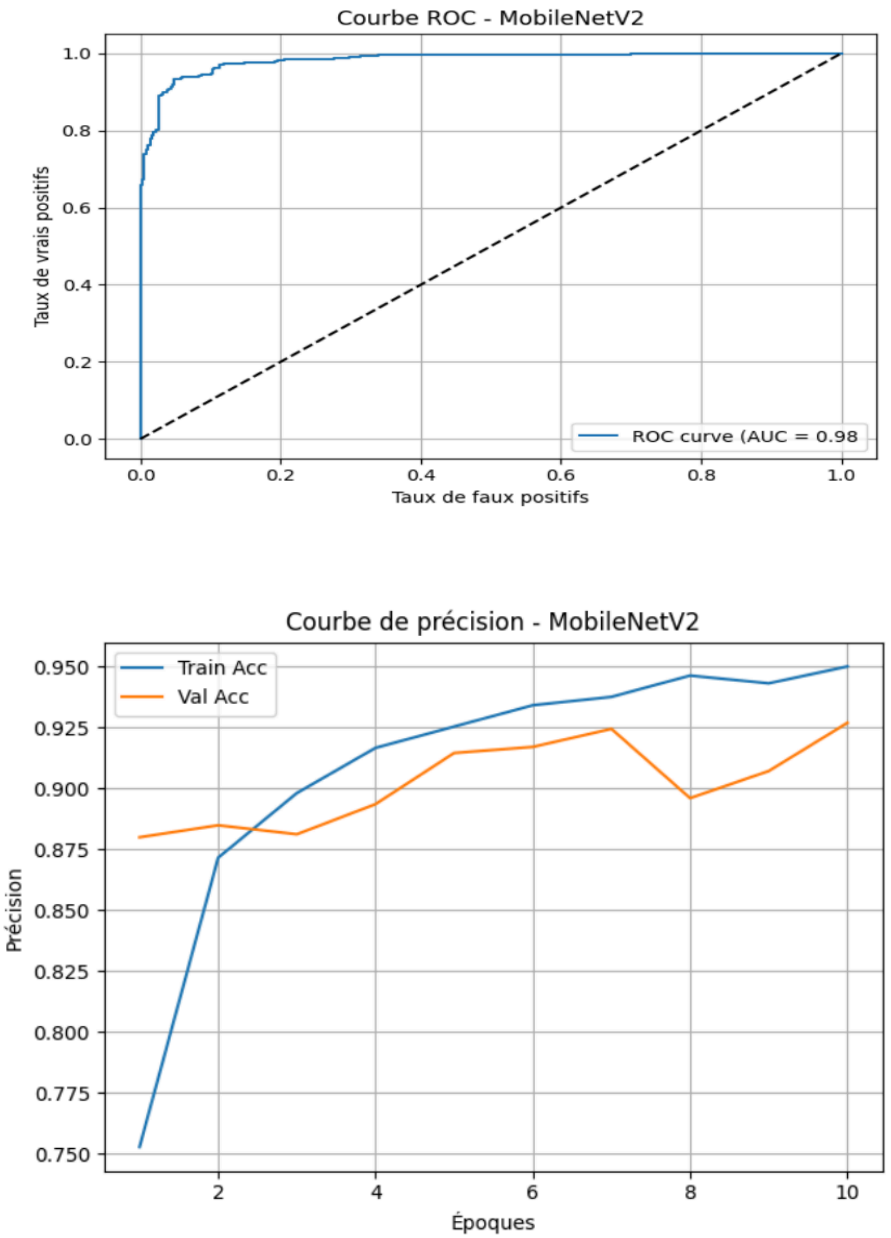


Figure 4.13: Rapport de détection des malwares

4.3.1.5 Analyse des performances

Comparaison entre le modèle CNN personnalisé et le modèle MobileNetV2

1. **Performances du modèle**

Métriques	MobileNetV2	CNN	Modèle le plus performant
Précision	0.93	0.91	MobilNetV2
Rappel	0.97	0.97	/
F1-score	0.94	0.92	MobilNetV2

Tableau 4.1: Comparaison des résultats d'évaluation des deux modèles

- **Précision :** MobileNetV2 atteint une précision de 93%, contre 91% pour le CNN. Cela signifie que MobileNetV2 commet moins de faux positifs et qu'il est plus fiable dans l'identification correcte des malwares.
- **Rappel :**Les deux modèles présentent un rappel de 97%, ce qui montre qu'ils détectent très bien les malwares sans en oublier beaucoup. Cependant, MobileNetV2 maintient cet excellent rappel tout en réduisant les erreurs.
- **F1-Score :** Le F1-Score de MobileNetV2 (94%) est supérieur à celui du CNN (92%). Cela montre que MobileNetV2 offre un meilleur équilibre entre précision et rappel, ce qui le rend plus performant globalement.
- Le modèle MobilNetV2 est clairement meilleur que le CNN personnalisé pour notre jeu de données actuel.

2. **Matrice de confusion**

Modèle	Vrais Positifs (VP)	Faux Positifs (FP)	Vrais Négatifs (VN)	Faux Négatifs (FN)
CNN	428	60	309	11
MobileNetV2	427	47	322	12

Tableau 4.2: Résultats des matrice de confusion des deux modèles

Le modèle MobileNetV2 est plus performant le CNN personnalisé car il fait beaucoup moins d'erreurs de classification, notamment sur les échantillons BENIGN.

3. Classification d'images

Image	Résultat réel	Résultat CNN	Score	Résultat MobileNetV2	Score
image 1	**BENIGN**	❌ MALWARE	0.9826	✅ BENIGN	0.0396
image 2	**BENIGN**	✅ BENIGN	0.0000	✅ BENIGN	0.4918
image 3	**MALWARE**	✅ MALWARE	0.9752	✅ MALWARE	0.9875
image 4	**MALWARE**	✅ MALWARE	1.0000	✅ MALWARE	0.9800

Tableau 4.3: Classification des images par les deux modèles

- **image 1 :** le modèle MobilNetV2 prédit correctement benign avec très haute confiance (score = 0.0396), tandis que le CNN personnalisé se trompe en la classant comme malware
- **image 2 :** les deux modèles prédisent correctement benign , mais le modèle CNN a une confiance plus élevé
- **image 3 :**les deux modèles prédisent correctement malware, mais le modèle MobileNetV2 a une confiance légèrement plus élevé
- **image 4:**les deux modèles prédisent correctement malware , mais le modèle CNN a une confiance légèrement plus élevé

4.3.2 Détection des comportements anormaux

4.3.2.1 Dataset

Le data-set DCSASS ""Dataset for Complex Scene Abnormality in Surveillance Systems" correspond à la sélection de données choisie pour détecter les comportements anormaux des humains dans la vidéo surveillance.Cet ensemble de données contient des

vidéos basées sur les 13 classes suivantes : Abus, Arrestation, Incendie criminel, Agression, Accident, Cambriolage, Explosion, Bagarres, Vol qualifié, Fusillade, Vol, Vol à l'étalage et Vandalisme. Chaque vidéo est étiquetée comme normale (0) ou anormale (1) en fonction de son contenu.L'agencement de ce jeu de données est comme suit :
On dénombre 16853 vidéos au total, avec 9676 classées comme normales et 7177 comme anormales.

4.3.2.2 Étapes d'implémentations

Cette section détaille les étapes clés de la mise en œuvre du jeu de données DCSASS pour l'identification des comportements anormaux chez les humains, qui repose essentiellement sur l'analyse spatio-temporelle des vidéos. Cette analyse combine les caractéristiques visuelles tirées des images (frames) avec la dynamique du mouvement au fil du temps. Elle fait également appel à des modèles d'apprentissage profond tels que le ConvLSTM ou les Autoencoders spatio-temporels, aptes à saisir simultanément les détails visuels (postures, objets) et les séquences d'actions.

L'implémentation de ce jeu de données se déroule en deux phases majeures , l'intégration du dataset lui-même suivie de son ajustement à notre propre contexte vidéo. Ce processus s'appuie sur plusieurs étapes clés :

- Pré-traitement des données.
- Chargement des données.
- Entraînement du modèle.
- Évaluation et classification du modèle.

1. **Pré-traitement des données**

   La phase de prétraitement est essentielle pour la détection des comportements anormaux.Dans le cadre de notre projet, nous sauvegardons au préalable les séquences d'images extraites des vidéos sous forme de fichiers.Chaque séquence dans le fichier npy est constituée de plusieurs frames qui ont été redimensionnées en (32 x 32 pixels) à l'aide la fonction cv2.resize.

Pour rendre ces données prêtes pour l'apprentissage du modèle ConvLSTM, une normalisation est effectuée : Chaque pixel est normalisé en divisant sa valeur par 255, afin de restreindre les données à une plage de [0, 1].

```
# === Paramètres ===
IMG_SIZE = 32  # ↓ Taille réduite ici
CATEGORIES = [("Normal", 0), ("Anomalous", 1)]
```

Figure 4.14: Code de redimensionnement des images

```
# Normalisation
X_train = X_train / 255.0
X_val   = X_val / 255.0
X_test  = X_test / 255.0
```

Figure 4.15: Code de normalisation des pixels

2. Chargement des données

Le chargement des données constitue un étape cruciale dans la préparation d'un modèle d'apprentissage profond.Dans cette partie les fichiers NumPy prétraités ,X_train.npy, X_val.npy, X_test.npy pour les données d'images (X),ainsi que Y_train.npy, Y_val.npy, Y_test.npy pour leurs étiquettes correspondantes (Y) sont chargés de manière efficace en mémoire à l'aide de la fonction np.load().

Cette technique garantit une préparation rapide des ensembles d'entraînement, devalidation et de test du modèle tout en garantissant la cohérence des données ainsi qu'une optimisation de la mémoire lors de l'apprentissage.

```
# ===  Chargement des données ===
print(" Chargement des fichiers .npy...")

X_train = np.load('X_train.npy')
X_val   = np.load('X_val.npy')
X_test  = np.load('X_test.npy')
y_train = np.load('y_train.npy')
y_val   = np.load('y_val.npy')
y_test  = np.load('y_test.npy')
print(f" Données chargées :")
```

Figure 4.16: Code de chargement des données

3. Entraînement du modèle

Pour saisir les dynamiques spatio-temporelles présentes dans les vidéos de surveillance, un modèle utilisant des réseaux de neurones récurrents convolutifs (ConvLSTM) a été établi.Il est particulièrement approprié pour modéliser les séquences d'images en considérant à la fois l'information spatiale (contenu de chaque image) et le déroulement temporel (enchaînement des images).

➢ **Préparation des séquences :** Les données vidéo, initialement présentées comme des images indépendantes, ont été organisées en séquences. Chaque échantillon d'entrée représente une séquence de 10 images consécutives.Ce processus de séquençage a pour but de modifier les données d'entraînement, de validation et de test afin qu'elles soient adaptées à l'entrée requise par la couche ConvLSTM2D.

```
# === Séquençage des données ===
sequence_length = 10

def create_sequences(X, y, seq_len):
    X_seq, y_seq = [], []
    for i in range(len(X) - seq_len):
        X_seq.append(X[i:i+seq_len])
        y_seq.append(y[i + seq_len - 1])
    return np.array(X_seq), np.array(y_seq)

X_train_seq, y_train_seq = create_sequences(X_train, y_train, sequence_length)
X_val_seq, y_val_seq     = create_sequences(X_val, y_val, sequence_length)
X_test_seq, y_test_seq   = create_sequences(X_test, y_test, sequence_length)

print(f" Données séquencées :")
print(f"   ➤ X_train_seq : {X_train_seq.shape}")
print(f"   ➤ X_val_seq   : {X_val_seq.shape}")
print(f"   ➤ X_test_seq  : {X_test_seq.shape}")
```

Figure 4.17: Code de séquençage des données

Nous avons opté pour la fonction d'activation ReLU, car elle génère les résultats les plus performants par rapport à d'autres fonctions.

Nous avons remarqué qu'il existe un problème de surapprentissage lors des formations successives du modèle, ce qui a entraîné une diminution de la valeur d'Accuracy.Le problème auquel nous sommes confrontés est le OVERFITTING. Pour y remédier, nous appliquons la méthode du Dropout (0.5) afin de régulariser par l'abandon aléatoire de 50 % de la précision des données d'entraînement et de validation.

Le modèle est élaboré avec la fonction de perte binary_crossentropy, un optimiseur Adam dont le but est d'ajuster les poids d'un réseau de neurones afin de minimiser la perte tout en réduisant l'erreur au minimum, et utilise l'accuracy comme critère d'évaluation.

```
# ===  Modèle ConvLSTM ===
print(" Construction du modèle...")

model = Sequential([
    ConvLSTM2D(filters=32, kernel_size=(3, 3), activation='relu',
               input_shape=(sequence_length, 32, 32, 3),
               padding='same', return_sequences=False),
    BatchNormalization(),
    Flatten(),
    Dense(64, activation='relu'),
    Dropout(0.5),
    Dense(1, activation='sigmoid')
])

model.compile(optimizer='adam', loss='binary_crossentropy', metrics=['accuracy'])
model.summary()
```

Figure 4.18: Implémentation du modèle

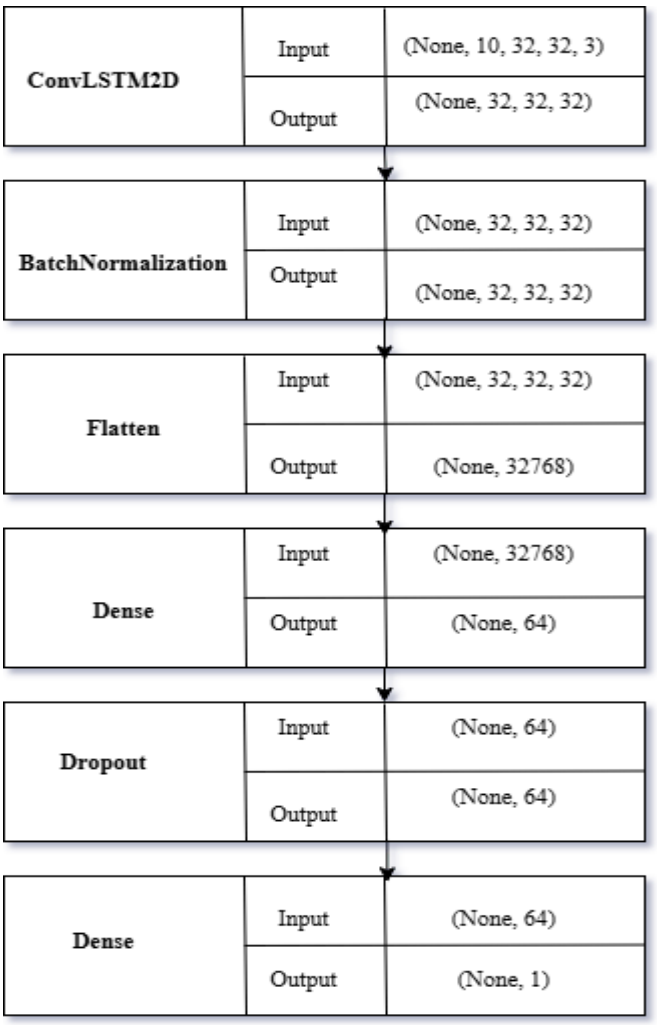


Figure 4.19: Architecture du modèle

3.3 Entraînement : Le modèle a été formé sur 5 époques en utilisant une taille de lot (batch_size) de 32.On a eu recours à deux méthodes de régularisation :

- **EarlyStopping:** une méthode pour stopper l'entraînement si la perte de validation cesse de progresser.
- **ModelCheckpoint:** une fonctionnalité pour enregistrer automatiquement les poids du modèle le plus performant basé sur la précision de la validation.

```
# ===  Entraînement ===
print(" Entraînement...")

history = model.fit(
    X_train_seq, y_train_seq,
    epochs=5,
    batch_size=32,
    validation_data=(X_val_seq, y_val_seq),
    callbacks=[checkpoint, earlystop]
)
```

Figure 4.20: Entraînement du modèle

4. Évaluation et classification du modèle

Après l'entraînement, le modèle a été évalué sur les données de test, l'évaluation comprend la perte (loss) et la précision (accuracy) calculées sur le jeu de test, fournissant une première évaluation globale des performances.

Par la suite, nous avons effectué une classification globale en utilisant un rapport de classification qui fournit les métriques telles que la précision, le rappel et le F1-score pour chaque catégorie.

En outre, un examen détaillé des erreurs a permis de distinguer les faux positifs (prédictions incorrectes anormales) et les faux négatifs (prédictions incorrectes normales), ce qui a facilité la compréhension des limites du modèle.
Les résultats sont présentés à l'aide d'une matrice de confusion et de courbes d'apprentissage, et résumés dans un rapport PDF détaillé.

```
# ===  Evaluation ===
loss, accuracy = model.evaluate(X_test, y_test, verbose=1)
print(f" Perte sur test : {loss:.4f}")
print(f" Précision sur test : {accuracy:.4f}")

# ===  Prédiction ===
print(" Génération des prédictions sur le test...")
y_pred_probs = model.predict(X_test)
y_pred = (y_pred_probs > 0.5).astype(int)

# ===  Rapport de classification ===
report_text = classification_report(y_test, y_pred, digits=4)
print(" Rapport de classification :\n")
print(report_text)
```

Figure 4.21: Evaluation et classification du modèle

4.3.2.3 Présentation de l'interface

Dans cette partie, nous allons exposer l'interface conçue pour l'identification de comportements anormaux, obtenue en cliquant sur le bouton « Détection de comportements » situé dans l'interface d'accueil déjà décrite ci-dessus.

Cette dernière permet d'évaluer un modèle de deep learning et de procéder à une détection sur notre propre vidéo en utilisant le modèle ConvLSTM pré-entraîné sur notre jeu de données. Elle est equipée d'une zone de logs qui permet de suivre les actions (chargement , évaluation, erreurs éventuelles), afficher les messages d'état et est organisée en deux grandes sections :

1. **Evaluation du modèle :** avec trois boutons principaux

- **Charger les données :** pour charger les fichiers X_test.npy et Y_test.npy Il s'agit des caractéristiques et étiquettes pour l'évaluation du modèle.
- **Charger le modèle :** permet de sélectionner un fichier .h5 contenant le modèle à évaluer.
- **Evaluer le modèle :** lance l'évaluation avec les prédictions ,rapport de classification,courbes de précision/perte et la génération automatique du rapport pdf "rapport_evaluation.pdf".

  Barre de progression sous ces boutons pour montrer l'avancement.

2. **Détection sur vidéo :** cette section contient

- **Zone pour choisir une vidéo à analyser :** input + bouton pour choisir une vidéo "mp4".
- **Zone pour charger le modèle :** input + bouton pour choisir un modèle ".h5".
- **Bouton Lancer la détection :** lancer la détection sur la vidéo choisie en utilisant le modèle sélectionné.

  En fin d'évaluation un rapport pdf est créé automatiquement avec un rapport de classification, une matrice de confusion et les courbes de précision/perte.

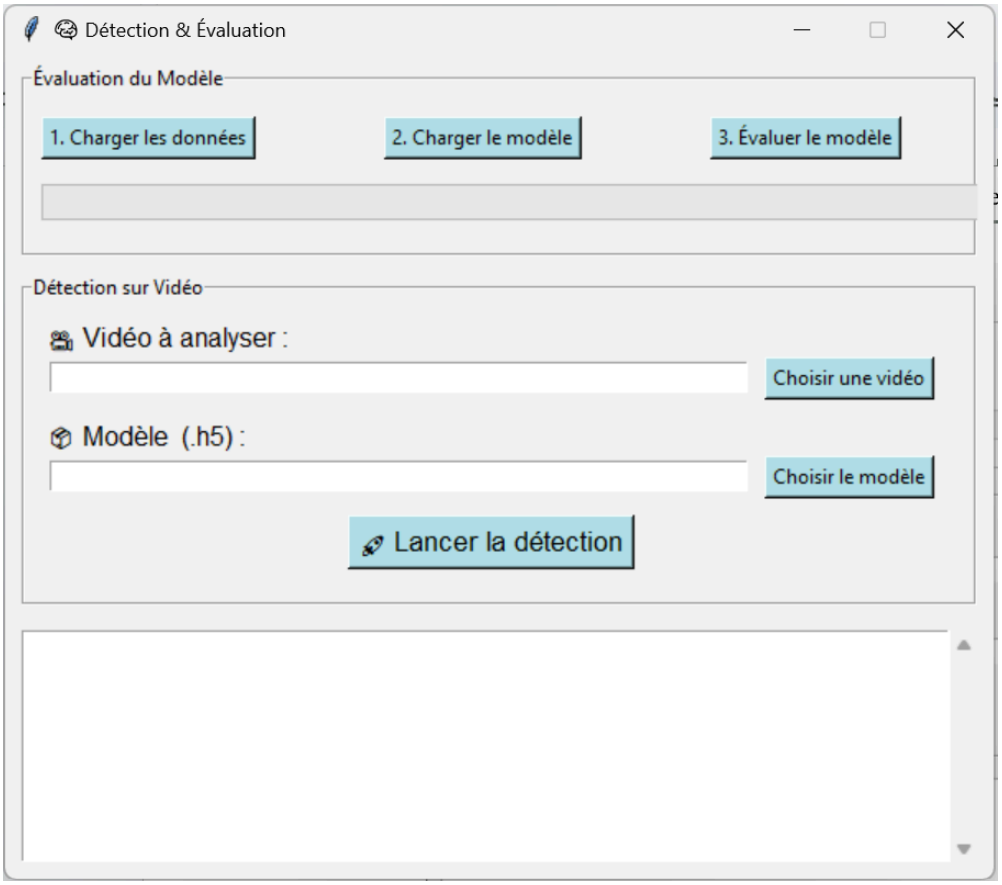


Figure 4.22: Interface Détection & Evaluation

4.3.2.4 Résultats

Les résultats exposés proviennent de l'entraînement du modèle sur le jeu de données DCSASS, puis sur notre environnement vidéo.

1. **Performances du modèle**

   les résultats sont présentés dans la figure 4.29 ci dessous font partie du dataset DCSASS :

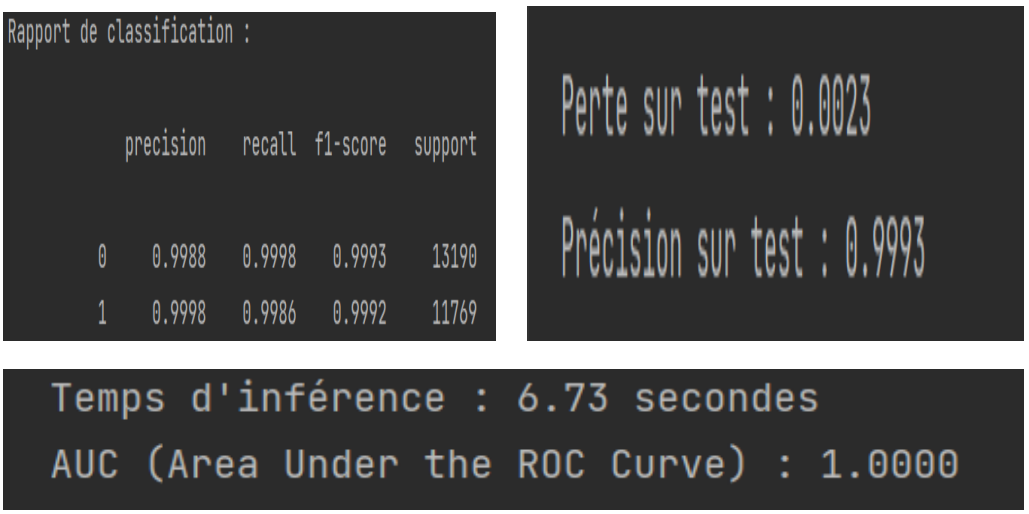


Figure 4.23: Performances du modèle

Les résultats de l'évaluation du modèle indiquent une performance remarquable sur le jeu de test , avec une précision globale atteignant (Accuracy= 99.93%).Les indicateurs de classification montrent des résultats très élevés pour les deux classes, avec une précision, un rappel et un score F1 dépassant 99.8%, que ce soit pour la classe normale (0) ou la classe anomalous (1). Ces résultats montrent que le modèle a la capacité de différencier efficacement les deux sortes de comportements avec un taux d'erreurs extrêmement bas.
La perte (loss) tres basse de 0,0023 renforçant encore notre observation suggerant un bon apprentissage du modele.

Le modèle a effectué les prédictions sur le jeu de test en 6,73 secondes, illustrant ainsi une rapidité d'inférence appropriée pour les applications en temps réel. De plus, le score AUC (Area Under the ROC Curve) de 1.0000 témoigne d'une performance parfaite du modèle dans la différenciation des classes normales et anormales, sans une seule erreur de classification. Ce résultat indique l'efficacité d'un modèle de haut niveau, même si cette performance hors du commun nécessite une validation sur des données plus diversifiées pour écarter toute possibilité de surapprentissage.

2. Matrice de confusion et courbes

La matrice de confusion est générée pour évaluer précisément la performance du modèle CoonvLSTM en montrant comment il classe correctement ou incorrectement chaque catégorie (normal ou anormal).

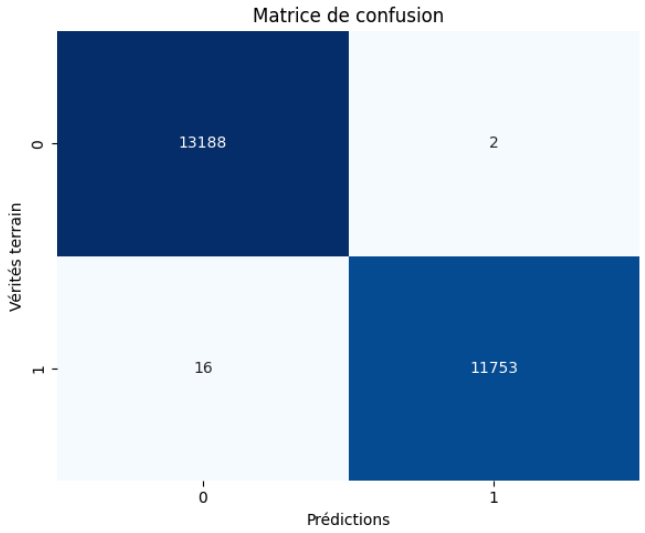


Figure 4.24: Matrice de confusion

- **[0,0] = 13188 Vrai négatif (vn) :** le modèle a bien identifié la classe 0 "Normal" pour 13188 instances.
- **[0,1] = 2 : Faux positif (fp) :** le modèle a estimé la classe 1 "anormal " alors que la réalité indiquait 0, ce qui constitue une erreur.
- **[1,0] = 16 : Faux négatif (fn) :** le modèle a estimé 0 alors que le résultat correct était 1, ce qui constitue une erreur.
- **[1,1] = 11753 : Vrai positif (vp) :** le modèle a efficacement identifié la classe 1 pour 11753 échantillons.

La matrice indique que le modèle est très efficace, ayant classé correctement 13 188 comme normaux et 11 753 comme anormaux, avec un total de seulement 18 erreurs (2 faux positifs et 16 faux négatifs).Cela indique que le modèle fait une bonne distinction entre les deux classes et reflete une grande fiabilité dans ses prédictions.

Les courbes de précision et de perte représentent la progression des performances du modèle durant l'entraînement, ce qui permet de mesurer son aptitude à bien apprendre et à généraliser sur les données.

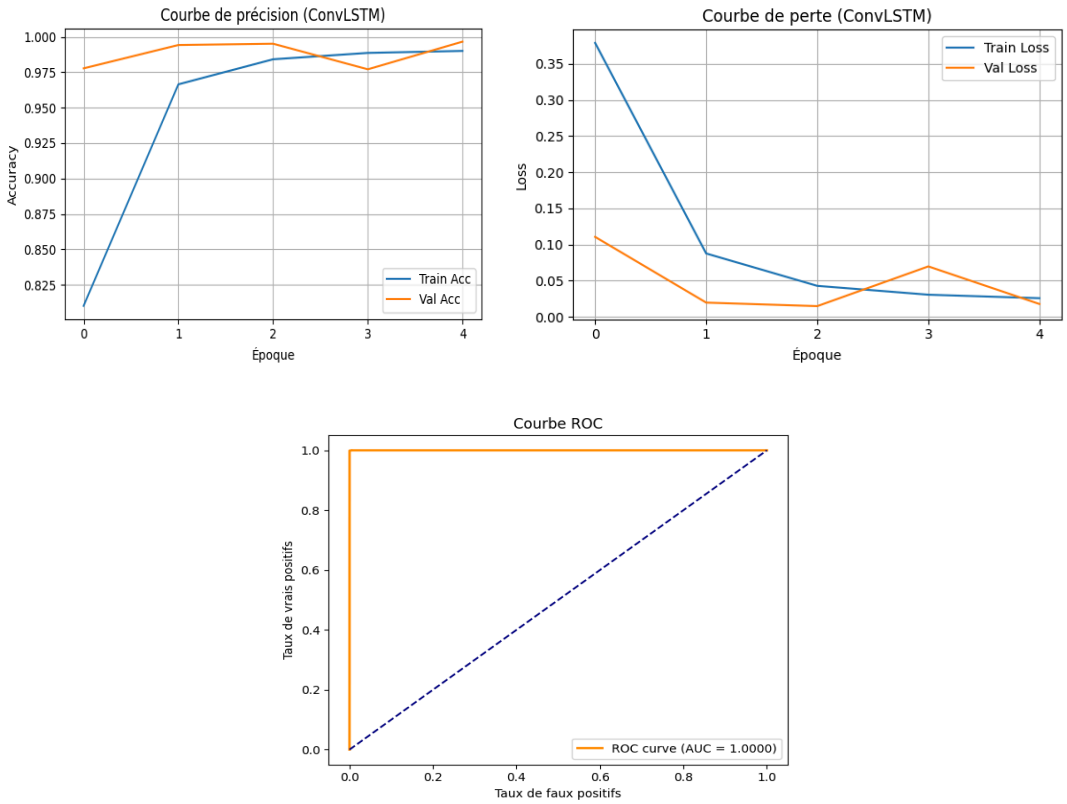


Figure 4.25: Courbes

3. Résultats de classification vidéo

Par la suite, nous avons évalué ce modèle ConvLSTM dans notre environnement vidéo et nous avons obtenu ces résultats :

```
[ i  ] Probabilité moyenne d'anomalie sur la vidéo : 0.062
=> Vidéo classée comme : Normale
```

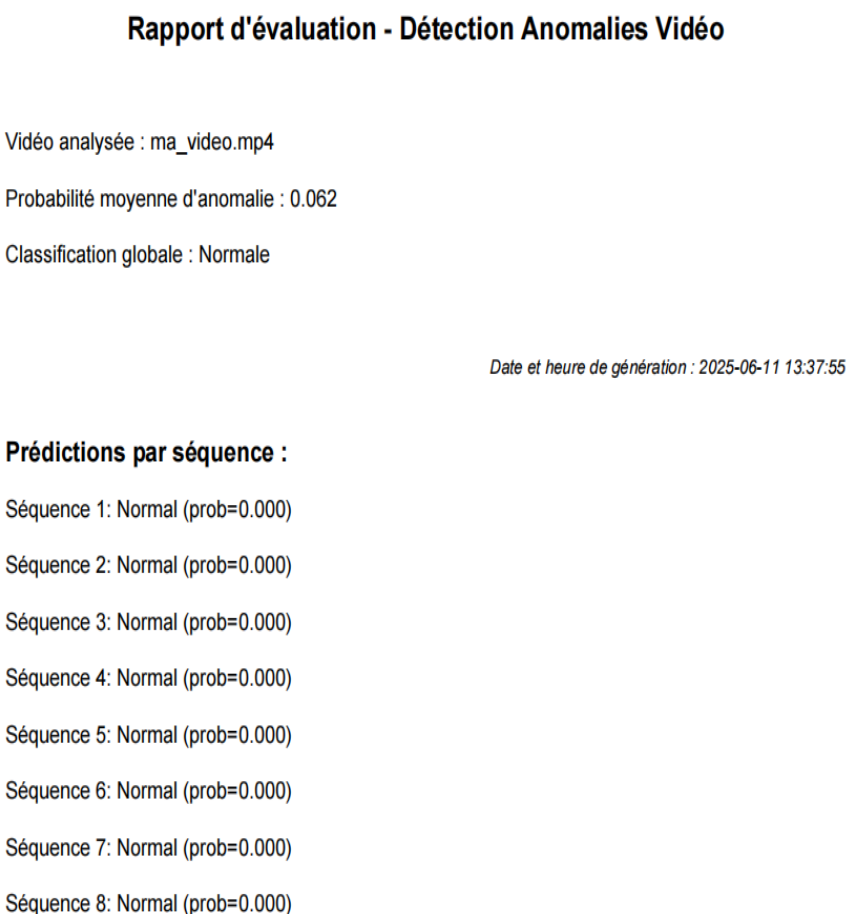
Figure 4.26: Résultats de classification de vidéo

Parmi toutes les séquences examinées, quasiment toutes ont été considérées normales avec un risque d'anomalie de 0.000, hormis quelques séquences isolées identifiées comme anormales avec une probabilité de 1.000. Malgré cela, la probabilité moyenne de détection d'anomalie sur l'ensemble de la vidéo est de 0.062, un chiffre très bas qui conduit à une classification finale de la vidéo en tant que normale.

4. Rapport

Les résultats de prédiction du modèle mentionnés ci-dessus ont été exportés avec succès sous format PDF , tout comme celles de détection vidéo qui inclut les séquences de prédictions créées pour chaque segment analysé.

Il s'agit d'un aperçu des séries de prédictions contenues dans le rapport, compte tenu de leur grand nombre (693), il n'est pas possible de toutes les intégrer ici :



Rapport d'évaluation - Détection Anomalies Vidéo

Vidéo analysée : ma_video.mp4

Probabilité moyenne d'anomalie : 0.062

Classification globale : Normale

Date et heure de génération : 2025-06-11 13:37:55

Prédictions par séquence :

Séquence 1: Normal (prob=0.000)

Séquence 2: Normal (prob=0.000)

Séquence 3: Normal (prob=0.000)

Séquence 4: Normal (prob=0.000)

Séquence 5: Normal (prob=0.000)

Séquence 6: Normal (prob=0.000)

Séquence 7: Normal (prob=0.000)

Séquence 8: Normal (prob=0.000)

Figure 4.27: Rapport de détection d' anomalies vidéo

4.4 Conclusion

La conception de la solution proposée repose sur une approche structurée et adaptée à la complexité des enjeux de détection des malwares et des comportements atypiques.L'implémentation de jeux de données appropriés est essentielle pour assurer la solidité et la crédibilité du système.

Dans le cadre de la détection des malwares, nous avons mis en œuvre deux modèles de deep learning le CNN et MobileNet, en exploitant le jeu de données Malware Detection with images. Nos résultats montrent que notre modèle CNN est plus efficace que MobileNet, car il commet beaucoup moins d'erreurs de classification, en particulier pour les échantillons benign.

En ce qui concerne l'identification des comportements anormaux, notamment à partir de séquences vidéo, nous avons employé le jeu de données DCSASS. La modélisation a été améliorée grâce à l'utilisation du ConvLSTM qui associe l'extraction spatiale des CNN à la modélisation temporelle des LSTM.L'organisation des données en séquences favorise l'apprentissage profond, ce qui améliore la détection d'anomalies complexes.

Pour résumer, l'accent mis sur la qualité et l'organisation des ensembles de données a permis de développer une solution à la fois cohérente et efficace, capable d'identifier avec exactitude les malwares et les comportements anormaux tout en alliant précision et efficacité.

Conclusion Générale

La vidéosurveillance joue un rôle primordial dans la protection des personnes et des biens, que ce soit dans des espaces privés ou publics. Toutefois, malgré son importance croissante, ce domaine présente encore plusieurs limites, notamment en matière de surveillance continue, de charge cognitive pour les opérateurs, et de vulnérabilité face aux cybermenaces.

Dans le cadre de ce travail de fin d'études, nous avons analysé le système de vidéosurveillance de l'entreprise Béjaïa Mediterranean Terminal (BMT) et avons identifié deux défis majeurs :

L'amélioration de la détection des comportements anormaux, afin de garantir une surveillance plus efficace et moins dépendante de l'attention humaine.

Le renforcement de la protection contre les cyberattaques, notamment les logiciels malveillants sophistiqués capables d'échapper aux solutions de sécurité traditionnelles.

Pour répondre à ces défis, nous avons proposé une solution , basée sur les techniques avancées de deep learning et reposant sur deux volets complémentaires :
La détection automatique des logiciels malveillants, en utilisant des méthodes de deep learning basées sur la visualisation d'images permettant une classification efficace, y compris face à des malwares complexes et furtifs.

La détection automatique des comportements anormaux dans les flux de vidéosurveillance, dans le but de réduire la charge cognitive des opérateurs et d'accélérer la détection des incidents critiques.

Afin de valider notre approche, nous avons développé une application intégrant des interfaces conviviales, facilitant l'interaction avec les utilisateurs et les opérateurs de sécurité. L'évaluation des performances des systèmes proposés, réalisée à l'aide de jeux de données pertinents et de classificateurs adaptés, a confirmé l'efficacité et la pertinence de notre solution dans le cadre de la sécurisation globale de BMT.

Cependant, il est important de souligner que la performance de notre système dépend fortement de la qualité et de la diversité des jeux de données utilisés. L'intégration de bases de données plus larges et variées serait nécessaire pour renforcer la robustesse et la capacité de généralisation des modèles développés. Par ailleurs, la détection des malwares demeure un défi mondial. Si leur éradication totale reste difficilement envisageable, il est néanmoins possible de réduire significativement leur impact en maximisant le taux de détection et en minimisant les faux négatifs.

Bibliographie

[1] « Qu'est-ce qu'un système de vidéosurveillance et comment fonctionne-t-il ? » *Algotive*, 5 avr. 2023, https://www.algotive.ai/fr-fr/blog/quest-ce-quun-systeme-de-videosurveillance-et-comment-fonctionne-t-il. Consulté le 2 févr. 2025.

[2] DIASIVI, Arnold. « Vidéosurveillance. » *ISTA Gombe-Matadi*, 2015, https://www.memoireonline.com/04/19/10748/m_Videosurveillance0.html#toc1. Consulté le 20 févr. 2025.

[3] Ben Chehida, Ramzi. *« Chapitre 3 : Évolution des systèmes de vidéosurveillance. »* Technologue Pro, 26 nov. 2017, https://www.technologuepro.com/cours-videosurveillance/Chapitre-3-evolution-des-systemes-de-videosurveillance.html. Consulté le 24 févr. 2025.

[4] « Chapitre 2 : Vidéosurveillance. » *Technologue Pro*, https://www.technologuepro.com/cours-videosurveillance/Chapitre-2-videosurveillance.pdf. Consulté le 24 févr. 2025.

[5] Monideepa Mrinal Roy. « Le côté obscur des brèches des caméras de surveillance. » *ManageEngine Blog*, 6 juin 2024, https://blogs.manageengine.com/fr/2024/06/06/le-cote-obscur-des-breches-des-cameras-de-surveillance.html. Consulté le 23 avr. 2025.

[6] «vulnérabilités.» Alerte vulnérabilité informatique] Vulnérabilité impactant des caméras IP Hikvision, publié le 27 septembre 2022, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/alerte-vulnerabilite-informatique-vulnerabilite-impactant-des-cameras-ip-hikvision . Consulté le 27 avril 2025.

[7] « Les différents types de caméras de surveillance. » *Inomega Blog*, INOMEGA, 6 juin 2024, https://inomega.fr/blogs/blog-inomega/les-differents-types-de-cameras-de-surveillance. Consulté le 01 juin 2025.

[8] «Composants d'un système de vidéosurveillance » *Micro-Center*, Micro Electronics Inc., https://www.micro-center.fr/les-composants-dun-systeme-de-video-surveillance-et-dalarme/ . Consulté le 05 mai 2025.

[9] « Équipements vidéosurveillance intelligente. » *Veesion*, 12 mars 2024, https://veesion.io/quels-equipements-pour-une-videosurveillance-intelligente-fonctionnelle/ . Consulté le 08 juin 2025.

[10] « Caméra IP. » *Wikipédia*, Wikimedia Foundation, dernière modification le 8 juin 2025, https://fr.wikipedia.org/wiki/Cam%C3%A9ra_IP. Consulté le 10 mai 2025.

[11] « Qu'est-ce qu'un malware ? » *Oracle*, https://www.oracle.com/fr/cloud/malware-logiciel-malveillant/. Consulté le 4 avril 2025.

[12] Baker, Kurt. *« Les 11 types de logiciels malveillants les plus courants. » CrowdStrike*, 14 janv. 2022, https://www.crowdstrike.com/fr-fr/cybersecurity-101/malware/types-of-malware/. Consulté le 4 avr. 2025.

[13] Bhatnagar, Abhishek. « Introduction to Deep Learning. » *GeeksforGeeks*, 6 févr. 2025, https://www.geeksforgeeks.org/introduction-to-deep-learning/. Consulté le 6 avr. 2025.

[14] Kamel, M. (2023). *Modèles probabilistes et apprentissage statistique/automatique avancé pour la détection des anomalies : application dans l'industrie de télécommunication* [Thèse de doctorat, École Nationale Supérieure des Mines de Saint-Étienne]. HAL. https://theses.hal.science/tel-04954528v1.Consulté le 6 avr.2025.

[15] Daniel,Gibert, Carles Mateu. « *Convolutional Neural Network for Classification of Malware Represented as Gray-Scale Images.* » *Journal of Computer Virology and Hacking Techniques*, vol. 15, no. 1, mars 2019, pp. 15–28. Using convolutional neural networks for classification of malware represented as images | Journal of Computer Virology and Hacking Techniques. Consulté le 3 mai 2025.

[16] « Deep Learning. » *MathWorks,* https://ch.mathworks.com/fr/discovery/deep-learning.html. Consulté le 7 mai 2025.

[17] Medel, Jefferson Ryan, et Andreas Savakis. « Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks. » *arXiv*, 15 déc. 2016, https://arxiv.org/abs/1612.00390. Consulté le 20 mai 2025.

[18] Rossum, Guido van. « Python (langage) — Wikipédia. » *Wikipédia*, https://fr.wikipedia.org/wiki/Python_(langage). Consulté le 24 mai 2025.

[19] « PyTorch — Wikipédia. » *Wikipédia*, https://fr.wikipedia.org/wiki/PyTorch . Consulté le 24 mai 2025.

[20] Vaughan, Jack. « What Is TensorFlow? » *SearchDataManagement, TechTarget,* https://www.techtarget.com/searchdatamanagement/definition/TensorFlow. Consulté le 24 mai 2025.

[21] Frutos, Romain. « Keras : tout savoir sur l'API de Deep Learning. » *DataScientest*, https://datascientest.com/keras. Consulté le 24 mai 2025.

[22] Jain, Sandeep. « What is OpenCV Library? » *GeeksforGeeks,* 15 avr. 2024, https://www.geeksforgeeks.org/opencv-overview/. Consulté le 25 mai 2025.

[22] Jain, Sandeep. « What is Python Scikit Library? » *GeeksforGeeks*, 12 avr. 2024, https://www.geeksforgeeks.org/what-is-python-scikit-library/. Consulté le 25 mai 2025.

[23] « Introduction to NumPy. » *W3Schools*, https://www.w3schools.com/python/numpy/numpy_intro.asp. Consulté le 25 mai 2025.

[24] Jain, Sandeep, et Step Guide. « What is Tkinter for Python? » *GeeksforGeeks*, 24 avr. 2024, https://www.geeksforgeeks.org/introduction-to-tkinter/. Consulté le 25 mai 2025.