Contextualizing Mobile Network Dynamics: Advances in Adaptive Video conferencing

1. L.P Rakotondrazaka	Telecommunication, Automation, Signal and Images Research Laboratory (LR - TASI) (lovasoa.rlp@gmail.com)
2. M.A Rafidison	Doctoral School in Sciences and Technics of Engineering and Innovation University of ANTANANARIVO PO Box 1,500 Ankatso Antananarivo - MADAGASCAR (mamynyaina@gmail.com)
3. H.M Ramafiarisona	Doctoral School in Sciences and Technics of Engineering and Innovation University of ANTANANARIVO PO Box 1,500 Ankatso Antananarivo - MADAGASCAR (mhramafiarisona@yahoo.fr)

ABSTRACT

In the field of mobile networks, characterized by their dynamic and often unpredictable nature, this article explores cutting-edge advances in adaptive video conferencing. Our innovative solution addresses these challenges by integrating a mobile application with a bandwidth monitoring module, a video compression module specifically designed for mobile network conditions, and an AES encryption module to ensure the security of the data exchanged. On the server side, we took a virtualized approach, leveraging virtual machines (VMs) and Docker, to improve scalability and resource efficiency. This comprehensive approach aims to address the challenges posed by changing network conditions, providing users with an adaptive and seamless video conferencing experience, regardless of bandwidth variations and network unforeseen events. By exploring the integration of mobile-specific modules and server virtualization, this research contributes to the ongoing dialogue on optimizing video communication in the dynamic mobile network landscape. In terms of performance, our solution aims to provide optimal video quality by dynamically adjusting the resolution based on the available bandwidth. Video compression by interpolation optimizes bandwidth usage without compromising visual quality too much. Additionally, server virtualization ensures efficient resource management, thereby improving the scalability of the application to meet growing demands. This comprehensive approach results in a more reliable, adaptable and secures video conferencing experience, redefining the standards of communication in the complex context of mobile networks.

Keywords: Mobile Video Conferencing, Contextual Application, Video Compression by Interpolation, AES Encryption, Virtual IT Environment.

1- Introduction

Since the advent of video conferencing in the 1960s, technological advances have transformed this communication modality from expensive systems to everyday consumer applications.

The evolution of mobile networks, from 3G to 5G, has considerably influenced video conferencing. Challenges related to mobility, variable bandwidth and latency are in focus. Previous research has explored adaptive mechanisms to optimize the quality of real-time communications.

Despite progress, questions remain, including managing network quality and adapting the Video Conferencing Application to rapid changes in bandwidth.

In this article, we will explore the challenges of video conferencing over mobile networks, highlighting the need to adapt to network fluctuations. First, we'll look at the introduction which sets the context for mobile video conferencing. Next, we'll dive into the context of mobile video conferencing. Third, we will focus on the context-aware mobile video conferencing application. We'll detail its fundamental purpose and key features, including modules for bandwidth monitoring, interpolation video compression, and AES encryption.

Next, we'll explore the application server, breaking down the components of the front end, REST API, backend, and looking at things like application servers, XMPP, databases, file servers, virtual environment, Docker containers, Linux Ubuntu Server 18 operating system, Nginx web server, and communication and security protocols. We will discuss the results and evaluation of the application.

In conclusion, we will summarize the key points discussed in the article and an evolutionary perspective.

2- Context of mobile video conferencing:

In the current panorama of digital communication, mobile video conferencing has emerged as an essential vector of connectivity. It allows individuals, businesses and educational institutions to come together virtually, transcending physical boundaries to enable real-time collaboration. However, despite the considerable benefits it offers, mobile video conferencing faces a complex set of challenges that merit careful consideration.

Table 01: Summary of the main features of each Mobile Network Generation

Mobile Network type	Generation	Frequencies	Bandwidth	Maximum Throughput	Key Features
2G	Second	900 MHz, 1800 MHz	30 KHz	236 Kbps (**Low**)	Voice, SMS, low Data Speed.
3G	Third	850 MHz, 900 MHz, 1900 MHz, 2100 MHz	5 MHz (WCDMA)	7.2 Mbps (HSDPA) (**Medium**)	Voice, SMS, Medium Data Speed, Mobile Internet, Streaming Video.
4G	Fourth	Multiple frequency bands	20 MHz (LTE)	1 Gbps (LTE-A) (**High**)	High Data Speed, Voice other LTE (VoLTE), Fast Internet, High Definition Video.
5G	Fifth	Millimeter waves and	Variable	Up to 10 Gbps	Very High Data Speed, low latency,

		sub-6 GHz		(mmWave) **(High)**	Internet of Things (IoT), High Speed Communications.

One of the major challenges facing mobile video conferencing is the variability of network quality. When users engage in video chats on the go, they rely on mobile networks, which are characterized by constantly changing characteristics. Fluctuations in bandwidth, latency and network stability are all parameters that can affect the quality of video conferencing. These variations can manifest themselves subtly or abruptly, impacting the fluidity of exchanges, audio clarity and visual clarity.

Let's take for example the case of the 4G Network, in our previous article entitled **"Evaluation of the QoS of a Mobile Network using Markov Modelling"** during a 4G Drive Test and over a 10-minute section less than half of the journey, the signal level is Good.

Table 02: Summary of 4G Mobile Network of Quality

Qualité du Réseau 4G	Bad	Medium	Good
Expected Service Time (in minute)	2.83 minutes	1.84 minute	3.92 minutes

The essential challenge that arises is therefore to guarantee an optimal user experience, whatever the situation of the mobile network. This quest for excellence is inextricably linked to the ability to adapt to changing network conditions. Indeed, adaptability is the pivot around which the improvement of mobile video conferencing revolves. This involves not only anticipating network fluctuations, but also reacting pro actively to minimize disruptions and maintain communication quality.

With this in mind, this section lays the foundation for our exploration of context-aware video conferencing application. It highlights the challenges faced by mobile video conferencing, emphasizing network variability as a key element. Additionally, it highlights the compelling need for constant adaptation to mobile network conditions to ensure a seamless user experience.

As we progress in this article, we will dive deeper into the mechanisms underlying this adaptation to the network context, as well as the technological innovations associated with it.

3- The context aware mobile video conferencing application

In the quest for excellence in mobile video conferencing, the context-aware application stands as a milestone in technological innovation. We will reveal the mysteries of this application by highlighting its fundamental objective and its key functionalities, while highlighting the central role of its mobile network bandwidth listening module in establishing context sensitivity.

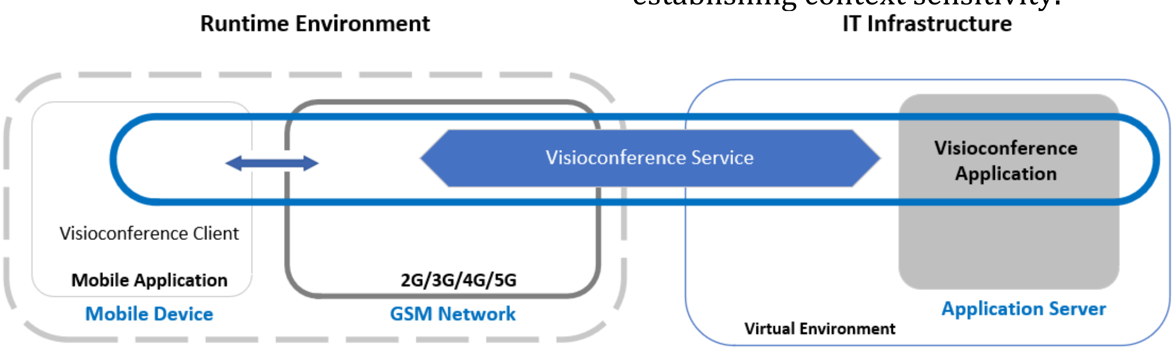

Figure 01: Context-sensitive video conferencing service

3.1 Fundamental objective

The overarching goal of this application is to optimize the quality and stability of mobile video conferencing, intelligently adapting to changing mobile network conditions. It strives to ensure a smooth and seamless user experience, regardless of any network challenges.

3.2 Key features of application

This application comes with a set of key features that converge towards achieving its goal.

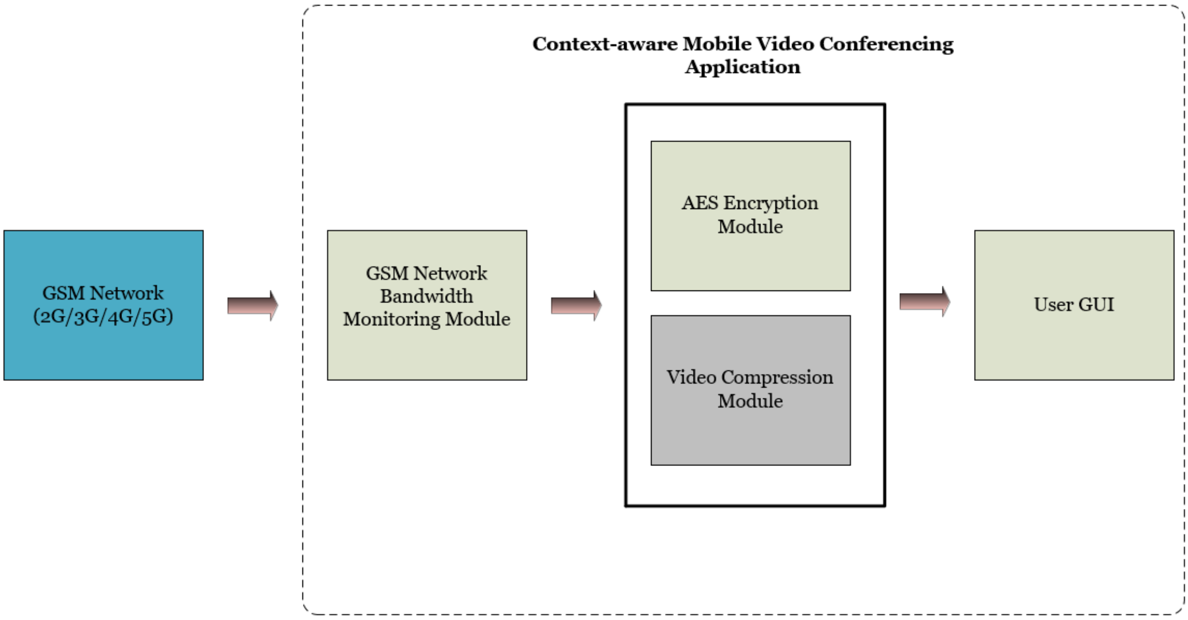

Figure 02: List of key features

3.2.1 Mobile network bandwidth listening module

The listening module constitutes the backbone of this application. Its ability to discern and react to variations in the mobile network gives the application unparalleled context sensitivity. By being able to determine whether the network is optimal or has constraints, the application can adapt its settings to ensure a smooth video conferencing experience.

The listening module continuously monitors the mobile network bandwidth, categorizing the network status into three levels: **Low**, **Medium** and **Good**. This real-time evaluation constitutes the foundation on which the context sensitivity of the application rests.

Depending on the network status detected by the listening module, the application makes real-time decisions to adjust the quality of the video conference.

3.2.2 Video compression module by interpolation

At the heart of the context-aware video conferencing application is the essential notion of interpolation video compression, a crucial technology for data security in an ever-changing mobile network environment. This section delves into this concept, explains how it is implemented to preserve data security, and describes how the application enables or disables this feature in response to changing mobile network quality.

Demonstration: Linear Interpolation Formula

Heuristic: The closer a pixel is, the higher the weight assigned

Principle: Line fitting with polynomial fitting (analytical formula)

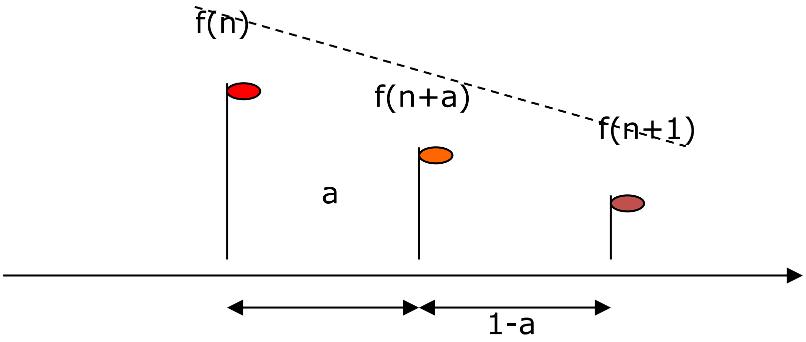

Figure 03 : Polynomial Representation of Linear Interpolation

$$f(n+a) = (1-a)\times f(n) + a\times f(n+1),\ 0<a<1 \quad (01)$$

Note: when a=0.5, we simply have the average of two functions

Numerical Examples

$$f(n)=[0,120,180,120,0] \quad (02)$$

Interpolate at 1/2-pixel

$$f(x)=[0,60,120,150,180,150,120,60,0],\ x=n/2 \quad (03)$$

Interpolate at 1/3-pixel

$$f(x)=[0,20,40,60,80,100,120,130,140,150,160,170,180,\ldots],x=n/6 \quad (04)$$

A Guarantor of Data Security, video compression by interpolation is a technique that optimizes the transmission of video using intelligent interpolation methods. It allows you to reduce the amount of video data without significantly compromising visual quality. This is particularly crucial in conditions where bandwidth is limited, as is often the case in mobile networks.

Image Interpolation Algorithms

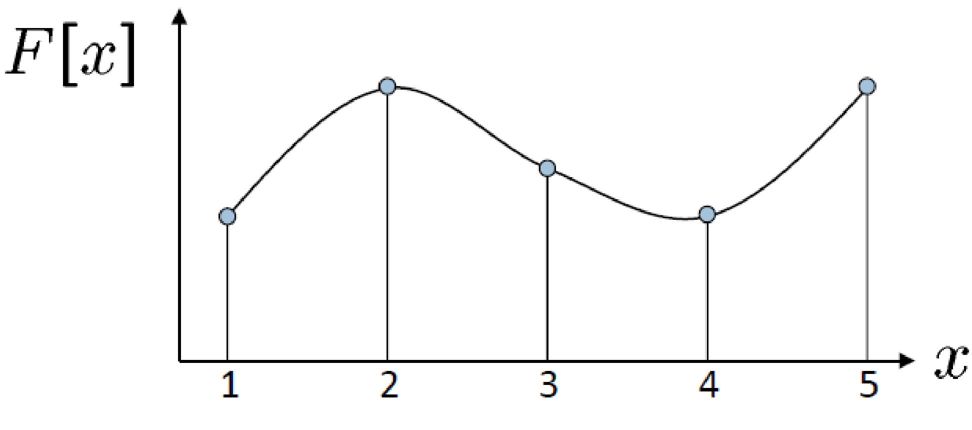

Figure 04 : Example of Formation of a Digital Image for d=1

$$F[x, y] = \text{quantize } \{f(xd, yd)\} \quad (05)$$

- This is a discrete point sampling of a continuous function.
- If we could somehow reconstruct the original function, any new image could be generated, at any resolution and scale.

A digital image f (n1, n2) can be considered as a sampled region of a analog image f (x,y) having continuous coordinates.

$$f(n1, n2) = f(x,y)\ \Big|_{z= n1\ T1,\ y= n2\ T2} \quad (06)$$

As already described above, T1, T2 are the sampling intervals along the axes $x, y,$ if the analog image f(x, y) is band limited:

$$F(\Omega_1, \Omega_2) = 0 \text{ for } |\Omega_1| \geq \frac{\pi}{T_1},\ |\Omega_2| \geq \frac{\pi}{T_2} \quad (07)$$

And if the sampling frequencies are higher than the Nyquist frequencies, it can be recovered from the sampled image f (n1, n2) using the sinc interpolation formula:

$$f(x,y) = \sum_{n1=-\infty}^{\infty} \sum_{n2=-\infty}^{\infty} f(n1, n2) \frac{\sin\frac{\pi}{T1}(x-n1\ T1)}{\frac{\pi}{T1}(x-n1\ T1)} \frac{\sin\frac{\pi}{T2}(x-n2\ T2)}{\frac{\pi}{T2}(x-n2\ T2)}$$

(08)

During transmission, only residual images and information about key frames are sent. The receiver reconstructs the video sequence using this data to decode and display the images. This section has shed light on the fundamental role of video compression through interpolation in data security, explaining how the context-aware video conferencing application dynamically reacts to enable or disable this function based on mobile network quality. In the next section, we will further explore security aspects, including the role of Advanced Encryption Standard (AES) in protecting sensitive data.

3.2.3. Advanced Encryption Standard (AES) Encryption Module

The AES encryption module is an essential component of our context-aware video conferencing application. Its primary role is to ensure the security of data transmitted during video calls, utilizing the AES encryption algorithm.

AES-128 encrypts a 128-bit plain text block using a 128-bit cryptographic key block. These two blocks are represented by two arrays of 16 bytes, each composed of four rows and four columns. Such an array is called a data state or an AES state in the following. A round function is applied to a data state at each round. For AES-128, 10 rounds are necessary to create an encrypted block. For each round, a round key is used and generated by a key scheduling algorithm from the original secret key. The decryption procedure differs from encryption by using the round keys in reverse order and by the reverse application of calculations performed in the round function.

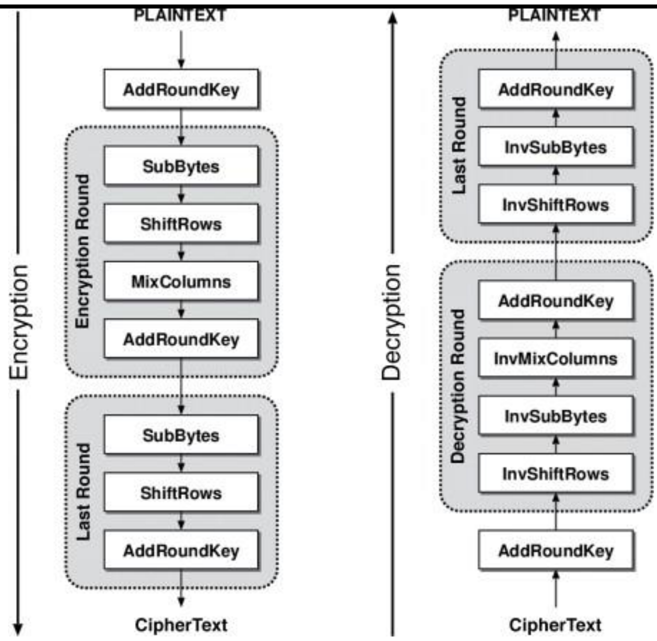

Figure 05: Main construction of AES algorithm: (left) Encryption and (right) Decryption.

- AddRoundKey

Adding a round key to the state using a simple XOR process. The round key is added by XORing each byte of the data state with the corresponding byte of the round key. The size of the round key is therefore the same as that of the manipulated data state, i.e., 128 bits. It is noteworthy that the round key for the first application of AddRoundKey corresponds to the original cryptographic key. The XOR operation of the round key with the state matrix provides a means of introducing the secret key information into the encrypted data. It ensures that each encryption cycle uses a different part of the extended key, thereby enhancing the security of the encryption process. The XOR operation is chosen for its cryptographic properties, including reversibility and its ability to create a one-to-one correspondence between bits.

- SubByte

This operation is the only non-linear transformation, ensuring the confusion property. It involves substituting one byte with another and is applied to each of the 16 bytes of an internal state. This substitution is called an

S-box. The SubBytes transformation acting on a byte is illustrated in Figure 04. It is performed using the same

S-box defined over GF(28).

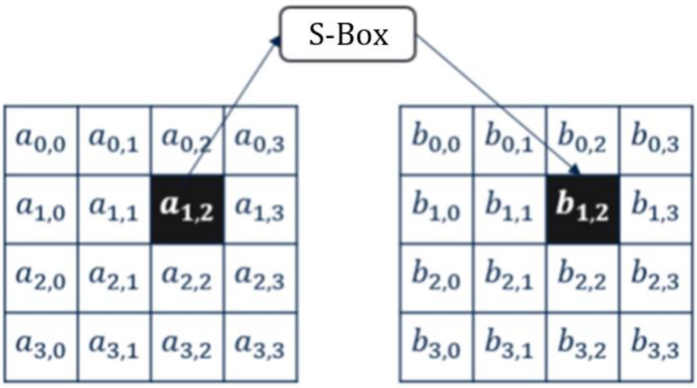

Figure 06: S-Box for AES Substitution

An S-box is often precomputed before the execution of AES-128 and stored in a Lookup Table (LUT). Figure 06 illustrates all possible substitutions of a byte in its hexadecimal notation in a double-entry table. It is also possible to represent the AES S-box by composing an inverse function and an affine function.

The substitution of a byte 'a' in the internal state by the AES S-Box, denoted as SBox, is defined by the following algebraic decomposition:

$$SBox(a) = AF_{AES}(INV_{AES}(a)) \quad (09)$$

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 07: Lookup Table for AES-128 S-Box for a Byte in Hexadecimal Notation, starting with the row and then the column. For example, the byte 9a is substituted with the byte b8.

Like this:

- $AF_{AES}(a)$ is an affine transformation defined by $AF_{AES}(a) = M_{AES}(a) \oplus CST_{AES}$, (10)

where the matrix MAES is defined over $GF(2)^8 \times GF(2)^8$ by:

$$M_{AES} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (11)$$

and the constant CSTAES is defined by the 8-bit column vector

$$CST_{AES} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \qquad (12)$$

The operation INV_{AES} is defined by $INV_{AES} : a \in GF(2^8) \longmapsto a^{254} \in GF(2^8)$,meaning the multiplicative inverse of **a** in the field $GF(2^8) \simeq GF(2)[a]/(a^8 + a^4 + a^3 + a + 1)$. (13)

- ShiftRows

The cyclic shift of different bytes shifts the numbers. This linear transformation cyclically shifts the rows by a data ratio to the left, as shown in the figure below. In particular, the first row is not shifted, the second is shifted by one position, the third by two positions, and the fourth by three positions. These positions are chosen to ensure the diffusion property of the algorithm.

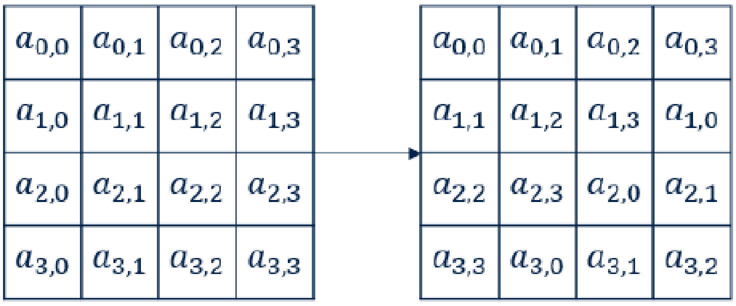

Figure 07: ShiftRows Operation on an AES-128 Data State

- MixColumn

This linear function contributes to the diffusion property by mixing the columns of a data state. It takes a column of the state as input and multiplies it by a matrix, as shown in the figure below.

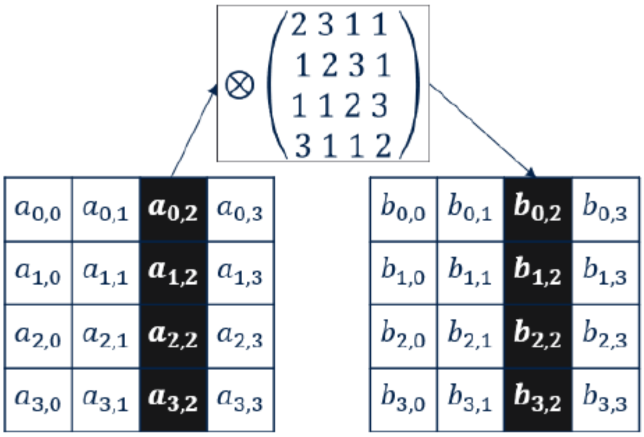

Figure 08: MixColumns Operation on a Column of an AES-128 Data State

4. Context-Aware Video Conferencing Application Server

The technical architecture is the core of our context-aware mobile network video conferencing solution. Our solution introduces a "Modular Architecture," embodying intricate engineering that enables our application to comprehend and adapt to real-time variations in the mobile network. In this section, we will delve into this architecture, unveiling the essential components and mechanisms that make it operational. From context management to security protocols, we will reveal how each element of this architecture contributes to creating a seamless user experience, marking a significant advancement in the field of mobile video conferencing.

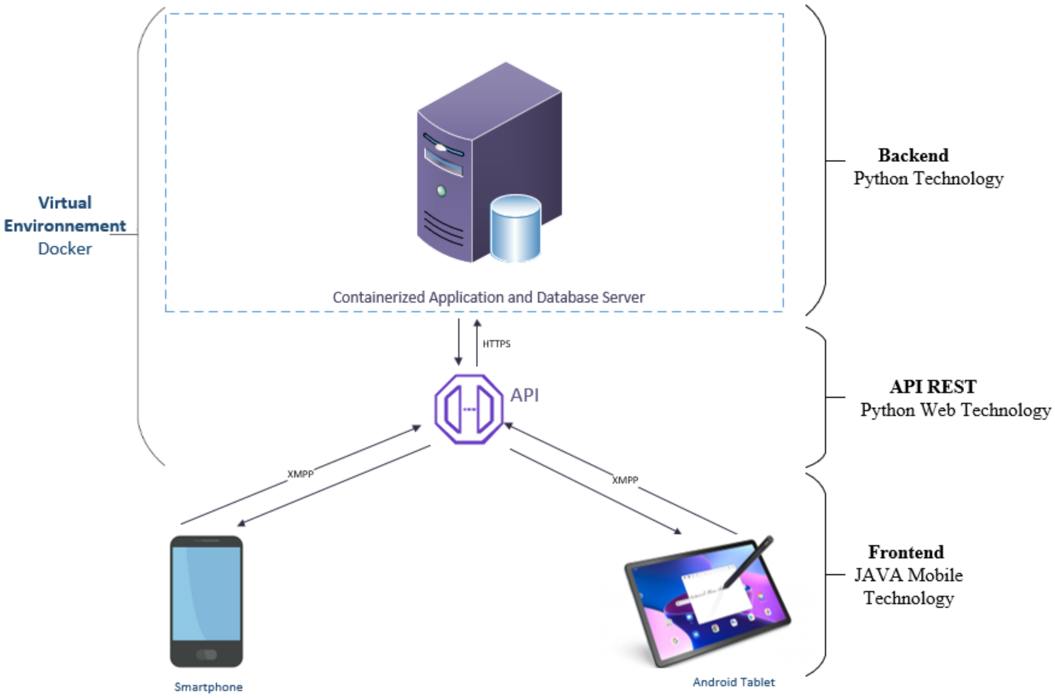

Figure 09 : Technical Architecture of the 'Context-Aware Video Conferencing' Solution

4.1. Frontend

The frontend is responsible for data presentation and user interaction. It collects user inputs, displays information on the screen, and manages communication with the backend when necessary.

4.1.1. Mobile Application

In addition to the web frontend, our solution includes a dedicated mobile application to provide an optimal experience on mobile devices. This application is designed to operate on Android platforms, offering a native interface and mobile-specific features such as push notifications and offline access.

4.2. REST API

To facilitate communication between the frontend (web and mobile) and the backend, we have implemented a REST API. This API exposes endpoints that allow frontend clients to retrieve data, send updates, and perform various operations related to projects and tasks.

Tableau 03 : Comparison of REST and SOAP APIs

Critère	API rest	API soap
Format des données	Utilise généralement JSON (JavaScript Object Notation) ou XML (eXtensible Markup Language).	Utilise principalement XML.
Protocole de communication	Utilise des protocoles légers comme HTTP (Hypertext Transfer Protocol) ou HTTPS.	Utilise des protocoles plus lourds comme HTTP, SMTP (Simple Mail Transfer Protocol), ou JMS (Java Message Service).
Facilité d'utilisation	Plus facile à utiliser, car les données sont généralement lues directement dans le corps de la demande HTTP.	Plus complexe en raison de la structure XML et des besoins de configuration supplémentaires.
Performance	Généralement plus rapide en raison de la simplicité de la structure de données et de l'utilisation de protocoles légers.	Peut être plus lent en raison de la surcharge liée à l'utilisation d'XML et des protocoles plus lourds.
Flexibilité	Très flexible en raison de l'utilisation de formats de données légers et de la conception orientée ressources.	Moins flexible en raison de la rigidité de la structure XML et des conventions strictes.
Visibilité	Facile à comprendre en raison de l'utilisation de standards Web comme HTTP.	Moins visible en raison de la complexité des messages XML et des actions nécessaires pour accéder aux services.
Sécurité	Peut être sécurisé avec HTTPS, mais la sécurité dépend souvent de l'implémentation spécifique.	Offre des normes de sécurité intégrées telles que WS-Security.
État de l'application	REST est sans état (stateless), ce qui signifie que chaque requête du client au serveur doit contenir toutes les informations nécessaires pour comprendre et traiter la demande.	SOAP peut être sans état (stateless) ou avec état (stateful), selon la mise en œuvre.
Compatibilité avec les navigateurs	Facilement exploitable par les navigateurs en raison de son utilisation du protocole HTTP.	Peut rencontrer des problèmes de compatibilité en raison de la complexité et des contraintes imposées par certains navigateurs.

The REST API (Representational State Transfer Application Programming Interface) is a crucial component of our context-aware mobile video conferencing application, especially when using the Django framework for its development.

- What is the REST API?

The REST API is a set of rules and conventions for creating programming interfaces that enable communication between different parts of an application or between distinct applications. It is based on the principles of the REST architecture, which promotes a simple and consistent data exchange using standard HTTP operations such as GET, POST, PUT, and DELETE.

- Role in the Application

In the context of our video conferencing application, the REST API enables communication between mobile clients (applications on user devices) and the application server. It plays a central role in managing application features such as creating video conference sessions, user management, data exchange, and real-time update reception.

4.3. Backend

4.3.1. Application Server

The application server is the heart of our solution. It handles business logic, processes user requests, interacts with the database, and provides services such as project, task, and user management. We use Python as the runtime environment, with Django as the framework to simplify backend development.

4.3.2. XMPP Server

The acronym XMPP refers to "Extensible Messaging and Presence Protocol," a protocol for extensible messaging and presence in online communications. XMPP is based on the client-server architecture and the open XML standard, where an XMPP client on the user's terminal communicates with other subscribers via an XMPP server. In our study, we will use Ejabberd, an open-source instant messaging server known for its reliability, high performance, and ability to handle real-time communications on a large scale. It offers a range of powerful features, making it an ideal choice for context-aware mobile network video conferencing applications.

At the core of the technical architecture of our video conferencing application, the Ejabberd XMPP Server module plays an essential role. Here is a detailed explanation of its operation in this context. The Ejabberd XMPP Server module manages real-time communications, including instant messaging and signaling for video conference calls. Here's how it contributes to the efficiency of our application.

4.3.3. Database

The database stores all crucial data for our application, including information about projects, tasks, users, etc. We use PostgreSQL as a relational database management system, ensuring the robustness, reliability, and scalability of our solution.

4.3.4. File Server

To manage attachments and documents associated with projects and tasks, we have a dedicated file server. It securely stores and provides files to authorized users.

4.4. Computing Environment

4.4.1- Virtual Environment

A virtual computing environment refers to creating a virtual space that allows running applications and operating systems on a software layer rather than directly on physical hardware.

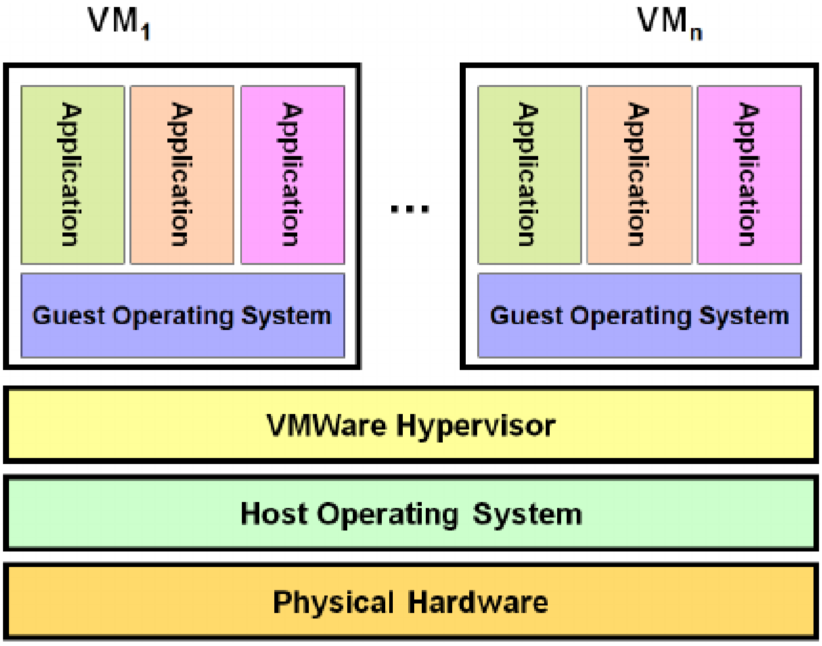

Figure 10: Virtual Information Technology Environment

This technology offers significant advantages in terms of isolation, management, and flexibility. In the context of the Context-Aware Mobile Video Conferencing Application for the mobile network, the use of a virtual computing environment is of great importance to ensure the proper functioning of the system.

Table 04: Virtual Machine Specifications Used

Virtual Machine		
vCPU	vRAM (Go)	HDD (Go)
2	1	40

4.4.2. Docker Containers

Docker containers are lightweight and portable software environments that encapsulate an application and all its components, including code, libraries, and dependencies, into a single, standalone package. This technology provides significant isolation, efficiency, and ease of deployment. In the context of the Context-Aware Mobile Video Conferencing Application for the mobile network, the use of Docker containers plays a crucial role in ensuring smooth management of the application components.

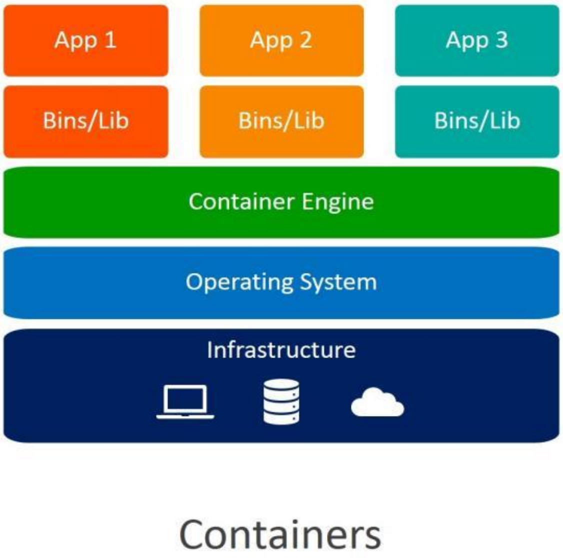

Figure 11 : Docker container

4.4.3. Operating System: Linux Ubuntu Server 18

Linux Ubuntu Server 18 is a Linux distribution specifically designed for server environments. It offers high robustness, security, and stability, making it a wise choice for systems that require continuous availability and optimal performance. Ubuntu Server is widely recognized for its user-friendliness, ease of management, and a broad range of features.

4.4.4. Nginx Web Server

Nginx is a high-performance open-source web server widely used for serving web pages and applications. It stands out for its lightweight design, speed, and ability to handle heavy web traffic loads. In the context of the Context-Aware Mobile Video Conferencing Application for the mobile network, the integration of Nginx is of significant importance to ensure efficient resource distribution and traffic security.

4.4.5. Communication and Security Protocol

HTTPS, short for "HyperText Transfer Protocol Secure," is a widely used secure communication protocol on the Internet. It is essential for securing data exchanges between a user and a web server. HTTPS ensures that data is encrypted and protected against unwanted interceptions. In the context of the Context-Aware Mobile Video Conferencing Application for the mobile network, the adoption of HTTPS is crucial to ensure the confidentiality and integrity of exchanged sensitive data.

TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are security protocols that provide a layer of data encryption during communication over the Internet. These protocols are used to establish secure connections between a client (in this case, the mobile video conferencing application) and a server. They ensure the confidentiality and integrity of exchanged data, as well as the authentication of the parties involved. In the context of the Context-Aware Mobile Video Conferencing Application for the mobile network, TLS/SSL is essential to secure the transmission of video and audio streams.

5. Results and Evaluation

Our Mobile Application provides users with a user-friendly and intuitive interface for easily planning, joining, and managing video conferences. Video call, screen sharing, and chat controls are generally accessible with a simple touch.

When the application detects a mobile network in "Low" mode or with limited bandwidth, it activates video compression by interpolation. This intelligent compression reduces the amount of video data to be transmitted, enabling smoother communication despite network limitations. However, it does so while ensuring that the video quality remains acceptable for users.

Table 05 : Minimum Required Configuration for Mobile Phones

Software	Hardware	
Android	**Random Access Memory (RAM)**	**Storage Space**
Version 7.0	1Go	1Go

One of the key features of the application is its ability to dynamically enable or disable video compression through interpolation. The application continuously monitors the conditions of the mobile network using its bandwidth monitoring module. When the network degrades and bandwidth decreases, the application promptly reacts by activating compression.

Conversely, when the network returns to a higher quality state, the application can disable video compression through interpolation to provide the best possible video quality while maintaining data security. This dynamic approach allows users to enjoy a smooth and high-quality video conferencing experience, adapting in real-time to changing conditions in the mobile network.

When a user initiates a video conference, the AES encryption module automatically generates a unique encryption key for the ongoing session. This key is used to encrypt all video and audio data transmitted between participants. Before transmitting data, the application encrypts it using the AES key. The AES algorithm transforms this data into an unreadable form without the appropriate decryption key. This ensures that even if the data is intercepted, it remains secure.

Table 06: Advantages of AES Cryptography

Advantages
Fast Encryption/Decryption
Handling Large Volumes of Data Encryption
Relatively Short Keys
Low System Resource Usage

On the other end of the communication, the AES encryption module automatically decrypts the received data using the same encryption key. This allows users to seamlessly see and hear the video and audio.

Thanks to AES encryption and intelligent key management, our application provides end-to-end security, meaning that only legitimate users with the appropriate decryption key can access the data. With the AES encryption module, users can be assured that their video conversations remain confidential and secure, even in varying mobile network conditions.

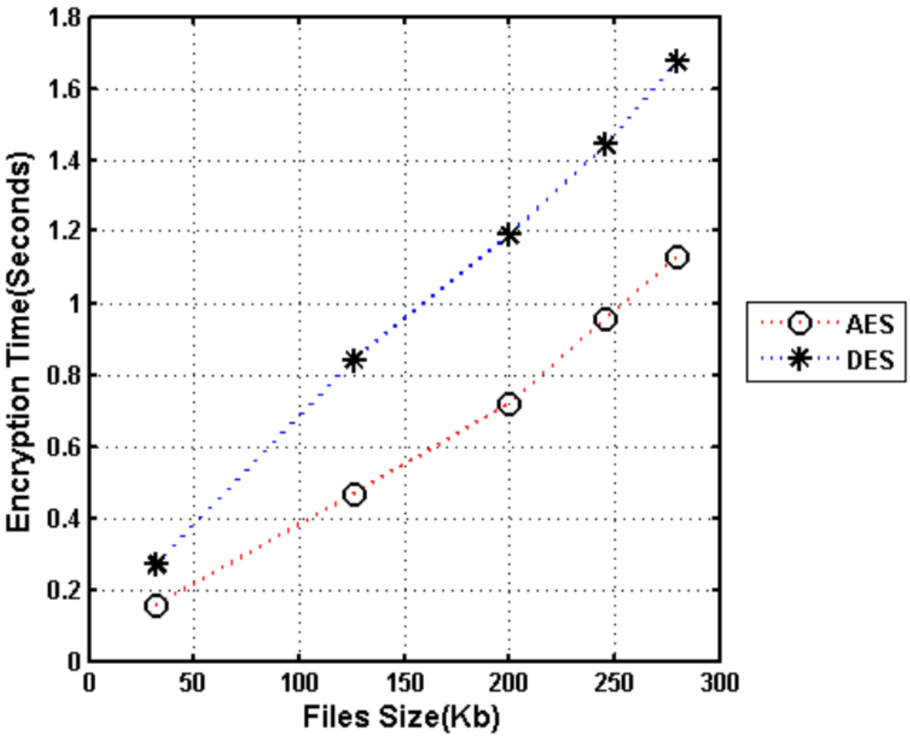

Figure 12: AES and DES Encryption Time Comparison

The AES encryption module plays a crucial role in protecting users' privacy and data security during their video conferences. It ensures that only authorized individuals have access to the exchanged information, thereby enhancing trust in our context-aware mobile network video conferencing application.

In terms of IT infrastructure, our choice has focused on a virtual computing environment, referring to the creation of a virtual space that allows the execution of applications and operating systems on a software layer rather than directly on physical hardware. This technology offers significant advantages in terms of isolation, management, and flexibility. In the context of the Mobile Network Context-Aware Video Conferencing Application, the use of a virtual computing environment is of great importance to ensure the proper functioning of the system.

Table 07: Native Server vs. Virtual Server Deployment Comparison

Features	Native Server	Virtual Server
Definition	A dedicated physical server for a specific task.	A virtual instance running on a shared physical server.
Cost	Higher initial cost for dedicated hardware.	Potentially lower cost by sharing physical resources.
Isolation	Complete isolation of server resources.	Virtual isolation between different instances.
Scalability	Limited by the physical server's capacity.	Easier scalability by adding or removing virtual instances.

Flexibility	Less flexible in terms of dynamic changes.	More flexible, allowing dynamic resizing of resources.
Resource Usage	Generally more efficient use of hardware resources.	Efficient resource consumption is possible but depends on the hypervisor and sharing.
Deployment Time	Deployment may take longer due to purchase, configuration, and installation of hardware.	Faster deployment with quick creation of virtual instances.
Redundancy	More complexity in setting up physical redundancy.	Redundancy can be more easily implemented with virtual instances spread across multiple servers.
Maintenance	Maintenance requires server downtime.	Maintenance can often be performed without interruption through live migration of instances.
Environmental Impact	May be less environmentally friendly due to exclusive use of hardware resources.	Potentially more environmentally friendly due to resource consolidation and energy optimization.

The decision to implement a virtual computing environment in the architecture of the Context-Aware Mobile Video Conferencing Application is justified by several crucial reasons:

- Virtual environments enable the isolation of each component of the application, including database servers, application servers, and XMPP servers. This isolation enhances security by preventing potential interference between different elements of the system.

- A virtual environment centralizes resource management, making updates, monitoring, backup, and software patch management much more straightforward. This significantly simplifies the tasks for system administrators.

- The use of a virtual environment allows for easy addition of new virtual nodes or scaling resources as needed without requiring significant hardware investments.

- A virtual environment optimizes the use of existing hardware resources, reducing costs associated with purchasing and maintaining dedicated physical servers.

- Virtualization offers great flexibility, allowing application components to be deployed on virtual machines in a containerization environment like Docker. This facilitates application management and the addition of new features.

Overall, the use of a virtual computing environment perfectly aligns with the needs of the Context-Aware Mobile Video Conferencing Application in terms of security, management, scalability, and flexibility. This approach contributes to ensuring the efficient and reliable operation of the application while allowing optimal resource management.

The adoption of Docker containers in the architecture of the Context-Aware Mobile Video Conferencing Application is based on several determining factors:

- Docker containers provide complete isolation, ensuring that each component of the application operates independently without interfering with other elements. Additionally, they are portable, meaning they can run consistently across different environments, whether development, testing, or production servers.

- Docker containers are incredibly lightweight and quick to deploy. They optimize the use of hardware resources while reducing the overhead associated with traditional virtualization.

- Docker container management is simplified with centralized management tools and the ability to deploy, update, and monitor containers automatically.

- Docker containers are designed to scale easily, making them ideal for meeting the application's usage peaks.

- Docker technology supports various environments and operating systems, offering great flexibility for deploying the application on different platforms.

In summary, the use of Docker containers is essential to ensure the isolation, portability, efficiency, ease of management, scalability, and flexibility required for the Context-Aware Mobile Video Conferencing Application. It also streamlines the application development and deployment process, contributing to its efficiency and reliability.

The choice of Linux Ubuntu Server 18 within the architecture of the Context-Aware Mobile Video Conferencing Application is based on several essential advantages. Firstly, Ubuntu Server offers enhanced security through regular updates and long-term support, ensuring the protection of sensitive user data. Additionally, it has a vast user and developer community, facilitating issue resolution and access to valuable resources.

Furthermore, Ubuntu Server is highly customizable, allowing the configuration of servers tailored to the specific needs of the Video Conferencing Application. Its compatibility with a wide range of open-source software and native support for essential technologies such as Docker simplifies the development, deployment, and management of the application.

Lastly, Ubuntu Server is renowned for its performance and reliability, fundamental for ensuring the availability and responsiveness of the video conferencing application, even in varied network conditions. Its use within the architecture ensures a solid foundation for the application's backend, providing an optimal user experience and high-quality video communications.

The decision to integrate the Nginx web server into the architecture of the Context-Aware Mobile Video Conferencing Application is based on several crucial advantages:

- Nginx is known for its high performance, ability to handle many users simultaneously, and efficient resource distribution. This ensures a smooth user experience when using the video conferencing application, even under heavy loads.

- Nginx supports load balancing, distributing traffic across multiple backend servers, improving the stability and availability of the application.

- Nginx offers advanced security features, including SSL/TLS certificate management, protection against DDoS attacks, and communication security. This is essential for ensuring data confidentiality and user security.

- Nginx optimizes the use of system resources, reducing memory consumption and improving server stability.

- Nginx is highly configurable and can be adapted to the specific needs of the video conferencing application, providing great flexibility.

The integration of Nginx into the architecture of the Context-Aware Mobile Video Conferencing Application ensures high performance, efficient load balancing, advanced security management, and optimization of application resources. This guarantees a quality user experience and reliable distribution of application resources.

The decision to implement HTTPS in the architecture of the Context-Aware Mobile Video Conferencing Application is based on several fundamental considerations:

- HTTPS encrypts all data transmitted between the mobile application and the server, ensuring the confidentiality of exchanged information, including video and audio streams.

- The HTTPS protocol incorporates advanced security mechanisms, such as server identity verification (SSL/TLS authentication), providing robust protection against attacks such as data interception (MITM) and malicious intrusions.

- Users are increasingly aware of the importance of online security. Activating the green padlock in the web browser's address bar is a trust-inducing sign that strengthens the application's credibility in the eyes of users.

- HTTPS is often required to comply with data protection regulations such as GDPR and security requirements for mobile applications.

- HTTPS implementation is widely supported by many web servers and is relatively simple to implement.

In summary, the adoption of HTTPS in the architecture of the Context-Aware Mobile Video Conferencing Application is crucial to ensure data security, protection against attacks, user trust, and compliance with security standards. It is a critical element to guarantee the confidentiality and integrity of communications within the application.

The integration of TLS/SSL into the architecture of the Context-Aware Mobile Video Conferencing Application is based on the following major benefits:

- TLS/SSL encrypts all data transmitted between the mobile application and the server, ensuring that video and audio streams remain confidential and unintelligible to any malicious third party.

- SSL/TLS certificates allow verifying the identity of the server, confirming that the application connects to the correct server and not a malicious entity.

- TLS/SSL provides robust protection against attacks such as data interception (MITM) by verifying data integrity and providing enhanced security against threats.

- TLS/SSL implementation is often a requirement to comply with regulations and security standards, crucial in the context of context-aware video conferencing.

- The presence of the green padlock in the browser or application address bar enhances user confidence in communication security.

In summary, the integration of TLS/SSL into the architecture of the Context-Aware Mobile Video Conferencing Application is crucial to ensure confidentiality, authentication, protection against attacks, and compliance with security standards. It is an essential component to secure video and audio streams during video conferencing.

In their article "Modeling of multimedia architectures : the case of video conferencing with guaranteed quality of service," Philippe OWEZARSKI and Marc BOYER also propose a video conferencing solution based on Petri Nets, but unlike ours, their solution is an asynchronous video conferencing solution.

6. Conclusion

In conclusion, this article has explored significant advancements in the field of adaptive video conferencing in the context of dynamic mobile networks. We have highlighted the growing importance of adaptive video conferencing in an always-connected world, where communication quality is essential. By analyzing the complex dynamics of mobile networks, including bandwidth fluctuations, latency, and stability, we emphasized the challenges faced by video conferencing applications. However, technological advancements, such as adaptive video compression, are increasingly overcoming these challenges, allowing for an optimal user experience.

We also addressed the crucial issue of data security in this context, showcasing advanced encryption protocols such as AES.

In conclusion, adaptive video conferencing is poised to play a central role in how we communicate, collaborate, and share information, bringing significant value to various sectors, from business to education and healthcare. Technological advancements will continue to enhance this experience, making adaptive video conferencing an indispensable cornerstone of our connected future.

In summary, these advancements in adaptive video conferencing pave the way for promising prospects, emphasizing the importance of adaptability to the dynamics of mobile networks and suggesting avenues for future improvements. Emerging trends include the use of artificial intelligence for more proactive adaptation, exploration of 6G networks, and deeper integration of augmented reality environments in video interactions. These developments open the door to future research for even more efficient and immersive mobile video conferencing. Standardization efforts will contribute to achieving seamless interoperability in this evolving landscape.

References

[1] N. Ferry, S. Lavirotte, G. Rey, and J.Y. Tigli. Adaptation Dynamique d'Applications au Contexte en Informatique Ambiante. Research Report I3S (Université de Nice- Sophia Antipolis/CNRS), number I3S/RR-2008-20-FR, 36(0), 2008.

[2] B. Grosof, A. Arbor, and M. Kifer. The SILK System : Scalable and Expressive Semantic Rules. In International RuleML Symposium on Rule Interchange and Applications - RuleML'09, 2009.

[3] J. I. Hong, J. A. Landay, and S. Hall. An Infrastructure Approach to Context-Aware Computing. Human-Computer Interaction, 16(2) :287–303, 2001.

[4] Brown, P.J. The Stick-e Document: a Framework for Creating Context-Aware Applications. Electronic Publishing '96 (1996) 259-272.

[5] H. Khlifi and J.-C. Gr. IMS Application Servers : Roles, Requirements, and Implementation Technologies. IEEE Internet Computing, 12(3) :40–51, May 2008.

[6] M.M. Kokar, K. Baclawski, and Y.A. Eracar. Control theory-based foundations of self-controlling software. Intelligent Systems and their Applications, IEEE, 14(3) :37–45, 1999.

[7] R. Laddaga. Creating robust software through self-adaptation. IEEE Intelligent System, 14(3) :26–29, 1997.

[8] P.K. McKinley, S.M. Sadjadi, E.P. Kasten, and B.H.C. Cheng. Composing adaptive software. IEEE Computer, 37(7) :56–64, 2004.

[9] A. Minaburo and J.-C. Point. Signalisation pour la QoS de Bout en Bout Dans les Reseaux NGN. Techniques de l'ingénieur. Télécoms, pages 1–8, 2007.

[10] Brown, P.J. Triggering Information by Context. Personal Technologies, 2(1) (1998) 1-9

[11] Cooperstock, J., Tanikoshi, K., Beirne, G., Narine, T., Buxton, W. Evolution of a Reactive Environment CHI '95 (1995) 170-177

[12] C.C. Kim, S.C. Shin, S.Y. Ha, S.Y. Han, and Y.J. Kim. End-to-end qos monitoring tool development and performance analysis for NGN. Management of Convergence Networks and Services, pages 332–341, 2006.

[13] H. Koumaras, A. Kourtis, D. Martakos, and J. Lauterjung. Quantified PQoS assessment based on fast estimation of the spatial and temporal activity level. Multimedia Tools and Applications, 34(3) :355–374, March 2007.

[14] Chris Stewart and Kristin Marsicano, Android Programming: The Big Nerd Ranch Guide par Bill Phillips, 2019

[15] Reto Meier, Professional Android 4th Edition, 2018

[16] Philippe OWEZARSKI – Marc BOYER, Modeling of multimedia architectures: the case of visioconferencing with guaranteed quality of service

[17] L.P Rakotondrazaka, M.A Rafidison, H.M Ramafiarisona - "EVALUATION OF THE QOS OF A MOBILE NETWORK BY MARKOV MODELING" - European Journal of Research Development and Sustainability (EJRDS) https://www.scholarzest.com - Vol. 4 No 08, August 2023 - ISSN: 2660-5570