International Journal of Networking & Computer Engineering
ISSN 0975-6485 Volume 16, Number 2 (2025) pp. 113-124

http://www.ripublication.com

Architectural Models for Combating Identity Theft Attacks in the Transfer of Financial Flows of NGFS (New Generation of Financial Structures)

TOUDOU MAHAMAN Mabrouk, ISSOUFOU TIADO Mahamadou, ABOUBA Gandou, BOUBACAR TAWAYE Abdoul-Aziz
Department of Mathematics and Computer Science,
Research team on Network and Telecommunication,
University of Abdou Moumouni, BP 10662 Niamey – Niger
mahamanmabrouk@gmail.com, Issoufou_tiado@yahoo.fr, gandouabouba@yahoo.fr, tawaye9799@gmail.com

Abstract

The new technologies linked to the rapidly expanding Internet network have positively led to the development of many activities with the emergence of NGFS (New Generation Financial Structures). Negatively, harmful activities have proliferated, including cybercrime, which always poses new and increasingly complex challenges to scientific research. With cases of system intrusion and identity theft recorded, the limit of the traditional solution has been reached by these NGFS. In this paper, we propose as a first approach, an architectural solution to guarantee security and optimize Quality of Service (QoS). In a second approach, we contribute with a solution based on the intervention of a third party in the model of public and private keys systems [RFC 2716] (example of Kerberos) to certify the identity of customers in transaction. Thus, a new platform is proposed that integrates the contribution of biometrics to achieve an even higher level of security. The mathematical model for calculating the break-even point is also developed with the model for calculating the confidence level.

Keywords: Financial structure, financial transfer, cybercrime, QoS, Security.

Introduction

The capitalization of the advantages of Internet-related technologies has served as the basis for the emergence of NGFS. The overall architecture of the network operated by these structures is based on a simple layout that associates the machines of the

counters with a server managed by these structures. At the current stage of the evolution of their activity, their digital banking nature not only reflects a significant complexity, but also insistently poses in a first dimension the security problem of dealing with cybercriminal acts. In another dimension, it raises the problem of ensuring the level of QoS (Quality of Service) to build customer loyalty when conditions are favourable to them, particularly in a competitive environment. To highlight the main characteristics of this mode of operation of the Internet network by these digital banks, this paper deals specifically with the architecture of the network, the traditional mode of operation before presenting the traditional identity verification system. It makes a detour on the types of cybercriminal attacks with a first level of contribution related to the specification of the available architectural solutions that are internal to the NGFS 's global network.

Network architecture

Description of the architecture

NGFS uses a classic Internet access mode with a mixed architecture based on the trunking between Ethernet local networks, the Internet and GSM (Global System for Mobile communications). The interconnection between the Ethernet backbone and the Internet is usually done via ADSL (Asymmetry Digital Subscriber Line). The NGFS has a main server accessible via this network by the machines of the various counters spread throughout the national territory. The inclusion of the GSM environment in this service for transferring financial flows allows to use instant messaging through SMS (Short Message Service) sent to customers concerned by a transaction.

Mathematical Model of Transaction Volume Invoicing (2MTVI)

The aim here is to establish the mathematical equation that gives the formulas for calculating the break-even point of the initial activity of transferring financial flows. In general, the notion of volume billing is a concept that has already been tried and tested in the world of networks, which is here adapted to the context of this transfer. In a volume-billed Internet access, the ISP gives the price of each megabyte (MB) or a block of megabytes per promotion and the customer charges his Internet account by buying these megabytes which constitute a stock of bits that the customer can use before his account is completely emptied. By transposing the ISP dialectic to the level of NGFS provision, the profitability of the financial flow transfer service is achieved if the conditions of the 2MTVI below are verified. Indeed, the principle of consumer billing is more practical than the setting of a fixed threshold by step based on the range intervals of the amounts to be transferred as initially used at the launch of the NGFS. The flaw of the tiered model is that if X_2 is the threshold for switching from tariff Y to Z (with Z > Y), for an amount Mt to be transferred within the range defined by the NGFS ($Mt \in [X_1, X_2[$), then it is possible to record shortfalls. In other words, if as soon as Mt exceeds X_2, the Service Billing Fee (FFS) goes from Y to Z, then the customer's natural reflex to minimize the FFS is to transfer X_2-1, hence a loss for the NGFS equal to (Z-Y) for a single point of difference.

Taking into account the distribution of the counters of an NGFS throughout the territory and the evolution of its activities, we assume an evolution of new

counters that are added in the architecture from existing offices. The law of the market will dictate that the more the number of counters increases, the more the NGFS develops its activities with a break-even point depending on both the number of transfers (customers) and the amount transferred. The break-even point can be calculated for a counter, and for an area, in which case some counters will compensate for the deficit of the others. The charges are as follows: C_1=rental, C_2=monthly staff salaries, C_3=monthly electricity fee, C_4=monthly depreciation of equipment, C_5=monthly Internet connection fee, C_6=monthly GSM fee, C_7=any other monthly charge:

C_1=0 if the NGFS provides the local

C_2 = amount depending on the number of staff recruited according to the queue

C_3=0 if the NGFS uses solar panels and batteries

C_7 = cumulative amount of any other monthly charges

Mathematical modelling: formula for calculating the gross monthly profit B_G of a counter

Mt_i = Amount transferred by a customer i

Nb_c = Number of customers in the reporting period

$B_G = X * (\sum (i=1..Nb_c) Mt_i)/Y$ with X=NGFS pricing for Y transferred amount

The Break-Even Point for a Counters BEPC in the one-month period is:

$BEPC = B_G – (\sum (i=1..7) C_i)$

The traditional modus operandi

NGFS ensure the transfer of funds between natural persons via a secure Internet connection between the counter and the main server of the NGFS, and then between the sender and the recipient with the constraint of guaranteeing the accuracy of their identities. The NGFS counters are spread across the country. These counters equipped with machines that access the central server form an architecture in itself that is quite complex in terms of size and the number of customers who come to use these services. These parameters describe the nature of the traffic and the amount of requests that can converge on the server, forming spikes at times. The service provided by these NGFS is described as follows:

- The sending customer goes to one of the NGFS counters
- He presents his identity document, gives his telephone number as well as that of his correspondent in addition to the indication of the identity of the latter
- The customer pays the amount to be sent with the transfer fee
- The transaction is recorded on the interface of the NGFS counter application
- Then the transfer order is sent via the Internet to the NGFS server
- The sending customer and his correspondent automatically receive SMS announcing the transfer through their GSM numbers
- The correspondent goes to an NGFS counter in his or her destination city
- He presents his identity document, gives his telephone number and, if necessary, the transfer number and the amount to be received
- The teller queries the NGFS server to verify all this information

- If it is accurate, it simply checks
  - if the face of the correspondent is that of the photo of the identity document provided and whether the first and last names written on the identity document correspond to the information carried by the transfer financial flow
  - in the event of a match, he proceeds to pay the amount.

Traditional Identity Verification System

The traditional solution is to take the correspondents' identity document issued by the administrative authorities and to visually compare the textual information contained in the document with that carried by the financial flow. In the event of a match, the teller then visually compares the photo of the document provided by the receiver with the face he perceives with his eyes in front of him, according to what his vision allows him to observe. From this concordance, the teller concludes that he is the legitimate owner and gives him access to the flow. However, he has no guarantee that the identity document provided is not falsified, nor that the photo of the document corresponds to the face of the person who presents himself. In the case of a resemblance as in the case of identical twins or a simple disturbance of visual abilities, then the fatal error can quickly occur.

Types of Cybercriminal Attacks

Cybercrime is one of the new forms of crime or delinquency on the Internet, which is proving to be the third major threat in the world after chemical, bacteriological and nuclear weapons. There are two categories of cybercrime offenses in particular, identity theft and illegal access to data. The most important types of electronic crime are:

- Traditional forms of crime related to computer crimes: scams, identity theft, fake payment cards, etc.
- Breach of the confidentiality, integrity and availability of data and systems: illegal access, illegal interception of messages, infringement of intellectual property, etc. [1].

Cases of a malicious intrusion into the NGFS system

A lived experience of a cybercriminal act against a NGFS relates to copying application of flow forwarding by a malicious maintainer. Subsequently, the latter uses his own machine, launches the application and connects at late hours to the NGFS server to make large transfers of amounts to neighbouring countries. In this modus operandi, he sends his accomplice constituting the correspondent registered in the financial flow in these countries to recover the stolen flow. Once back, the two cybercriminals share their "loot". This modus operandi lasted for quite a long time before the NGFS managers simply realized the decline in their performance without any other technical means. It is the agents of the cybercrime department who will discover the process thus established which exploits the flaws in the system and the operating mode of this financial flow transfer service.

Cases of impersonation of the recipient

Identity theft is the deliberate impersonation of another person, usually for the purpose of carrying out fraudulent actions, such as accessing finances, committing a misdemeanor or felony, or improperly accessing rights. This is a major risk faced by emerging and sensitive financial structures for money transfers. This spoofing develops with the limitation of the means of authentication by leaving the possibility for a malicious person to appropriate the account or a transferred financial flow belonging to another individual. Concrete cases reveal fake correspondents who use false identity documents to successfully carry out acts of embezzlement. If this previous diagram presents security flaws at the computer level, the involvement of the teller indicates other flaws in the system:

1. Inability to certify that a document provided is legal or false,
2. It is impossible to certify that the correspondent is who he claims to be.

Architectural solutions internal to the NGFS network

Many architectural solutions exist today through several technologies allowing NGFS to face both the security challenge and that of a better QoS for the survival of the financial transfer services they offer. Among these technologies derived from the field of scientific research, we propose to explore the possibilities offered by VPN (Virtual Private Network) [2], MPLS (Multi-Protocol Label Switching) [3] and assurance of QoS guarantee with IntServ (Integrated Services) [4] and DiffServ (Differentiated Services (DS) [5].

Security solutions

In the context of NGFS, we recommend the implementation of an internal VPN linking the NSFC counters and server through the Internet. Indeed, VPN works with tunnel creation by imposing the constraints of (1) user authentication, (2) data encryption, (3) access key management, (4) multi-protocol support. It uses PPTP (Point to Point tunneling Protocol) [6] which uses a PPP connection over an IP network. It uses Internet Protocol Security (IPsec) [7] or MLPS at level 3, and SSL protocol at level 4 [8].

QoS Guarantee Solutions

The purpose of QoS is to manage, optimize, and maximize the use of a network's resources. In addition, QoS must ensure that applications perform well when traffic packets [9]. Taking into account the type difference between all packets, their processing must also follow the same difference [10]. For this reason, QoS models have been defined that determine how these packets should be handled in the network based on their nature. Among the proposals, we present those of the IETF (Internet Engineering Task Force) with The following protocols: IntServ, RSVP (Resource ReSerVation Protocol), DiffServ, MPLS.

IntServ (RFC6437, RFC6780)

IntServ is an Internet traversal solution for NGFS. Its services architecture defines one of the extensions of the Internet's Best Effort (BE) model to provide QoS to

applications. This architecture has several key components, including a set of service definitions, load-controlled service and guaranteed service. It is based on the use of explicit signaling mechanisms to route information to routers that must provide the requested services to the various flows. RSVP is the most widely known example of an initialization mechanism. However, the architecture of IntServ can work with other mechanisms and its services are implemented at the level of network components such as machines, routers, links, more complex entities such as the ATM (Asynchronous Transfer Mode) network, 802.3, including DiffServ networks.

Le RSVP (RFC2998)

RSVP is an Internet traversal solution that accompanies IntsServ for NGFS. It offers signaling for applications to request network resources which responds by explicitly accepting or rejecting. Thus, it signals to the routers its resource needs per flow, using the parameters of IntServ. The routers apply IntServ admission control to report requests. Network nodes traffic control are configured to ensure that each accepted flow receives the requested service in strict isolation from other traffic. This protocol configures micro flow (MF) packet classifiers in the traffic flow path routers and that support the IntServ service. Additional mechanisms are available relating to control policy, access control, authentication and accounting.

DiffServ (RFC4594)

DiffServ is an Internet traversal solution for NGFS. It classifies packets into aggregated streams or "classes" with different priorities. It uses the DSCP (DiffServ CodePoint) placed in the IP header of each packet to specify the type of service to apply. This is a BA (Behaviour Aggregate) classification. Each DiffServ router processes packets with a "Per–Hop Behavior" (PHB) invoked by the DSCP. Thus, the PHB determine the processing corresponding to the flows that have been differentiated in the network. DiffServ is based on the differentiation of services, facilitates scalability, eliminates the need for state and stream processing.

MPLS (RFC5462)

MPLS is a potential bushing solution for NGFS. This standard uses entry nodes in the network called Label Edge Routers (LERs) with the role of assigning labels to packets or frames. Inside the network, forwarding nodes called LSRs (Label Switched Routers) ensure the node-to-node "relaying" of packets using these labels. The path that a packet follows is called the Label Switched Path (LSP). The labels or references included in the frames are distributed using a signaling protocol, the most important of which is the LDP (Label Distribution Protocol). MPLS also offers the possibility of using RSVP, which can be combined with a routing protocol such as BGP (Border Gateway Protocol) or OSPF (Open Shortest Path First).

Solutions based on biometric systems

Definition of Biometrics

Biometrics is a science that studies and values the measurement of an individual's biological characteristics. It is concerned with the identification of individuals on the

basis of mathematical analyses and through biological, behavioral, or morphological attributes that are reliable, tamper-proof, universal, measurable, permanent, non-changing over time, and recordable [11]. Many methods for the recognition of individuals have been developed starting with the identification of the face, fingerprints, iris of the eye, vocal, hand geometry, tine, palm, ear shape, DNA, gait, signature, typing dynamics. In our case of NGFS, we are limited to morphological biometrics, which include fingerprints, facial and voice recognition.

Operation of a biometric device

A biometric device is used through the following steps:

- ✓ Sensors of the biometric data of the individual to be identified (electronic instruments)
- ✓ Conversion of these data into digital form and determination of the characteristic points constituting the data used as a basis for comparison
- ✓ analysis and comparison of these data with those recorded in a repository and determination of a result based on predefined margins of error [12].

The mechanism for recognizing individuals is broken down into two stages:

- The first step, called "Enlistment," is to obtain a representation of the individual's characteristics. This representation is rigorously unique and permanent [13] in order to avoid doubt about any similarity.
- ✓ The second step is the test or recognition stage itself with the receipt of data from a NGFS counter. The test consists of measuring the resemblance between the data provided by the counter and the existing model in the database corresponding to the identity announced.

We propose an identification mode that is based on a "1 to N" comparison in which the system looks for the perfect similarity by comparing the data provided by the counter with the models stored in the database. The following figure provides a descriptive overview of the new system as an illustration of the identification process.

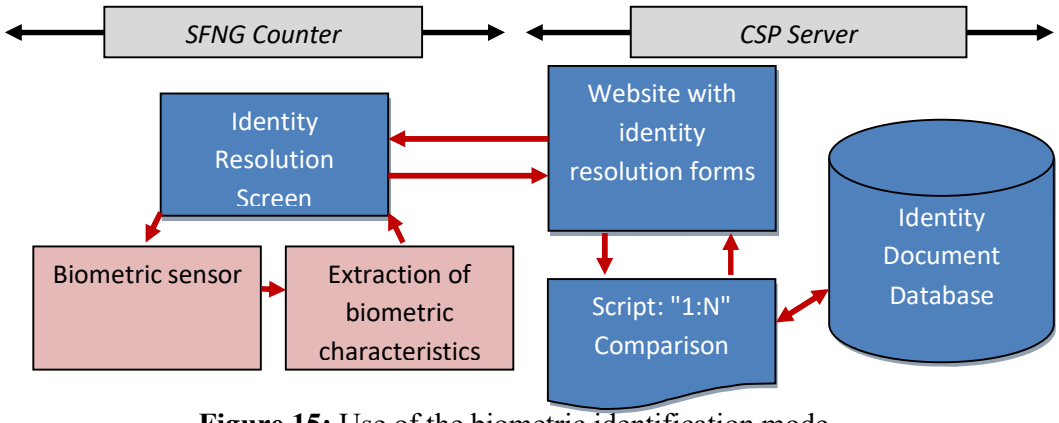

Figure 15: Use of the biometric identification mode

Fingerprint-based identification

The individual or natural person is described by a large number of criteria that refer, for example, to his or her character, personality, image, reputation or cultural, geographical and social origins. By definition, it is possible to consider the identity of the individual through various signs that distinguish him from others and make him unique. Civil status is one of the documents that contributes to the unique identification of an individual as well as an acquired or innate detail such as the shape of the face, nose, forehead, scars, hair color, complexion, fingerprints, DNA (Deoxyribonucleic Acid), etc.

Civil status is of interest to us through the many documents such as the National Identity Card (CNI) and the passport containing information for the identification of individuals, including fingerprints. By definition, it is a design formed by the lines of the skin of the fingers, palms, toes, and soles of the feet. It is a mark that can be left by the finger's contact with a surface, or raised by applying ink to the fingers and then pressing the coated fingers on a support. They are a simple and effective means of identification in many activities [14].

Identification based on voice biometrics

ASR or Automatic Speech Recognition is a mechanism that allows to switch from an acoustic speech signal to transcribing it into a written version. Its realization is based on programming to recognize the speaker. The program includes 4 phases:

0. Phase 1: declaration of speech recognition variables. They are intended to contain, for example, the number of individuals to be identified, and the five (5) voice samples given by each individual. These 5 samples are divided into two groups, 2 for tests and 3 for enrollment or speaker determination phase.
1. Phase 2: enlistment allowing to extract several characteristics from these sounds with special mathematical methods including for example the MFCC (Mel Frequency Cepstrum Coefficients) or FFT (Fast Fourier Transform) method. These characteristics are presented in the form of a comparison database.
2. Phase 3: recognition using testing. The speaker is recognized through the characteristics of his voice extracted from the sensors with the MFCC or FFT methods before being compared to those of the database (speaker signal vs. DB signal) in order to identify matches or not, for acceptance or rejection.
3. Phase 4: fusion with results to improve reliability and increase accuracy of ASR systems. For example, two or more feature extraction methods can be merged, such as MFCC and FFT.

The Comparison Support Base Solution

Medium Confidence Model

We define the Confidence Levels (CL) by considering a scale from 1 to 7 whose points are added by level of sufficiency as indicated in the following table. The first 5 criteria that are under the control of the NGFS have each a cost of 1. The last two most important points that are beyond the control of the NGFS have a cost of 1.5.

Criterion	Point	CL
Existence of the issuing window	1	0/7
Existence of the financial flow	+1	1/7
Issue Date Compliance	+1	2/7
Accuracy of Amount	+1	3/7
Accuracy of the recipient's telephone number	+1	4/7
First total of 5 points (criteria under the control of the NGFS), CL = 4/7		
Conformity of the Recipient's identity (Name and surname)	+1,5	5,5/7
Conformity of the Recipient's identity (Face photo)	+1,5	7/7

Table 6: Definition of Confidence Levels

We define the Medium confidence as a score of 4 on the scale from 0 to 7. All the points that add up at this level are internal to the NGFS for the teller. We define the confidence absolute as being synonymous with the rating of 7/7. Thus, in the traditional identity verification solution described above, tellers place absolute trust on the correspondent who presents himself to appropriate the financial flow transferred as well as in the identity document he presents to prove his identity, i.e. a score of 7 points. Since the document provided can be falsified (1.5 points less) and the individual who presents himself a usurper (1.5 points less), the level of trust that deserves to be granted is normally 4 for the proper functioning of the service due to the existence of at least the financial flow identified with a legitimate issuing counter as well as a compliant amount and telephone number as announced by the correspondent.

If the correspondent gives the number of the flow, the amount and his telephone number, the teller has the financial flow as a means of comparison to verify the veracity of his statement. On the other hand, when the correspondent presents him with an identity document, the teller has no comparison medium to certify its accuracy. It is therefore a visual verification process based on an identity document without a comparison medium. The verification is visual since it is only based on the assessment of the teller by using the photo of the identity document against the face of the natural person who presents himself.

First-level solution based on comparison media

Description of the first principle of certification

A first level of solution consists of deploying a platform on a server with a certification service offer based on comparative visual support that will be provided in real time to the tellers. This service will be provided by an entity referred to herein as a Certification Service Provider or CSP. In its operation, the platform interfaces with the Database (DB) of the state bodies issuing identity documents. Its operation also includes the processing of requests to certify the identity of the people in transaction using comparative analysis algorithms.

In this first level, the certification server simply sends in response to an Identity Resolution Request (IRR) bearing the number of an identity document, all the useful information so that the teller verifies the accuracy of the correspondent's

identity by comparing it with the document provided. And since the CSP server must calculate the amount invoiced per financial flow and per tranche, the RRI must be the same request of the financial flow converging to the NGFS server. In addition, to protect this CSP service from fraudulent use, the server must be locked and its access limited to authorized machines only.

Certification Platform Architectural Model

The architecture of the certification platform is presented with four (4) entities from E1 to E4 and two branches B1 and B2. The E1 entity groups the users' screens. E2 includes the website with the forms for managing the database and resolving identities. The E3 entity is the one for CGI scripts for managing the database and resolving identities. Finally, the database of identity documents is housed in the E4 entity. The first B1 feature branch is related to traditional DB operations and the second branch allows NGFS to perform identity resolution operations. Both branches use user interfaces that are linked to the ID database using Common Gateway Interface (CGI) scripts. The set of all interfaces forms a website or page base. The figure on the following page illustrates the architecture of our certification platform.

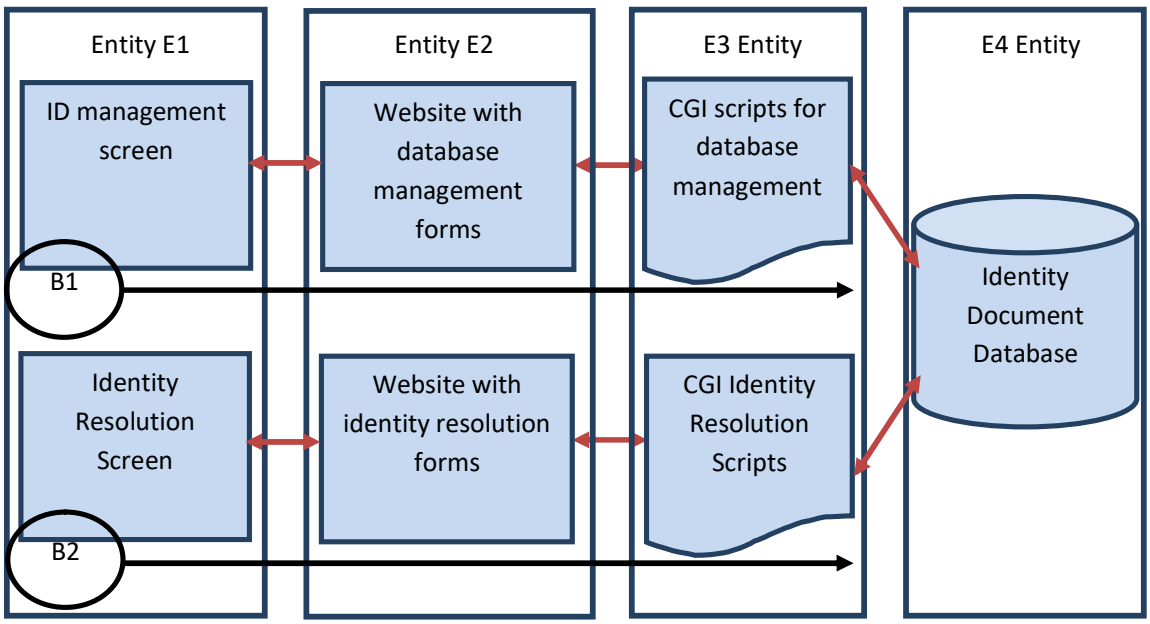

Figure 20: Internal architecture of the certification platform

The E1 and E2 entities are implemented using the markup languages, the E3 entity, with the query languages and E4 using a Database Management System (DBMS). The first branch of features B_1 is that of the operations offered by the DBMS creation, updating, modifying, deleting and managing access permissions by

means of user profiling. The second B2 branch is implemented using query languages for NGFS to perform identity resolution operations.

2MTVI model transformation

The initial 2MTVI model is adapted to the context of the calculation of the new break-even point by integration of our solution which adds a new burden to NGFS with the solicitation of the CSP (Certification Service Provider) paid services.

Example of illustration:

1. 1 transfer = identity resolution request
2. X_1: NGFS pricing for Y transferred amount
3. X_2: CSP pricing for Y transferred amount
4. X_3: pricing for the computerization of the state services for the issuance of identity documents for Y transferred amount
5. The monthly charges Ci (i=1..7) are maintained

The new gross monthly profit B_G generated by a counter is calculated as follows:

Mt_i = Amount transferred by a customer i

Nb_C = Number of customers in the reporting period

$B_G = (\sum (i=1..3)\ X_i) * (\sum (j=1..Nbc)\ Mt_j)/Y$

The break-even point for a BEPC in the one-month period is:

$BEPC = B_G - (\sum (i=1..7)\ C_i)$

Conclusion

In this paper, we have proposed the 2MTVI mathematical model for calculating the break-even point of the financial flow transfer activity. With the cybercriminal attacks presented, malicious intrusion into the system and identity theft of a recipient, we proposed architectural solutions internal to the NGFS 's global network which exploits QoS and service security technologies (VPN, IntServ, DiffServ, RSVP, MPLS). We have determined the contribution of biometrics with the implementation of an CSP to process identity resolution requests from all NGFS counters throughout the national territory. There is still an important part related to the evaluation of the performance of our architecture and the CSP platform as future work.

References

[1] INTERPOL, 2021 Evaluation Report, Cybercrime in Africa

[2] Daniele Bringhenti, Member, IEEE, Riccardo Sisto , Member, IEEE, and Fulvio Valenza , Member, IEEE, "Automating VPN Configuration in Computer Networks", IEEE Transactions on Dependable and Secure Computing, Vol. 22, No. 1, January/February 2025

[3] Azeddien M. Sllame, Maha Shaeban Ammarah, "VoIP Performance Comparison across MPLS-Based Networks with SIP, H.323 Signaling Protocols Enhancing the QoS through RSVP Protocol", The First Scientific Conference on Engineering Applications (ICEA'2024), Conference Proceedings, Vol. 04, No. 1, 2025, DOI: 10.51984/SUCP.V4I1.3851

[4] Ali Q. Mohammeda, Rana F. Ghanib, "Enhancing network Quality of Experience based on Artificial Neural Networks", Engineering and Technology Journal 43 (04) (2025) 234-243, Journal homepage: https://etj.uotechnology.edu.iq
[5] Dariusz Strze˛ciwilk, "Differentiated service quality analysis based on QoS traffic prioritisation", INTL Journal of Electronics and Telecommunications, 2025, Vol. 71, No. 1, PP. 285–292, doi:10.24425/ijet.2025.153572
[6] Sony Putra, Muhammad Iqbal, Andysah Putera Utama Siahaan, "Network Security Design Using Virtual Private Network (VPN) Method By Utilizing Point To Point Tunneling Protocol (PPTP) Technology On Local Area Network (LAN)", International Journal of Computer Sciences and Mathematics Engineering, 2024, E-ISSN 2962-4274, Journal homepage: www.ijecom.org
[7] Rezaeianfardouei, H., Townley, M. & Saedi, M., "Reducing Failover Latency in Cisco ASA Site-to-Site VPNs Through IPsec Parameter Tuning", Paper presented at the 2025 IEEE CyberSciTech/DASC/PICom/CBDCom Co-located Conferences, Oct 2025, Hokkaido, Japan
[8] Ranganathaswamy, M. K., Yadav, R. K., & Awasthi, A. (2024, June). "Symmetric Applied Cryptography for Secure Instant Messaging", In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE
[9] B. A. Tawayé, M. I. Tiado, S. Abdoulwahabou, M. Harouna, I. G. Noura, "Models of Quality of Service (QoS) in the GSM environment of the New Generation of Digital Open Universities (DOUNG)", International Journal of Wireless Networks and Communications, SSN 0975-6507 Volume 1 3, Number 1 (2021) pp. 1-13
[10] T. Szigeti, R. Barton, C. Hattingh Kenneth Briley, "End-to-End QoS Network Design", Cisco Press, ISBN-13: 978-1-58714-369-4, ISBN-10: 1-58714-369-0, November 2013
[11] Peter Gregory and Michel A. Simon, "biometrics for Dummies", Cisa, Cissp, 2008
[12] "Les technologies biométriques", https://www.biometrieonline.net/technologies/fonctionnement
[13] Abdelghani HARRAG, "Data Extraction from a base: Application to the extraction of locutor characteristics", Universty Ferhat ABBAS – Sétif, PhD Theses, 26/06/2011
[14] Véronique Messéant, Patrick Nizou, Nathalie Villain, "Modélisation Master Didactique des Mathématiques", Université Paris VII, June 2006, pp 6-23