New Smart Encryption Approach based on Multidimensional Analysis Tools

Salima TRICHNI[1], Fouzia OMARY[2], Mohammed BOUGRINE[3]
Faculty of Sciences Mohammed V University in Rabat Department of Computer Science
Rabat, Morocco

***Abstract*—In the last decade, with the new situation forced by the Covide-19 pandemic, the information systems are often forced to work remotely, they must communicate and share confidential data with several interlocutors. In such a context, ensuring the confidentiality of communications becomes a complex and difficult task. Hence, the need to have a flexible system that can adapt with different parameters involved in every exchange of information. We recently presented in [1] a new smart approach to data encryption that serves the same purpose. This approach uses the concept of artificial intelligence and apply BNL skyline algorithm to decide about the most suitable algorithm to ensure the best data privacy. However, with the evolution of dimensions and criteria to be considered for this smart encryption, we find that the complexity of the BNL algorithm increase, then, the response time of the application increase and the skyline encryption quality decreases. In this work, we propose a new idea to resolve this problematic. Indeed, this contribution consists in adding another Intelligence brick to dynamically define the Skyline algorithm depending on the type and number of dimensions. Through this paper, we provide an analysis and a comparison of some skyline algorithms for the multidimensional search. The results obtained by this study show the performance of this new approach whether in terms of execution time or in the quality of the dominant encryption solution.**

Keywords—Security; confidentiality; artificial intelligent; smart encryption; cryptography; skyline

I. Introduction

With the enormous development of the communication´s means and the current circumstances caused by the covid-19 pandemic, a new management culture was brutally imposed on almost all institutions, companies and especially manufacturers who have suffered very impacting economic shock. Indeed, this new culture enforced by the health threat, is essentially based on collaboration and remote work to minimize the people´s movements and frequentation. We find ourselves with several new approaches in several areas, namely: e-administration, telemedicine, E-Learning and finally e-commerce which continues its development in the field of online shopping.

On the other hand, this situation forces us to go through telecommunications and technologies in order to share secrets, very confidential and critical data in a private network but most of the time public and not mastered. The attackers (the malicious ones) are more and more active and in constant search of vulnerabilities. Indeed, the percentage of vulnerabilities is increasing every day.

Computer security has therefore become a challenge for any company in order to ensure the continuity of its services. Research in this field has taken a new direction and aims to exploit new technologies in order to support immense digital development. New concepts have emerged, such as the concept of Identity-Based Cryptography (IBS) in which several publications are occurring as in [2] which aims to integrate authentication and integrity in the DNS and eliminates key escrow problem. At the same time, another security approach is also experiencing enormous development. This is the Blockchain. This revolutionary technology using cryptography and ensuring the security of transactions in full transparency is becoming a trend, and several researchers are thinking about how it can be applied in different needs. In [3], for example, the authors are coming up with Industrial IoT (IIoT) and Blockchain for the smart industries. The last component of development in the field of computer security is that which aims to integrate artificial intelligence into cryptographic processes. It is within this context that our research is oriented. In [1], we presented a new approach of intelligent security, adjustable with each information exchange and thus allowing communication with multiple entities regardless of their security protocol. In this system we consider the encryption algorithms as skyline points and we are used the BNL algorithm to choose the best one that best meets our security constraints. BNL works well if the size of the resulting Skyline line is small, and ideally fits into the window that causes the algorithm to terminate in a single iteration. However, this algorithm may require a large number of passes until 'that the complete Skyline is calculated and eventually terminates. So its performance is very sensitive to the number of dimensions and the distribution of the underlying data. Hence the need for a new method to stabilize the performance of this approach regardless of changes in the number of dimensions and their distributions.

The idea of this work consists in proposing a new solution concerning this approach that defines the Skyline algorithm according to the requirement of each communication. So instead of the skyline search algorithm being fixed, we modify it according to the type and the number of dimensions to be considered in each communication.

To present our work we will proceed as follows: First, we will start by citing the work related to our field of research and which integrates artificial intelligence techniques into computer security. Then, we will describe the principle behind the Intelligent Approach of Encryption. In a third section, we will present this new contribution and an experiment study of all basic Skyline algorithm to show their performance according to the parameters of each execution. Finally, in the last section we will discuss about the results and give conclusions.

II. Related Work

Artificial intelligence is a revolutionary technology that has been able to implement applications aimed at mimicking a form of real intelligence in several areas. Particularly in the area of security, several works have been carried out to strengthen and improve the security of information systems.

In general, there are two types of artificial intelligence use in the field of security. The first consists in creating decision support systems in order to control and improve the security policy of companies.

In cybersecurity, different solutions have been designed to overcome vulnerabilities and anomalies in systems. For example, in cyber-attacks, the thesis [4] offers an intrusion detection system in a completely unsupervised environment. This system is based on the Mutual Information algorithm for the selection of features and on the Deep Learning PV-DM model for reading network packets.

In this same area, other solutions are already starting to take their places in the market, such as the AI2 platform which, from the log lines, identifies suspicious activities. AI2 applies unsupervised machine learning algorithms on the input data to nominate potential attacks. Then, IT security analysts intervene to confirm and decide which incidents are real attacks. This system is also capable of continuously generating new models within hours, which can dramatically improve the speed of its cyber-attack detection capability [5].

The article [5] gives a summary and a detailed state of the art on other AI systems used in the field of security whether at the level of infrastructure, network, cloud, terminals, mobile, applications, IoT, or others such as the Web and Identity Management.

All the solutions mentioned above, come to help and facilitate the prediction and / or the detection of the problems and the faults of the systems. On the other hand, there is another category of AI solutions in the field of computer security.

This second category consists of designing systems that provide one or more properties of computer security based on AI techniques.

To ensure confidentiality, for example, in [6] the Google team proposed a solution based on the training of learning machines for the encryption and decryption of messages. Indeed, the authors consider the protagonists Alice and Bob as neural networks that try to communicate with each other in complete confidentiality while preventing a third malicious neural network named Eve from decrypting their messages. This system resembles the principles of electronic games.

The author in [7] represents another way to design an encryption system based on one of the paradigms of artificial intelligence which are on evolutionary algorithms. The Symmetrical Evolutionary algorithm (SEC) is the first variant of this type of algorithm which performs an encoding of the text in the form of positions lists. Then, it applies a set of genetic operators (mutation and crossover) on these positions at the level of each iteration in order to reproduce potential solutions. Finally, and through a well-defined evaluation function, assesses individuals and decides the safest solution. Several extensions of this system have been developed in order to increase the level of intelligence of this system in choosing the most relevant solution. Sometimes by adding difficult problems in the encryption process like the case of [8], and in other cases by modifying the evaluation function like in [9] and [10].

Our approach falls rather in the first category and it consists of a Decision Support System for the encryption of confidential data.

III. Background

A. Skyline Algorithm

1) The concept of dominance: Given a dominance relationship in a dataset, a Skyline query returns objects that cannot be dominated by any other object.

In the case of a dataset made up of multidimensional objects, one object dominates another object if it is equally good in all dimensions, and better in at least one dimension.

Skyline's computation was an algorithmic problem in nature, and all data was assumed to reside in memory.

However, nowadays we are faced with large data sets which are stored in secondary memory. Having the data on the disk, the algorithms proposed for processing Skyline requests are separated into two categories: algorithms not based on indexes and algorithms based on indexes.

2) Algorithms not based on indexes

a) Block Nested Loop (BNL)

A naive algorithm for calculating a Skyline query is to compare each object with all of the other objects in the dataset using a nested loop. However, the quadratic complexity O (n2) makes this algorithm very inefficient (n is the total number of objects in the data set).

The Block-Nested-Loop algorithm [11] applies the same idea, but uses a window (block of memory with limited space), which contains a limited number of data objects. Any candidate object p is compared to the objects of the window.

Three cases can occur:

1) p is dominated by an object in the window! p is eliminated.

2) p dominates one or more objects in the window! These objects are eliminated and p is placed in the window.

3) There are no objects in the window! p is inserted directly into the window. (In case the window is full, a temporary disk file is used to contain the candidate objects).

BNL may require a large number of passes until the full Skyline is calculated and eventually terminate because at the end of each pass the size of the temporary file will be reduced.

b) Divide & Conquer (D&C)

The D&C algorithm [12] [13] calculates the median value of a dimension, and divides the space into two partitions P1, P2.

Then it calculates the Skylines S1, S2 of P1, P2, recursively dividing P1 and P2.

Recursive partitioning stops when there are only one (or a few) objects. The overall Skyline is calculated by merging S1 and S2, and eliminating objects in S2 that are dominated by any object in S1.

c) Bitmap

The Bitmap algorithm as it was proposed in [14] is based on a vector representation of all the dataset.

In order to describe the algorithm, let p be a point in a d-dimensional space represented by a vector of m bits.

$p = \{p.d_1, ..., p._{dj}\}, 1\leq j \leq d$

From these m bits, each p.di is represented by a number ki of bit slice. Each ki has as many bits as the number of distinct coordinate values of all points in the dataset in that dimension.

After constructing the bit slices, the algorithm performs 3 operations between 2 sets of bit parts. The first set contains the parts of bits Vx, Vy (one for each dimension) where resides the last bit of the point which is equal to 1. The second set contains the slices of bits Vx + 1, Vy + 1. In the case where the bit slices of the previous step are the last in order, we then use the bit slice zero (all bits at zero).

- The first operation A will be an AND operation between Vx and Vy.
- The second operation B will be an OR operation between Vx+1 and Vy+1.
- The third operation C will also be an AND operation between the results.

If the result of the final operation is zero, the tested point is a Skyline point.

3) Algorithms based on Index

a) Index

The index is a B-tree-based algorithm for two-dimensional data, where the data has two ordered indices.

For example, let a tree B and a tree B +, each represent a dimension. The algorithm calculates one over the entire Skyline line by scanning both indices simultaneously and stops as soon as a 'p' object is found in both indices.

Any object that has not been inspected in both indices is certainly not part of the Skyline line, as it is dominated by p. Therefore, candidate objects are those that have already been inspected in at least one index. These objects are kept in a separate set S (the superset of the Skyline line).

b) Nearest Neighbor Search (NN)

The first Skyline algorithm based on a spatial index (as R-tree), is the Skyline NN algorithm, proposed in [15]. It is called NN because of its relevance to the nearest neighbor search. It identifies Skyline objects by repeated NN search, using an appropriate distance measure.

The algorithm iteratively finds the closest object (NN) to the origin in a given region of space based on any monotonic distance function, e.g. the Euclidean distance. During the algorithmic process, entire regions dominated by a candidate object are ignored, and regions that cannot be ignored are added to a task list for further partitioning of space. And so on until the list becomes empty and, thus, the algorithm ends.

B. Description of Intelligent Approach of Encryption

The solution proposed in [1] is a decision-making system aimed to ensure the confidentiality of data in the most adequate way.

The following diagram shows the different steps in the framework of this strategy.

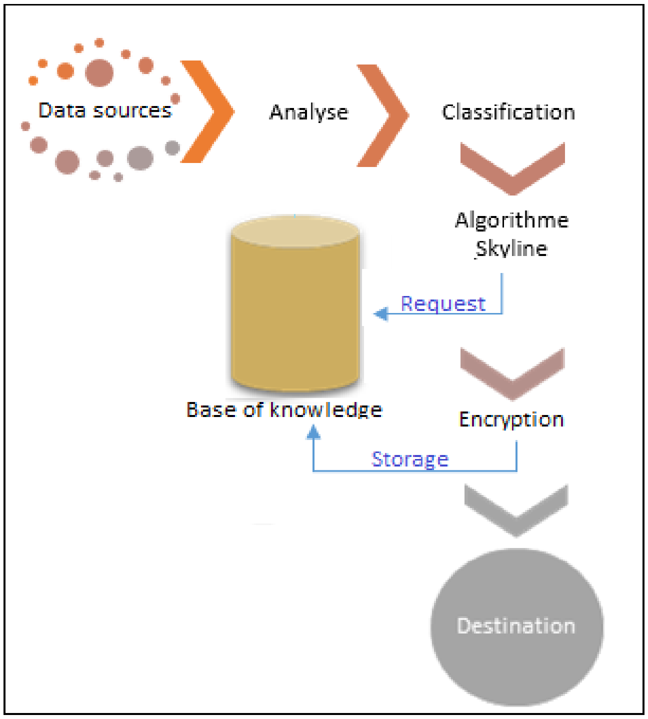


Fig. 1. Steps of the Intelligent Encryption Principle.

To explain the diagram of Fig. 1; we will detail each step in the following:

a) Step1: Analysis

Before proceeding with data encryption, in this solution we propose to rely on several characteristics of the encryption environment to decide the ciphering algorithm that best meets the security criteria to ensure in this communication.

This new encryption method begins with an analysis of the various elements that impact communication security. Indeed, we must analyze this impact at the level of:

- The source environment,
- The transmission channel,
- The destination environment

- The types of data to be transmitted,
- The generation of the keys, if not the possession of the keys.

Each part of this system represents a set of characteristics which considerably influence the security of this communication. Therefore, you have to focus on each part to extract the most relevant information.

b) Step2-Classification

Once this analysis has been carried out, we must move on to the second step which consists of classifying the data and storing all this information in an intelligent business architecture in order to subsequently decide on the most appropriate encryption.

The decisional database is a multidimensional base and knowledge base that includes a large number of experiments to cover the various cases possible.

c) Step3 - Skyline

In the third step, we launch the BNL skyline request on the previously established knowledge base by using the current communication requirement.

d) Step4 – Encryption and Storage

Depending on the chosen encryption algorithm we apply this encryption to our message and send the encrypted information.

Finally, the last step is a consolidation step in which we calculate the robustness of this encryption in terms of possible security indicators. Then, we feed the knowledge base by the feedback that we were able to complete.

IV. Contribution

A. *Problematic Description*

As noted in the previous section, the intelligent encryption approach uses the BNL algorithm to select the most dominant encryption algorithm against the specified criteria. This algorithm is very efficient in the case where one is satisfied with a very restricted set of dimensions with a dataset containing less candidates.

However, with the evolution of the knowledge base and the requirements to be taken into account for the security of communications, the complexity of this algorithm increases considerably and becomes quadratic of the order O (n ^ 2), where n is the size of the dataset to be examined; something that induces degradation of system performance.

In order to remedy this problem, we have carried out an in-depth study on certain Skyline algorithms, however we have come to the conclusion that each algorithm can be efficient and performant under certain conditions.

In what follows, we present this observation in detail and we propose a solution to circumvent this problem and grant a better flexibility of this approach.

B. *Description of Proposed Solution*

This contribution focuses more on step 3 of the Intelligent Encryption Principle. It seeks to optimize the use of Skyline algorithms for better results.

The solution is to add an extra step in this approach to dynamically choose the most suitable Skyline algorithm with respect to the data tuples to be examined.

Then the new process can be described as follow:

Step 1: Analysis of the data source/environment/channel

Step 2: Modeling and data classification in a BI database

Step 3: Building Criteria to Consider in the Skyline Query

Step 4: Skyline Algorithm Setting

Step 5: Application of the Skyline method

Step 6: Recovery of the most relevant encryption Skyline

Step 7: Evaluate the Solution and Enrich the Knowledge Base.

Below we prensent a summary diagram (Fig. 2) to illustrate how this new approach works to ensure the exchange of sensitive data between two entities (Alice and Bob) on different networks :

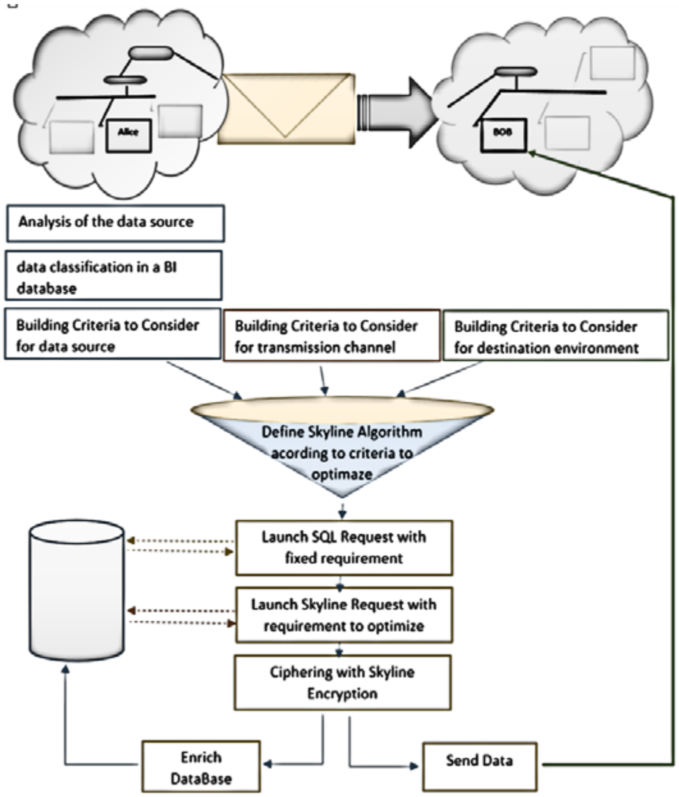

Alice
BOB
Analysis of the data source
data classification in a BI database
Building Criteria to Consider for data source
Building Criteria to Consider for transmission channel
Building Criteria to Consider for destination environment
Define Skyline Algorithm acording to criteria to optimaze
Launch SQL Request with fixed requirement
Launch Skyline Request with requirement to optimize
Ciphering with Skyline Encryption
Enrich DataBase
Send Data

Fig. 2. Diagram Summarizes the Steps of Our Contribution.

Now and after having stated the original contribution of this work which lies in adding an intelligent step allowing the configuration of the Skyline algorithm most appropriate to the criteria of our research. We chain in the following by an experimental study to analyze the impact of each criterion / dimension on the performance of the skyline algorithm in order to determine the set of parameters to be considered in the choice of Skyline.

For this, we will consider the following Skyline algorithms:

- Block Nested Loop (BNL)
- Divide & Conquer (D&C)
- Bitmap
- Index
- NN

C. *Experiences &Results*

To perform these experiments, we prepared a knowledge base with real data. Feeding this database has been made on the basis of an input data sample selected in an arbitrary manner which 100 texts same fixed characteristics.

Then, we applied to each text these five encryption algorithms: AES, Blowfish, DES, TripleDES [16] and ASEC which makes a total of more than a thousand test lines.

1) Specification of requirements: In an approach to optimization of processing, our method runs on two requests to attack the knowledge base as in [23].

The first query serves to minimize the volume of data to be examined in the next step. It uses fixed criteria in the SQL clause “Where” whose values are fixed at the start of each exchange.

The fixed criteria represent the properties of the current communication, for example:

- Type of data to be exchanged
- Characteristics of the source network
- Characteristics of the destination network
- The licenses available.
- The machine capacity of the encryption
- The machine capacity of the decryption
- Robustness of the transport channel between the two networks

The second query executes the skyline algorithm and considers the criteria to be optimized and from which the users' wishes in terms of the level of security to be acquired are made concrete. Hence the distinction between the two types of criteria.

For example: The criteria to be optimized:

- Quality (rate of randomness / entropy)
- The reputation of the algorithm
- encryption utilization frequency
- The cost of encryption / decryption
- The speed of encryption / decryption
- etc.

The test environment is based on an Intel (R) Core (TM) i7-6700HQ, 2.60GHz, 16GB RAM, 64bit OS machine.

2) Application of skyline algorithms: The application of Skyline algorithms was carried out by the Java programming language via the Spring Boot framework for the development of the Back End and Angular for the Front End part.

Through this application, users have the right to:

- Specify the number of dimensions.
- Specify the dimensions.
- Choose the operation to apply on each dimension.
- Choose the preferred algorithm for calculating Skyline points.

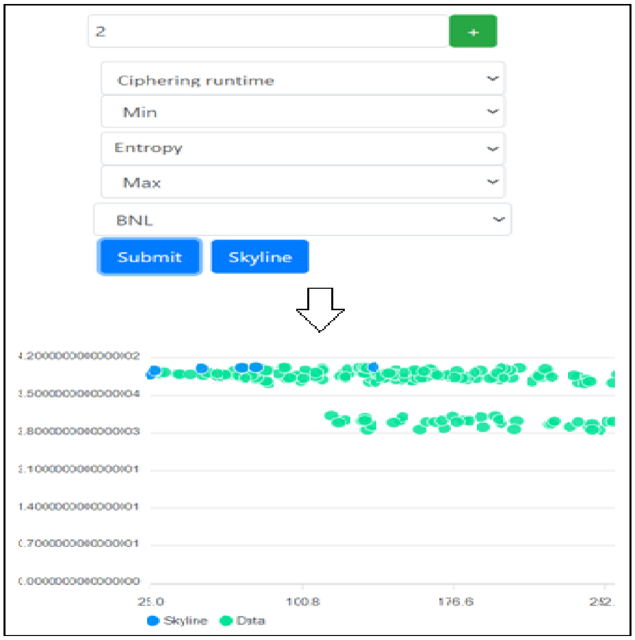
The application attacks the knowledge base and executes the chosen Skyline algorithm with the criteria entered as shown in Fig. 3, 4, 5, 6 and 7.

a) Scenario 1: On Two Dimensions

The objective of this experiment is to:

- Minimize encryption time
- Maximize entropy

Fig. 3 until Fig. 7 show the executions carried out for each Skyline algorithm and the output result.



2

Ciphering runtime

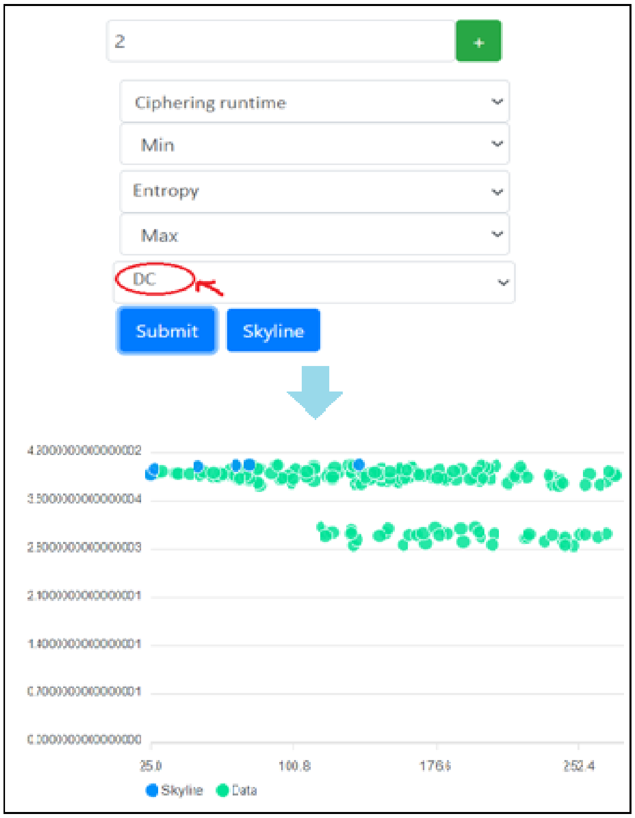
Min

Entropy

Max

BNL

Fig. 3. Application of BNL Skyline Algorithm with Two Dimensions.



2

Ciphering runtime

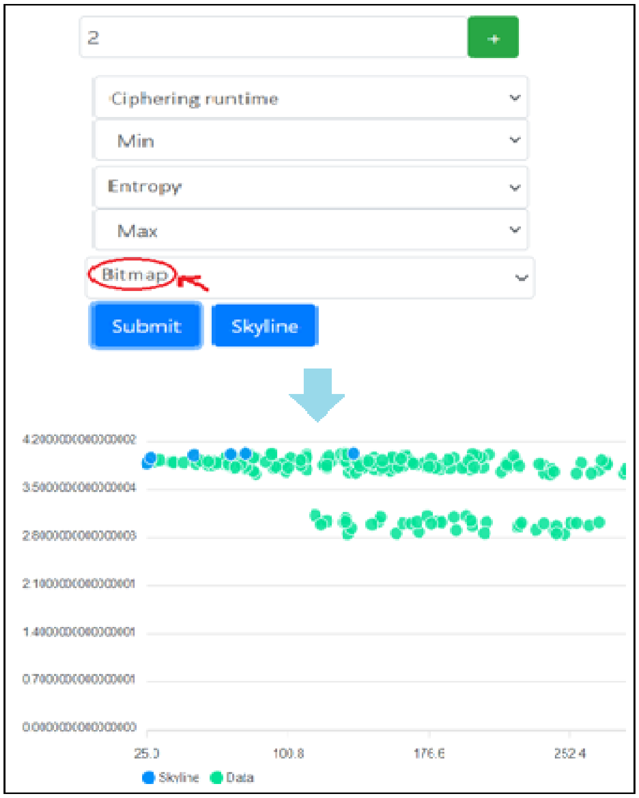
Min

Entropy

Max

DC

Fig. 4. Application of DC Skyline Algorithm to Optimize Entropy and Runtime Dimensions.



2

Ciphering runtime

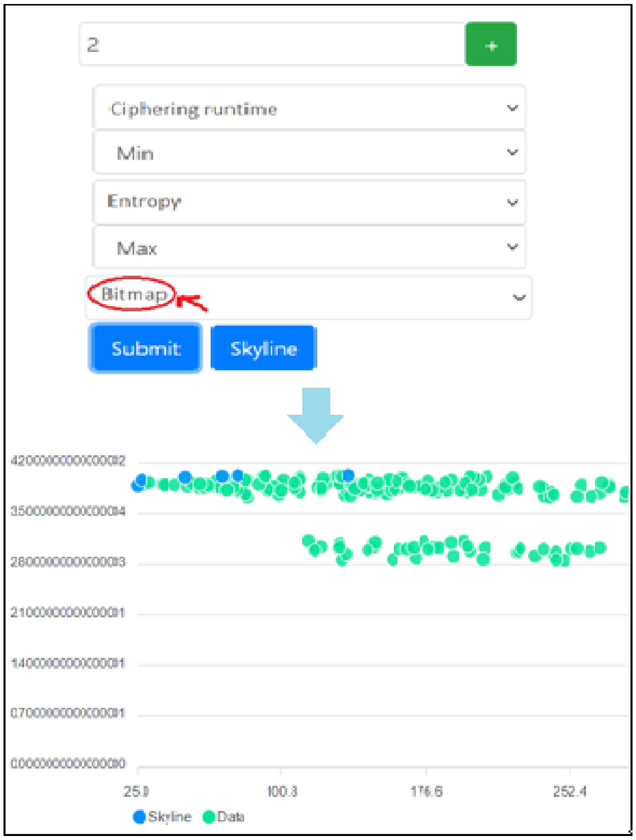
Min

Entropy

Max

Bitmap

Fig. 5. Application of Bitmap Skyline Algorithm to Optimize Entropy and Runtime Dimensions.



2

Ciphering runtime

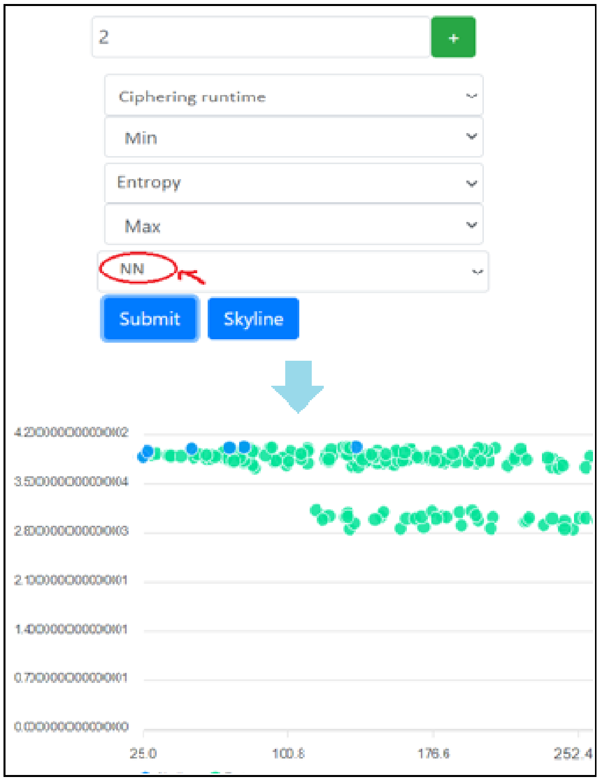
Min

Entropy

Max

Bitmap

Fig. 6. Application of Index Skyline Algorithm to Optimize Entropy and Runtime Dimensions.



2

Ciphering runtime

Min

Entropy

Max

NN

Fig. 7. Application of NN Skyline Algorithm to Optimize Entropy and Runtime Dimensions.

TABLE I. SKYLINE POINT FOR ENCRYPTION ALGORITHM THAT OPTIMIZE ENTROPY AND RUNTIME DIMENSIONS

Algorithm	**Ciphering Runtime(ms)**	**Entropy**
BLOWFISH	25	3.8870066417181426
BLOWFISH	27	3.9658710817437597
BLOWFISH	48	4.00235367813974
BLOWFISH	66	4.01642913400371
AES	73	4.026504332171881
BLOWFISH	126	4.027404704120802

- Results & Discussion of Scenario 1:

The results of the different algorithms were all the same and give out 6 skyline points as the dominant solutions. The following Table I summarizes this result:

The most efficient encryption algorithm is BLOWFISH comes after the AES algorithm in second. Indeed, in this case these two algorithms are well known in the community of computer security by their performance and their level of security [17] [18] [19] [22].

Now, if we go back to the performance of the Skyline algorithms, to come up with these results there is a huge difference in the execution time of these algorithms.

The diagram below shows the result of the execution time of each Skyline algorithm.

So from the Fig. 8, we can conclude that the BNL algorithm is the simplest and the best if we do not use the two dimensions encryption time / Entropy.

However, if we change the two dimensions considered in the first experiment and we opt for the following scenario:

b) Scenario 2: on Two Dimensions

- Objective 1: to minimize the decryption time.
- Objective 2: minimize the memory capacity required for decryption.

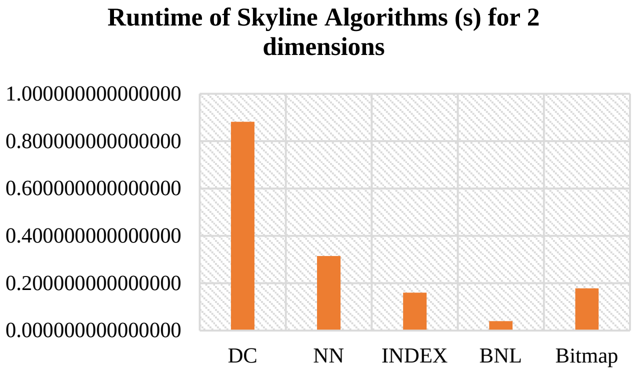


Fig. 8. Comparison of Runtime Skyline Algorithms (s) Executed with Entropy and Runtime Dimensions.

TABLE II. SKYLINE POINT FOR ENCRYPTION ALGORITHM THAT OPTIMIZE DECIPHERING RUNTIME AND USED MEMORY

Algorithm	**Deciphering Runtime(ms)**	**Deciphering Memory used (K)**
SEC	48	1695
SEC	56	1841
ASEC	93	2503
AES	243	2517

The application of the Skyline algorithms was carried out in the same way as the first experiment except for the types of dimensions which have just been modified to select the Decryption Runtime and the Memory dimensions.

In this experiment, the results in terms of Skyline points are different,

The Table II below is the summary of the results of the different executions:

- Results & Discussion of Scenario 2:

The SEC encryption algorithm is ranked first, followed by the ASEC (advanced version of SEC) algorithm, followed by the AES algorithm.

The result given by this system seems logical because SEC is an evolutionary algorithm [20] which takes enough time to perform the encryption and generate the key, however, in the decryption process it applies a single operation to the whole text at once. As a result, this type of algorithm performs best with respect to the cost of decryption.

On to the result of the skyline algorithm runtime, the following diagram illustrates the results of this scenario:

From this experience, we can see in Fig. 9 that the Bitmap algorithm performed well in this scenario.

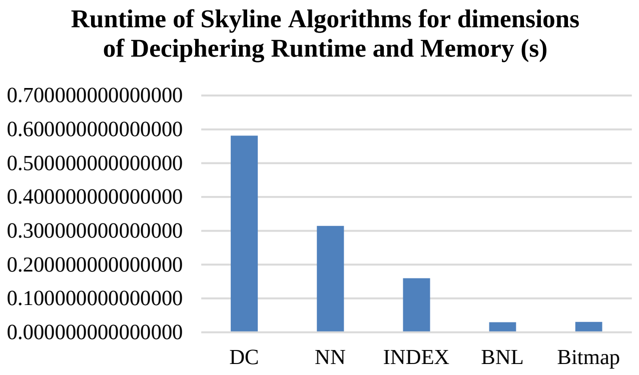


Fig. 9. Comparison of Runtime Skyline Algorithms for Dimensions of Deciphering Runtime and Memory (s).

This is because the Bitmap vector representation for these two dimensions is less complex. In fact, the more the number of values of a dimension are mastered, the algorithm becomes faster and more efficient [21]. In Scenario 1, the entropy dimension had very varied values and therefore the Bitmap vector representation will be very large and complex.

On the other hand, the BNL algorithm always remains efficient even by modifying the type of dimensions considered [21].

c) Scenario 3: for Four Dimensions

- Objective 1: minimize encryption time.
- Objective 2: maximize entropy
- Objective 3: minimize decryption time
- Objective 4: minimize the memory capacity required for encryption.

The diagram below shows the result of the execution time of the skyline algorithms.

- Results & Discussion of Scenario 3

From the results of Fig. 10, we see that the Bitmap algorithm becomes very complex however, the index algorithms become more efficient.

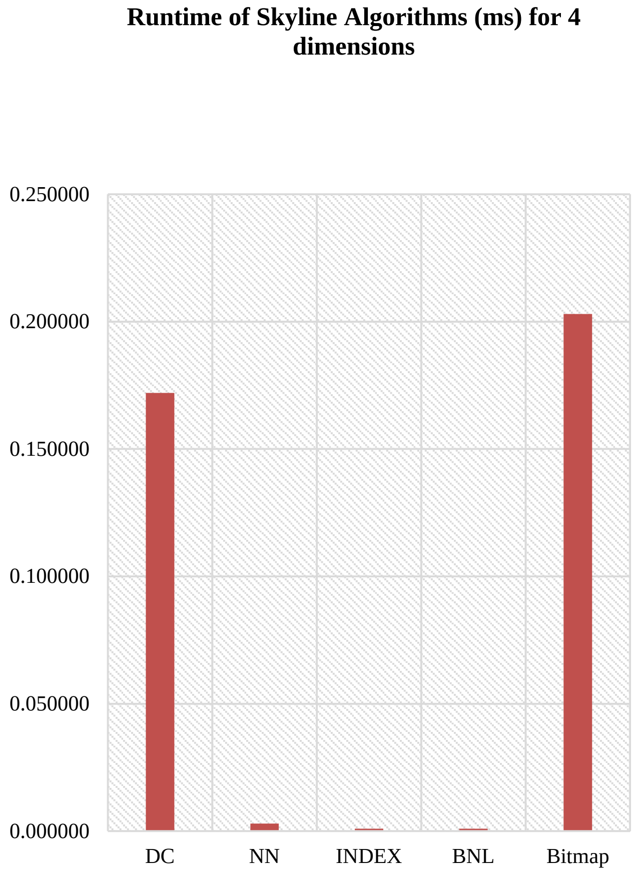


Fig. 10. Comparison of Runtime Skyline Algorithms (s) Executed with 4 Dimensions.

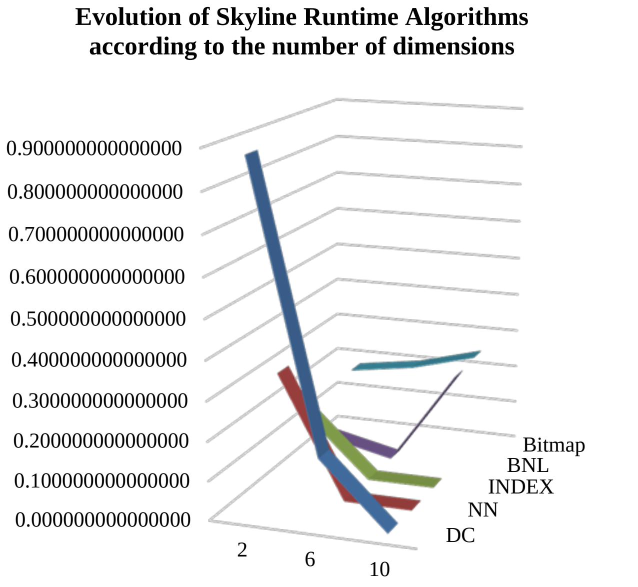


Fig. 11. Compariosn of Evolution of Skyline Runtime Algorithms according to the Number of Dimensions.

And so on, the more we add dimensions, the more the performance of the algorithms changes.

d) Scenario 4: up to 10 Dimensions

In this experiment, we ran the application on several dimensions to assess the impact of the number of dimensions on the speed of Skyline algorithms.

The Fig. 11 below shows the result of the execution time of the skyline algorithms against number of dimensions.

3) Comparison and discussion: As we have presented in previous experiences, we focused on two very important factors for the success of this approach, namely:

- The execution time of Skyline algorithms because it has a very significant impact on the speed of the entire system.
- The quality of the Skyline selected (the encryption to be implemented) because it represents the heart of this approach and embodies the robustness and security of the system.

The quality of the skyline solution can be evaluated based on the following characteristics:

- Guarantee: All returned points are skylines.
- Accuracy: All the points returned meet the criteria previously defined.
- Progressiveness: the sending of results is done instantly regardless of the size of the database are often huge.
- Completeness: at the end, all the points of the skylines are returned.

From this experiment study, we can conclude that there are two main parameters to satisfy all these characteristics and guarantee the performance of the skyline algorithms on encryption problem. These two parameters are:

- The Number of Dimensions
- The rate of variation which means the rate of the difference between numerical values of a given dimension. The greater this difference, the lower the rate of change and vice versa.

For example, to demonstrate the impact of the rate of change on the quality and performance of this approach, we can go back to experiments 1 and 2. In fact, in the first scenario we used two dimensions with different rates of change (the encryption with a normal rate of change and entropy for which the rate of change is very high). While in the second experiment we kept the same number of dimensions but with a normal rate of variation for both. The result of the first experiment favored the BNL algorithm however in the second experiment the Bitmap algorithm performed better. Otherwise, compared to the quality of the returned Skylines, they were all on the same level. In terms of:

Accuracy: criteria met

Guarantee: exact encryption

Completeness: same list of Skylines,

Progressivity: the list was returned all at once however this test is not interesting in this case since the number of dimensions is very low and the size of the base is fixed for the moment.

The two tables, Tables III and IV below summarize these results:

TABLE III. THE CRITERIA FOR CHOOSING THE SKYLINE ALGORITHM IN THE CASE OF 2 DIMENSIONS AND AN UNCORRELATED RATE OF VARIATION

Scenario 1	d=2			
	uncorrelated rate of variation			
	Progressiveness	Guarantee	Completeness	Speed
BNL	oui	oui	oui	1
D&C	oui	oui	non	5
Bitmap	oui	oui	non	3
Index	oui	oui	oui	2
NN	oui	oui	oui	4

TABLE IV. THE CRITERIA FOR CHOOSING THE SKYLINE ALGORITHM IN THE CASE OF 2 DIMENSIONS AND A UNIFORM RATE OF VARIATION

Scenario 2	d = 2			
	uniform rate of variation			
	Progressiveness	Guarantee	Completeness	Speed
BNL	oui	oui	oui	2
D&C	oui	oui	oui	5
Bitmap	oui	oui	oui	1
Index	oui	oui	oui	3
NN	oui	oui	oui	4

The objective behind the other two experiments is to demonstrate the impact of the dimension number on the quality and speed of the system. In fact, in these two experiments, we each time added additional dimensions to our research with different rates of variation.

From the results of these experiments, we find that the NN and D&C algorithms are starting to meet the demanded needs better than other algorithms. The Bitmap algorithm always responds very well in cases of dimensions with uniform rate of change regardless of the number of dimensions. However, the BNL algorithm is no longer favored if the number of dimensions is large.

At the end and to summarize all these results, we can use the Tables V and VI below to decide on the choice of the Skyline algorithm which gives us the most secure encryption:

TABLE V. GLOBAL CRITERIA FOR CHOOSING THE SKYLINE ALGORITHM IN THE CASE OF LESS THAN 4 DIMENSIONS

	d < 4			
	uniform rate of variation			
	Progressiveness	Guarantee	Completeness	Speed
BNL	-	oui	oui	oui
D&C	-	oui	oui	non
Bitmap	-	oui	oui	oui
NN	-	oui	oui	non
	uncorrelated rate of variation			
	Progressiveness	Guarantee	Completeness	Speed
BNL	-	oui	oui	oui
D&C	-	oui	non	non
Bitmap	-	oui	non	non
NN	-	oui	oui	non

TABLE VI. GLOBAL CRITERIA FOR CHOOSING THE SKYLINE ALGORITHM IN THE CASE OF MORE THAN 4 DIMENSIONS

	d >= 4			
	uniform rate of variation			
	Progressiveness	Guarantee	Completeness	Speed
BNL	non	oui	oui	non
D&C	non	oui	oui	non
Bitmap	oui	oui	oui	oui
NN	oui	oui	oui	oui
	uncorrelated rate of variation			
	Progressiveness	Guarantee	Completeness	Speed
BNL	non	oui	non	non
D&C	non	oui	oui	oui
Bitmap	non	oui	non	non
NN	oui	oui	non	oui

Then, if we come back to our new approach (Fig. 2), for the step 4 of this new contribution that consist in ‘Skyline Algorithm Setting’ we can conclude that we have tree general configuration of Skyline algorithms:

Configuration 1: when performance achieved on a small number of dimensions such as BNL.

Configuration 2: performance achieved if we work on a large number of dimensions such as the DC and NN algorithms

Configuration 3: performance achieved if we work on dimensions with a limited number of different values, then we can use Bitmap algorithm.

V. Conclusion

Despite the significant development of security tools, computer systems still suffer from malicious threats especially with the huge growth of emerging technologies.

To be able to support this revolution, these new technologies must be integrated into the various security components. During this work, we tried to develop a new approach to intelligent encryption that is based on the concepts of artificial intelligence. It uses Skyline algorithms to define the policy to be followed to ensure the confidentiality of exchanges. In this work we proposed a new version of this system included an additional step to define dynamically the Skyline algorithm to be executed for choice the good Encryption Algorithm. So, from the experimental demonstration we deduced that the choice of the Skyline algorithm has a perimeter role in this approach and the use of the BNL algorithm, as in the previous contribution, risks weakening the performance and the efficiency of this encryption system, especially if the variation rate of dimension values or their number increases We applied different Skyline algorithms and we compared the results. Finally, and after several scenarios we concluded that this system must absolutely change the choice of Skyline Algorithm taking into account two main parameters which are: The number of dimensions and the rate of variation.

References

[1] S.Trichni; F.Omary; A.Idrissi; M.Bougrine; M.Abourezq : New intelligent strategy for encryption decisional support system - International Journal of High Performance Systems Architecture (IJHPSA), Vol. 9, No. 4, 2020

[2] M. Patel, R. Patel : Improved Identity Based Encryption System (IIBES): A Mechanism for Eliminating the Key-Escrow Problem - Emerging Science Journal, Vol 5, No 1 (2021), DOI 10.28991/esj-2021-01259

[3] A. Iqbal, M. Amir, V Kumar, A. Alam, M Umair : Integration of Next Generation IIoT with Blockchain for the Development of Smart Industries, Vol 4 (2020) , DOI: 10.28991/esj-2020-SP1-01

[4] Samira Douzi : Vers un Deep Learning Système de Detection des Intrusions - Doctoral thesis dissertation- Jully 2019

[5] Vähäkainu, Petri & Lehto, Martti. (2019). Artificial intelligence in the cyber security environment Artificial intelligence in the cyber security environment. https://www.researchgate.net/publication/338223306_Artificial_intelligence_in_the_cyber_security_environment_Artificial_intelligence_in_the_cyber_security_environment

[6] Mart´ın Abadi and David G. Andersen Google Brain “LEARNING TO PROTECT COMMUNICATIONS WITH ADVERSARIAL NEURAL CRYPTOGRAPHY” arXiv:1610.06918v1 [cs.CR] 21 Oct 2016

[7] F.Omary : Application Of Evolutionary Algorithms To Cryptography (Applications Des Algorithmes Evolutionnistes À La Cryptographie).Doctoral Thesis, University Mohammed V Agdal , Faculty Of Science - Rabat Marocco. (July 2006).

[8] S.TRICHNI and al: A New Approach Of Mutation Operator Applied To The Ciphering System Sec. Iccit 2011,vol 63, no. 9;sep 2013.

[9] M.Bougrine, F.Omary , S.Trichni, : A new Evolutionary Tools for New Ciphering System SEC Version, 46ième International Carnaham Conférence On Security Technology (IEEE ICCST 2012),Boston Massachusetts, USA ISBN 978-1-4673-4807-2, ISSN :1071 ; p140-146.

[10] M.Bougrine, S.Trichni, F.Omary : Improving Performance of the Symmetrical Evolutionary Ciphering System SEC - International Journal of High Performance Systems Architecture (IJHPSA), (2021) (publication in progress)

[11] S.Borzonyi, D.Kossmann, K. Stocker : “The Skyline operator”, ICDE, pp.421-430, 2001.

[12] H.T. Kung, F. Luccio, F.P. Preparata : “On finding the maxima of a set of vectors”, JACM, Vol.22, No.4, pp.469-476, 1975.

[13] F.P. Preparata, M.I. Shamos : “Computational geometry : an introduction”,Springer-Verlag, New York, Berlin, 1985.

[14] K. Tan, P. Eng, B. Ooi : “Efficient progressive Skyline computation”, VLDB, pp.301-310, 2001.

[15] D. Kossmann, F. Ramsak, S. Rost : “Shooting stars in the sky : an online algorithm for Skyline queries”, VLDB, pp.275-286, 2002.

[16] W. DIFFIE, M. E. HELLMAN, “New Directions in Cryptography “ IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976 Pp 644 –654

[17] Zimmermann, P. R. (1991) PGP User’s Guide, 5th June 1991, Version 1.0, Phil’s Pretty Good Software.

[18] Florin G. Et Natkin S: Techniques Of Cryptography. Cnam 2002.

[19] Menezes A.J., Oorschot P.C. Van Et Vanstone S.A.: Handbook Of Applied Cryptography.(Crc Press, 1997).

[20] Shaul Drukmann: Evolutionary Algorithms.Encyclopedia Of Computational Neuroscience 2014, Pp 1-7.

[21] K.Tan, P.Eng, B. Ooi : Efficient Progressive Skyline Computation. VLDB, 2001.

[22] AK.Diaasalama and M. Hadhoud : Studying the Effect of Most Common Encryption Algorithms,” International Arab Journal of e-technology,Vol.2. No.1

[23] M. Abourezq and A. Idrissi : Introduction of an outranking method in the cloud computing research and selection system based on the skyline. In Research Challenges in Information Science (RCIS), 2014 IEEE Eighth International Conference on, pages1–12. IEEE. .(2014b).