NSS
Neutrosophic Sets and Systems, Vol. 72, 2024
University of New Mexico

An Efficient SuperHyperSoft Framework for Evaluating LLMs-based Secure Blockchain Platforms

Mona Mohamed [1], Alaa Elmor [2] and Florentin Smarandache[3], Ahmed A. Metwaly[4]
[1]Higher Technological Institute, 10th of Ramadan City 44629, Egypt
Email: Mona.fouad@hti.edu.eg;
[2,4]Zagazig University, 44519 Zagazig, Egypt
Email: alaaelmor@zu.edu.eg; a.metwaly23@fci.zu.edu.eg
[3]University of New Mexico, 705 Gurley Ave., Gallup, NM 87301, USA
Email: smarand@unm.edu.

* Correspondence: Mona.fouad@hti.edu.eg;

Abstract: In the age of modern technology, the use of the internet has become imperative. However, this widespread access presents a double-edged sword and opens doors for hackers and scammers to exploit vulnerabilities and engage in illegal activities. Accordingly, scholars and stakeholders are attempting to solve this matter. Large Language Models (LLMs) have provided highly effective methodologies and solutions in various cybersecurity sectors. Hence, we exhibited the efficacy of LLMs in several information and communication technologies (ICT) such as the Internet of Things (IoT), cloud computing, blockchain technology (BCT)…etc which are attacked and threatened. Accordingly, the objective of our study is to illustrate how LLMs are supporting ICT, especially BC to be secure against attacks. Another study's objective is to aid the stakeholders and enterprises that seek resilience and sustainability by recommending the most secure BC platform to adopt in critical sectors. Wherein, LLMs support BC in many directions as developing secure smart contracts and scanning the smart contract to protect it from any subversive acts by identifying anomalous activities. Hence, we suggested a soft opting model to rank the alternatives of BC platforms and recommend optimal BC. Also, the process of constructing this model requires leveraging several techniques. We applied for the first time SuperHyperSoft (SHS) as an extension of Hypersoft to treat various attributes and sub-attributes for BC based on LLMs. Multi-criteria decision-making (MCDM)techniques are utilized for their ability to treat conflicting sub-attributes. Hence, entropy and multi-objective optimization based on simple ratio analysis (MOOSRA) are utilized as techniques of MCDM. These techniques are working under the authority of the Single Value Neutrosophic (SVN) technique to support MCDM techniques in ambiguous situations.

Keywords: Large Language Models (LLMs); SuperHyperSoft; Blockchain; Cybersecurity; Multi-Criteria Decision Making (MCDM); Single Value Neutrosophic (SVN)

1. Introduction

The desire for sustainability and development on a global scale is seen as the driving force behind change and the growing rate of technological advancement. Indeed, in the recent interval, a new phenomenon dubbed Industry 4.0 [1] and eventually, Industry 5.0 has evolved.

These digital transformations permit devices and humans to communicate by utilizing smart devices as sensors in the Industrial Internet of Things (IIoT)[2] to collect data and process it through big data analytical (BDA) and store it in blockchain technology (BCT). Despite the importance of the technologies of Industry 4.0 in transferring and exchanging data, it is vulnerable to attacks. Accordingly, [3] indicated that the usage of cutting-edge technologies has expanded over the past several decades, leading to a significant increase in cyber-attacks and threats. This issue affects all stakeholders who utilize IoT systems, either directly or indirectly. Malicious assaults may cause enormous financial difficulties and incalculable losses, including data corruption, system breakdowns, privacy breaches, reputational damage, lost customers, dependability, and market share, especially for large enterprises. Wherein [4] claimed that only 16% of experts believe that their business is well-prepared to handle cybersecurity threats, even though 75% see cybersecurity as a priority.

Hence, [5] stated that it becomes imperative to have sophisticated and efficient detecting techniques. Similarly[6], as cyber threats evolve, the cybersecurity field can also benefit from state-of-the-art tools. These tools can support cybersecurity practitioners who are always looking for ways to apply new regulations or fortify technological defenses against the leakage of private data, illegal access, and other types of data abuse. According to the perspective of [7], it is imperative to develop proactiv5[5[5e technology for cyber defense. Wherein the defense is represented in harnessing various cutting-edge technologies such as Machine Learning (ML) techniques [5] and deep learning (DL) techniques [8] which are capable of automatically identifying, thwarting, also responding to various cyberattacks[9]. As well the new developments in transformers and large language models (LLMs)[10], which have demonstrated remarkable capabilities in natural language understanding, generation, and reasoning, have made significant strides in several security tasks, including threat detection, automated vulnerability analysis, intelligent defense mechanisms [11]. LLMs have a number of advantages, from customization and transparency to cutting-edge performance. LLMs are classified into open-source models like Llama [12] and Mixtral [13] or closed-source models like ChatGPT and Gemini[14]. They do, however, all have their limitations. Code-based LLMs, such as CodeLlama [15] and StarCoder [16, 17], are especially useful for tasks including automated code review, secure code development, and bug discovery. Their use in threat intelligence, binary analysis, IT operations, vulnerability detection, program repair, and anomaly detection highlights their revolutionary influence on cybersecurity.

1.1 Journey of Language Models Toward Large Language Models: Provenance

Contemporary techniques of artificial intelligence and machines have amalgamated to learn how to comprehend and communicate through human language [18] where a term of language modeling (LM) is the consequence of this amalgamation. This term has appeared in many

studies as [19] LM predominantly strives to forecast the probability of future or omitted tokens by modeling the generative probability of word sequences. As well [20] described the language model's evolution phases. The first phase formed in **statistical language models (SLMs)** [21]this model was initially introduced in the 1990s, and as it was constructed using the Markov assumption, its goal was to anticipate the next word based on the most recent context. The other side of it is bigram and trigram language models [19] where SLMs with a predetermined context length n that's why it's called n-gram language models. Generally, this is not a sufficient model, but newer versions have appeared due to some problems that this model suffered from. Worthwhile[22], neural networks (NNs) serve to predict the probability distribution of the following word in a sequence given the words that came before it as manner in phase two of **Neural Language Models (NLMs).** Wherein, the models of NLs are employed in this phase as multi-layer perceptron (MLP), Recurrent neural networks (RNNs), and (LSTM) [23]to provide a cohesive, comprehensive solution for different NLP. Phase three entails building what are known as **pre-trained language models (PLMs)** [24], which are contextualized word embeddings that seek to capture the meaning and context of words in a phrase or text. Nonetheless, several investigations have [25] examined the performance limitations PLMs encounter when training progressively broader PLMs. Thereby, Generative Pre-Trained Transformer -3 (GPT-3) and Generative Pre-Trained Transformer -4 (GPT-4) were developed to address the deficiencies in phase three. Due to[26], these models can be refined for certain downstream tasks, such as question answering or language translation, after being trained on vast volumes of text data. Accordingly, such models belong to **transformer language models [19]**, in another formula LLMs are considered motivators for phase four. Due to its ability to comprehend natural language and complete challenging tasks.

1.2 Motivations and incentives of study

Each phase finds a way to address the faults of the one before it, based on the discussion from the preceding subsection. In the final phase of LMs, GPT-3 as the model belongs to LLMs can solve a series of complex tasks that GPT-2 can't solve[27]. One of PLM's drawbacks[28], is it cannot generalize to unseen activities without task-specific training, although LLMs can do so without the need for task-specific training. As a result, LLMs serve as the study's focal point and foundation; further motivations will be covered.

A. **First incentive:** we conducted bibliometric analysis for various LMs. This analysis has been conducted on the Web of Science (WoS) database for various published studies from 2020 until 2024. Hence, we conducted a set of queries. Wherein these queries entailed the various techniques for different phases of LMs that were utilized in published studies.

B. These queries were conducted as in Fig 1

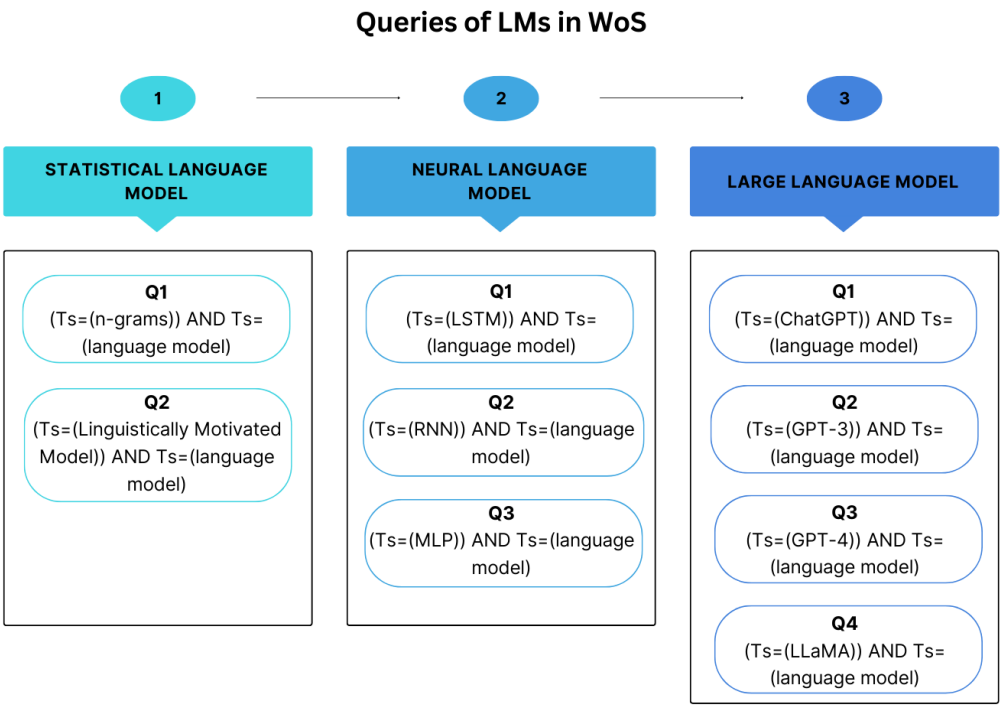
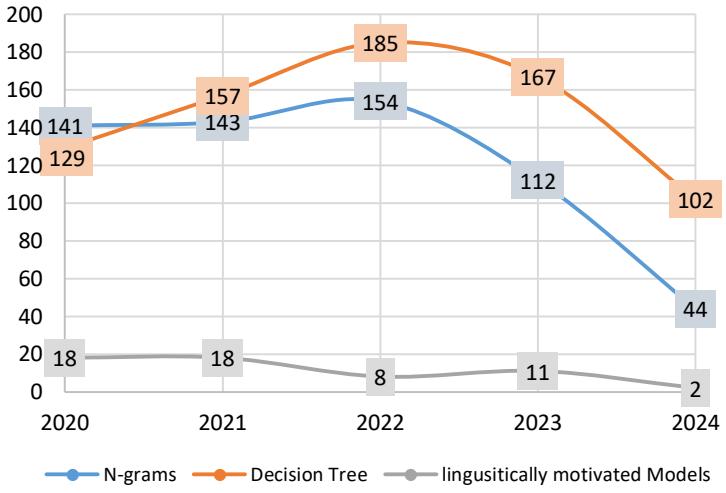


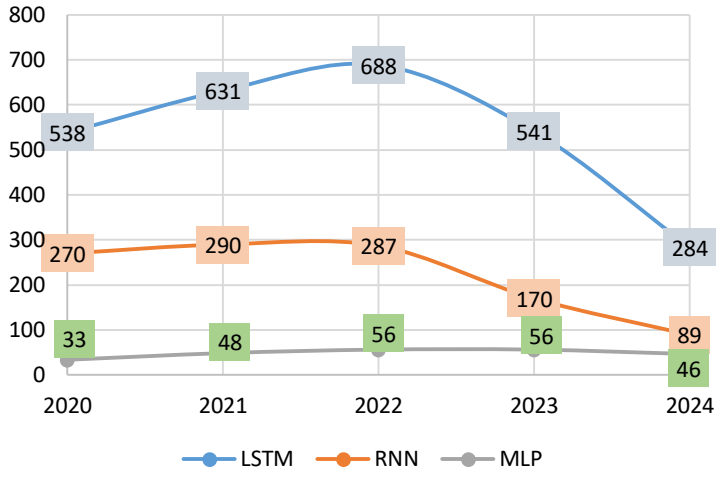
Fig 1. Methodologies of Techniques of Language Models Queries

The findings of conducted queries are illustrated in Fig 2 which comprises the queries' conclusions. This Fig indicated that the techniques of LLMs are constantly increasing over the years. In confirmation of this, in 2024 these techniques achieved the highest use in publishing studies compared to the other models of LMs.

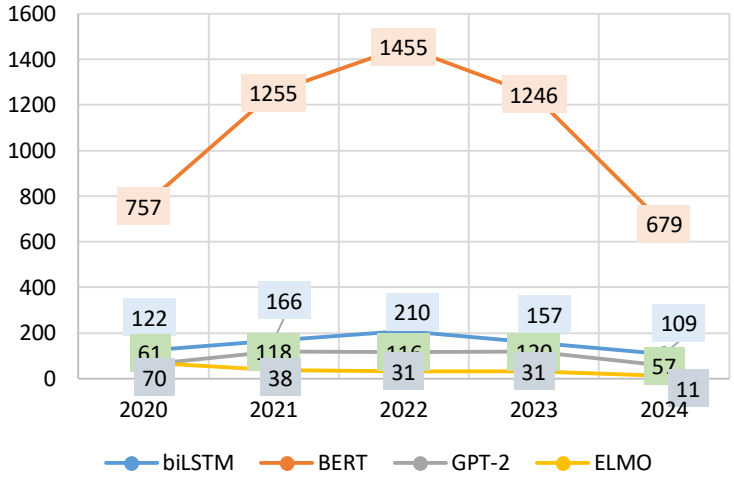
A. Second incentive: business environment and its chain, other domains such as healthcare, transportation, education…etc. are transforming their traditional strategies, planning, and operations into digital. In this light, [29] demonstrated that the urgency for effective security precautions has increased as individuals and enterprises depend on digital technology for essential infrastructure, interactions, and business. Thereby [30] stated that it is challenging for security practitioners to successfully identify, locate, and protect against them due to the magnitude and diversity of cyber threats. To address these issues, [31] suggested LLMs and [5] confirmed that LLMs help to swiftly find relevant threat intelligence, allowing consultants to decide on actions. Accordingly, [32]discussed various roles and contributions of LLMs in cybersecurity. Also [33] suggested Bidirectional Encoder Representations from Transformers (BERT) as an intrusion detection model and BERT outperforms other ML techniques in attack detection on a reputable dataset.



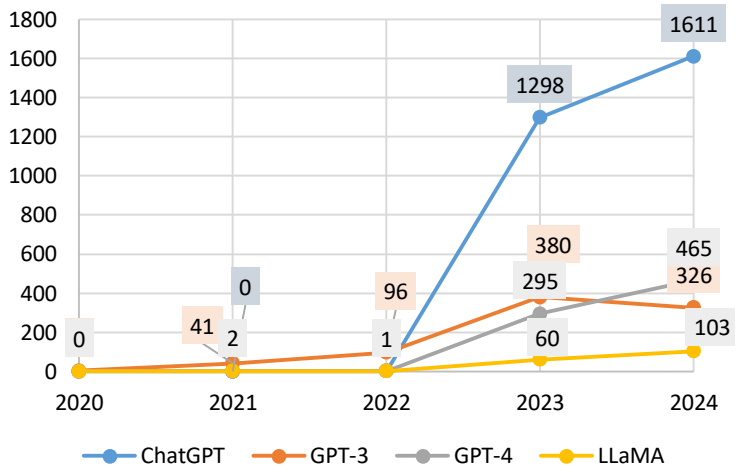
(a) Techniques of Statistical Language Models



(b) Techniques of Neural Language Model



(c) Techniques of Pretrained Language Model



(d) Techniques of Large Language Model

Fig 2. Queries' Findings for Language Models since 2020-2024

1.3 Scientific Contributions and Novelty:

This study attempts to solve the issue of cybersecurity by covering certain aspects as the following:

Theoretically: we conducted surveys in previous studies that related to our scope. We are trying to discuss and determine the main issues of security that threaten the enterprises economically and personally. Accordingly, we are studying the extent to which methods can solve this matter. The findings of our study are deployed in the next aspect (i.e. scientifically).

Scientifically: the findings of surveys are discussed by exhibiting the importance of generative artificial intelligence (AI)-LLMs for securing ICT technologies, especially BC. Also, evaluating the BC that adopting the models of LL is vital. Therefore, we proposed a soft opting model to evaluate these BC.

Practically: we applied the constructed model for two objectives. The first objective is aiding decision makers (DMs) and stakeholders at a loss to choose the secure BC by recommending secure BC based on LLMs. The second objective is to validate the accuracy of our model.

2. Empowering ICT technologies in the realm of LLMs

This section exhibits the role of LLMs in ICT technologies as security tools in various forms.

2.1 Cloud Computing Paradigm and IoT

Many scholars as[34, 35] described cloud computing (CC) as the multi-service paradigm for storing and retrieving data, computational capacity, and applications, such as internet-based on-demand services. CC has been harnessed successfully in several contexts Given that it offers a wide range of services such as control and management through various methodologies such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

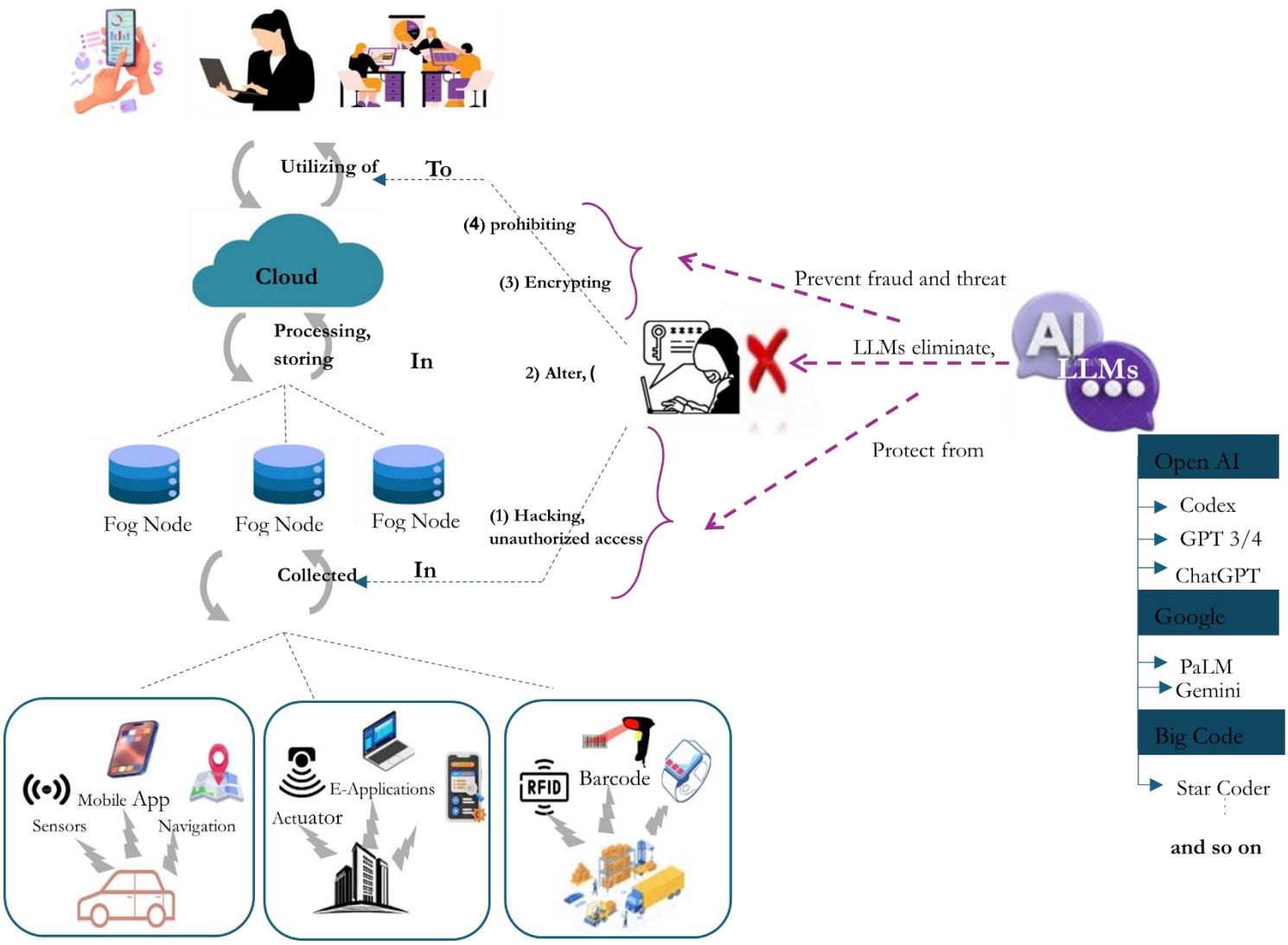


Fig 3. Role of Large Language Model in Securing Cloud-IoT against Threat

This paradigm integrated with other Contemporary technologies such as machine learning (ML) [36]to enhance the privacy, trust, and security of the cloud paradigm. But Cao et al., [37]had an alternative viewpoint and demonstrated that ML techniques are restricted to vulnerability analysis and categorization. Accordingly, the authors in [37] proposed LLMs as solvers for vulnerabilities of ML for securing the cloud. In the same vein [38] harnessed the CC paradigm in the internet of Vehicles (IoV) to store and process data collected from smart equipment as sensors in the Cloud paradigm and vice versa for retrieving data from the cloud. Wherein, LLMs play an important role as cybersecurity tools to countermeasure any threats and through [39] LLMs preserve resilience by facing hostile assaults, illegal access attempts, and data leaks. Fig 3 exhibits the role of LLMs which is discussed in [11] in securing data collected from IoT equipment and preventing hackers and spoofers from intrusion of information through unauthorized access. Also, LLMs are protecting information from encrypting, losing, and fraudulent vital information.

2.2 Blockchain Technology

Latterly, BCT is growing in popularity as a technology for promoting different domains[40]. As well, [41] indicated that Financial institutions brought in BCT to bolster their cybersecurity and investments. Distributed ledger (DL) technology allows BC to store transactions immutably. As stated by [42], BC security is an elaborate process that aims to protect the availability, integrity, and confidentiality of data processed and stored inside a blockchain network. Nevertheless, [43]admitted that the integrity and responsibilities of BC are in danger from several security flaws and threats. These threats formed in various forms as in [44] (see Fig 4) that exhibit vulnerabilities that jeopardize BC security.

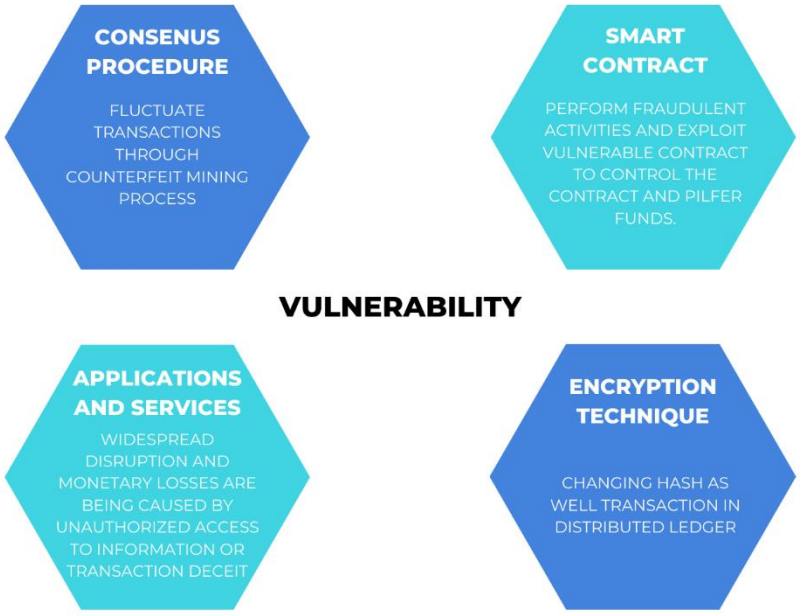


Fig 4. Blockchain Vulnerabilities

To eliminate and avoid the issues of vulnerability that jeopardize BC security, LLMs such as GPTScan [45], and AuditGPT [46] are introduced as auditors in smart contracts to detect and recognize vulnerabilities. As well, LLMs were introduced as detectors for unusual transactions and deceitful actions via leveraging BLOCKGPT[47].

3. Methodology

According to the influential role of LLMs as protectors against threats and risks, the evaluation of their roles in contemporary technology to be a secure technology is an important process. Accordingly, choosing the most secure technology amongst the set of alternatives to other technologies to serve the enterprises' objectives is crucial. This process requires prioritizing between the alternatives based on a set of conflicting criteria. Hence, MCDM techniques have been harnessed in this process due to their ability to treat such problems [48]. Yet experts may run into the issue of being unable to cope with uncertainties when using MCDM techniques, which prevents experts from being able to make an appropriate decision. To avert this issue, the SuperHyperSoft (SHs) technique is integrated with SVNSs to support experts when using MCDM techniques during the evaluation process amongst alternatives. Another impulse for this integration is to serve the study's objectives by constructing a soft opting model. These objectives entailed selecting and recommending the most secure BC platform that deploys LLMs as ChatGPT for developing smart contracts. The accuracy and security of smart contracts, which implement agreements without the need for middlemen, are crucial in BC.
Overall, the procedures of recommending a secure BC platform based on a soft opting model are conducted through the following subsections.
laying forth the assessment process's aspects

3.1 Laying forth the assessment process's main aspects

1. The alternatives of BC platforms are determined to be nominated in the evaluation process.
2. The main attributes and sub-attributes are determined to evaluate BC platforms based on them.
3. The expert panel is forming to contribute to the evaluation process for BC platforms based on attributes and sub-attributes.

3.2 Generative of attributes and sub-attributes weights: SVNSs-Entropy

The objective of this procedure is to generate weights for BC platforms' attributes and sub-attributes. Hence, the entropy of MCDM techniques is combined with SVNSs to generate weights. The generated weights are harassing in the next procedure of alternatives ranking. We implement a series of phases to accomplish the objective.

4. Transforming the utilized linguistic terms of DMs into Neutrosophic values based on the SVN scale which is mentioned in [49]. Thereby, Neutrosophic decision matrices are constructed based on the rating of DMs.
5. The score function in Eq.(1) is embraced for converting the constructed matrices into crisp matrices.

$$\boldsymbol{s}(\sigma_{ij}) = \frac{(2+ \alpha - \beta - \theta)}{3} \quad (1)$$

Where α, β, θ refer to truth, false, and indeterminacy respectively.

6. Aggregate the crisp matrices into a compiled matrix based on Eq.(2).

$$\wp_{ij} = \frac{(\sum_{j=1}^{N} \sigma_{ij})}{Z} \quad (2)$$

Where σ_{ij} refers to the value of the criterion in the matrix, and Z refers to the number of decision-makers.

7. Eq.(3) is utilized in the compiled matrix to normalize it to construct a normalized matrix.

$$\mathbb{N}or_{ij} = \frac{\wp_{ij}}{\sum_{j=1}^{m} \wp_{ij}} \quad (3)$$

Where $\sum_{j=1}^{m} \wp_{ij}$ indicates the sum of each criterion in the compiled matrix per column.

8. Eq.s(4),(5) are contributed to compute entropy.

$$En_{j=-h\sum_{i=1}^{m} \mathbb{N}or_{ij}} \ln \mathbb{N}or_{ij} \quad (4)$$

where,

$$h = \frac{1}{\ln(N)} \quad (5)$$

N refers to utilized alternatives

9. Finally, the weights of attributes are generated by employing Eq. (6)

$$\omega_j = \frac{1 - En_j}{\sum_{j=1}^{n}(1 - En_j)} \quad (6)$$

3.3 Recommending the most secure BC platform: SuperHyperSoft and SVNSs-MOOSRA

Herein, three techniques are integrated to rank BC platforms. Each technique plays a vital role in solving the problem of selection. SHS is utilized to determine and employ a power set of attributes to obtain the most secure and appropriate BC platform. While SVNSs are harnessed for supporting MOOSRA in uncertain environments and ambiguity of information during the ranking process.

3.3.1 SuperHyperSoft (SHS)

SHs introduced by Smarandache [50] this technique is considered an extension of HyperSoft and consists of several HyperSoft Sets. SHS was utilized in this study as the methodology for representing the determined attributes and sub-attributes for selecting the secure BC platform based on the selected attributes and sub-attributes.

- Suppose the universe set $\mathfrak{R}$= { BC_1, BC_2,… BC_n} which was determined in the previous procedure. Moreover, P ($\mathfrak{R}$) is the powerset of $\mathfrak{R}$. As well, A_1, A_2, A_3 are utilized attributes where BC platforms have been evaluated over these attributes. Hence, P(A_1), P(A_2), and P(A_3) are powersets of A_1, A_2, A_3.
- Let F: P(A_1) × P(A_2) × P(A_3) → P($\mathfrak{R}$), where × indicates to Cartesian product. Hence, this is called SHs over $\mathfrak{R}$.
- In this study Cartesian product for attributes and sub−attributes formed as

$$\mathrm{P}(\mathrm{A}_1)\times\mathrm{P}(\mathrm{A}_2)\times\mathrm{P}(\mathrm{A}_3)=\Big\{\big\{\{\mathrm{A}_{11}\},\{\mathrm{A}_{12}\},\{\mathrm{A}_{11},\mathrm{A}_{12}\}\big\}\times$$
$$\big\{\{\mathrm{A}_{21}\},\{\mathrm{A}_{22}\},\{\mathrm{A}_{21},\mathrm{A}_{22}\},\big\}\times$$
$$\big\{\{\mathrm{A}_{31}\},\{\mathrm{A}_{32}\},\{\mathrm{A}_{33}\},\{\mathrm{A}_{31},\mathrm{A}_{32}\},\{\mathrm{A}_{31},\mathrm{A}_{33}\},\{\mathrm{A}_{32},\mathrm{A}_{33}\},\{\mathrm{A}_{31},\mathrm{A}_{32},\mathrm{A}_{33}\}\big\}\Big\}.$$

  - According to Eq. (7), $\mathrm{P}(\mathrm{A}_1)\times\mathrm{P}(\mathrm{A}_2)\times\mathrm{P}(\mathrm{A}_3)=$

$$\left\{\begin{array}{c}\widetilde{s_1}\ (A_{11},A_{21},A_{31});\widetilde{s_2}\ (A_{11},A_{21},A_{32});\widetilde{s_3}\ (A_{11},A_{21},A_{33});\\ \widetilde{s_4}\ (A_{11},A_{21},\{A_{31},A_{32}\});\widetilde{s_5}\ (A_{11},A_{21},\{A_{31},A_{33}\});\widetilde{s_6}\ (A_{11},A_{21},\{A_{32},A_{33}\});\\ \widetilde{s_7}\ (A_{11},A_{21},\{A_{31},A_{32},A_{33}\});\widetilde{s_8}\ (A_{11},A_{22},A_{31});\dots\widetilde{s_{14}}\ (A_{11},A_{22},\{A_{31},A_{32},A_{33}\});\\ \widetilde{s_{15}}\ (A_{11},\{A_{21},A_{22}\},A_{31});\dots\widetilde{s_{21}}\ (A_{11},\{A_{21},A_{22}\},\{A_{31},A_{32},A_{33}\});\widetilde{s_{22}}\ (A_{12},A_{21},A_{31});\cdots\\ \widetilde{s_{28}}\ (A_{12},A_{21},\{A_{31},A_{32},A_{33}\});\widetilde{s_{29}}\ (A_{12},A_{22},A_{31});\cdots\widetilde{s_{35}}\ (A_{12},A_{22},\{A_{31},A_{32},A_{33}\});\\ \widetilde{s_{36}}\ (A_{12},\{A_{21},A_{22}\},A_{31});\ \cdots\widetilde{s_{42}}\ (A_{12},\{A_{21},A_{22}\},\{A_{31},A_{32},A_{33}\});\widetilde{s_{43}}\ (\{A_{11},A_{12}\},A_{21},A_{31});\cdots\\ \widetilde{s_{49}}\ (\{A_{11},A_{12}\},A_{21},\{A_{31},A_{32},A_{33}\});\widetilde{s_{50}}\ (\{A_{11},A_{12}\},A_{22},A_{31});\cdots\widetilde{s_{56}}\ (\{A_{11},A_{12}\},A_{22},\{A_{31},A_{32},A_{33}\});\\ \widetilde{s_{57}}\ (\{A_{11},A_{12}\},\{A_{21},A_{22}\},A_{31});\cdots\widetilde{s_{63}}\ (\{A_{11},A_{12}\},\{A_{21},A_{22}\},\{A_{31},A_{32},A_{33}\}).\end{array}\right\}$$

(7)

3.3.2 SVNSs-MOOSRA

Multi-objective optimization based on simple ratio analysis (MOOSRA)[51] is implemented under the authority of SVNSs based on SHS for ranking BC platforms that adopt ChatGPT-LLMs for developing secured smart contracts. After that recommend the most secure BC platform which implements the secured smart contract. Overall, the ranking procedures have been conducted as follows:

10. Constructing Neutrosophic decision matrices for each DM to evaluate BC platforms based on sub-attributes determined by SHS.
11. Transforming Neutrosophic decision matrices into de-neutrosophic decision matrices through using Eq.(1).
12. Eq.(2) is utilized for the second time to aggregate these matrices into an aggregated matrix.
13. Normalizing the aggregated matrix based on Eq.(8).

$$\mathrm{Nor}_{ij} = \frac{\wp_{ij}}{\left[\sum_{j}^{m} \wp_{ij}\right]^{1/2}} \quad (8)$$

14. Compute a weighted decision matrix based on Eq.(9).

$$\mathrm{weighted-matrix}_{ij=}\mathrm{Nor}_{ij} * \omega_j \quad (9)$$

15. Calculating ratio as in Eq.(10) to obtain final rank for alternatives.

$$\mathrm{Ratio} = \frac{\sum_{j=1}^{B} \mathrm{Nor}_{ij}}{\sum_{j=1}^{NB} \mathrm{Nor}_{ij}} \quad (10)$$

4. Implementation of the constructed soft opting model: Case-study

Herein we implemented our constructed soft opting model in realistic to validate the efficacy of the constructed model.

4.1 Problem Description

We exhibit the problem that our constructed model is supposed to be applied through the following scenario.

Scenario 1
One of the most significant technologies being utilized right now across a variety of sectors in BC, particularly in sectors with a long history and significant consumer data. This is because of the utilization of robust encryption techniques such as hash. Yet, because of the extensive usage of the Internet and its applications, hackers may now easily forge hash mining to alter and steal data, as well as smart contracts that expose the money and data of consumers to jeopardy. Hence, the business sectors exploit generative AI capabilities as LLMs to bolster the efficiency of BC as ChatGPT, PaLM…etc. these models of LLM support enterprises to be proactive and become resilient. Therefore, any business aiming for sustainability and resilience must

implement the strongest BC practices involving LLMs. Accordingly, businesses may face the problem of applying the strongest and most secure BC platform. We exhibit the problem of four enterprises that need to make accurate decisions for selecting the most secured BC platform based on LLMs amongst five alternatives of BC platforms.

Action: the businesses should follow the methodology for selecting the optimal and most secured BC which deploys the robust security models based on LLM. Herein, this methodology entails implementing the constructed soft opting model to aid stakeholders in deciding the optimal decision with various propositions toward securing businesses based on robust BC.

4.2 Toward Most Secure BC platform-based LLMs: Procedures

Herein, the process of recommending optimal BC has been conducted into two subsections for generating attributes' weights. These weights are used in another subsection to recommend optimal BC platforms.

4.1.1 Generating attributes' weights

Entropy based on SVNSs is implemented to serve the target of this subsection.

1. Three Neutrosophic decision matrices are constructed based on members of the panel to evaluate five BC platforms based on four attributes (see Fig 4). These matrices are transformed into de-neutrosophic matrices based on Eq.(1).
2. These matrices aggregated into the single matrix is an aggregated matrix as listed in Table 1 based on Eq.(2).
3. Table 2 exhibits the normalized matrix which is calculated based on Eq.(3).
4. Eq.(4) is implemented to compute entropy.
5. The final attributes' weights are obtained in Fig5 through executing Eq.(6) which indicates that A2 has the highest weight otherwise, A1 has the lowest value.

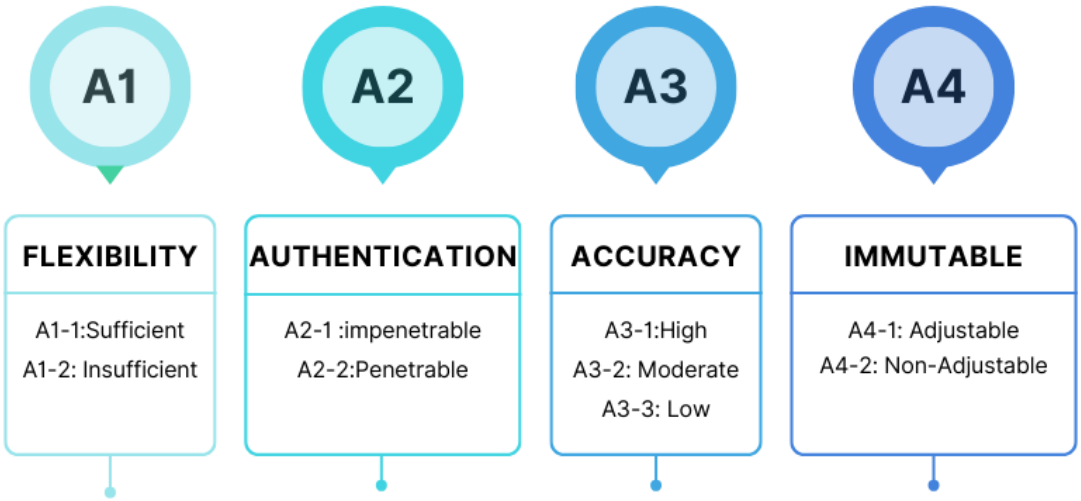


Fig 4. Attributes and Sub-attributes of BC based on LLMs

Table 1. Aggregated decision matrix

	A1	A2	A3	A4
BC1	0.604444444	0.5722222	0.42666667	0.672222222
BC2	0.816666667	0.5777778	0.71666667	0.9
BC3	0.538888889	0.38	0.5	0.537777778
BC4	0.705555556	0.8055556	0.65	0.816666667
BC5	0.644444444	0.7111111	0.81666667	0.838888889

Table 2. Normalized matrix

	A1	A2	A3	A4
BC1	0.182611615	0.18781911	0.137191854	0.178518737
BC2	0.24672709	0.189642597	0.230439443	0.239008557
BC3	0.162806311	0.124726477	0.160771704	0.14281499
BC4	0.213158778	0.264405543	0.209003215	0.216878135
BC5	0.194696207	0.233406273	0.262593783	0.222779581

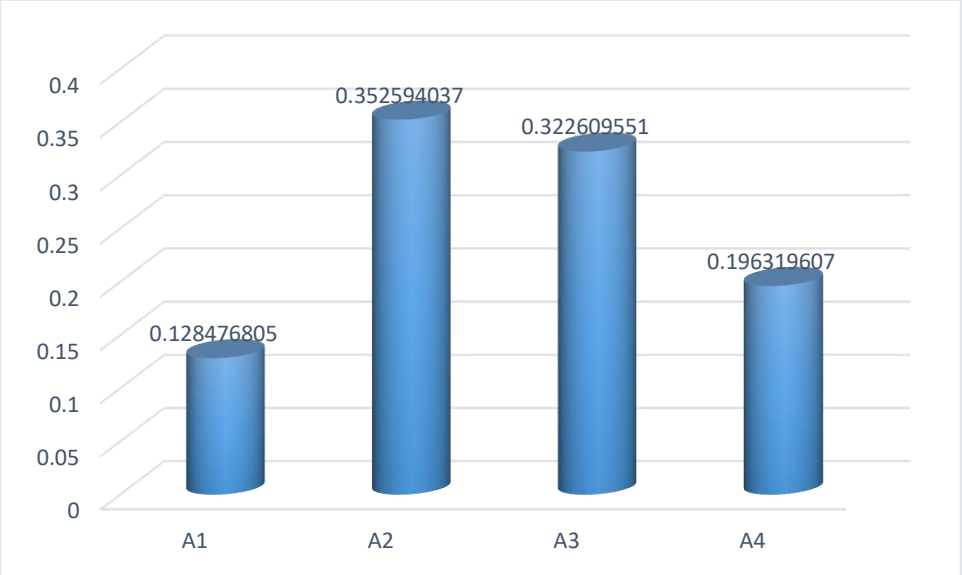


Fig 5. Attributes weights

4.2.2 Ranking BC Platforms

Based on the methodology of SHS we can suppose a set of propositions for sub-attributes to rank BC based on LLMs :

- let F({Sufficient, Non-sufficient}, {Impenetrable, Penetrable},{Low},{Non-Adjustable}).
- According to Eq.(7), there are four propositions for sub-attributes. in other words, there are four hypersofts:

proposition 1: Sufficient, Impenetrable, Low, Non-Adjustable.
proposition 2: Sufficient, Penetrable, Low, Non-Adjustable
proposition 3: Non-sufficient, Impenetrable, Low, Non-Adjustable
proposition 4: Non-sufficient, Penetrable, Low, Non-Adjustable

After that, we can implement SVNSs-MOOSRA to rank BC platforms and obtain the most secure BC.

According to Proposition 1:

- Three neutrosophic decision matrices are constructed for evaluating BC platforms based on sub-attributes according to the proposition.
- deneutrosophic these matrices based on Eq.(1).
- Aggregated these matrices into an aggregated matrix based on Eq.(2) as in Table 3.
- Table 4 represents the normalized matrix according to Eq.(8).
- Table 5 for the weighted normalized matrix is generated based on Eq.(9).

The final ranking for BC platforms is exhibited in Fig 6 which indicates that BC4 is the most secure platform.

Table 3. Aggregated matrix

	A11	A21	A31	A42
BC1	0.644444	0.56	0.353333	0.605556
BC2	0.498889	0.76	0.386667	0.777778
BC3	0.42	0.498889	0.538889	0.666667
BC4	0.598889	0.877778	0.732222	0.458889
BC5	0.565556	0.665556	0.632222	0.671111

Table 4. Normalized matrix.

	A11	A21	A31	A41
BC1	0.522865	0.365028	0.288437	0.420175
BC2	0.40477	0.495395	0.315648	0.539675
BC3	0.340764	0.325194	0.439911	0.462578
BC4	0.485904	0.572167	0.597735	0.318408
BC5	0.458859	0.433833	0.516102	0.465662

Table 5. Weighted Normalized matrix

	A11	A21	A31	A42
BC1	0.040783461	0.095272375	0.04384238	0.050421043
BC2	0.031572024	0.129298223	0.047978453	0.064760973
BC3	0.026579566	0.084875588	0.066866523	0.055509405
BC4	0.037900492	0.149335667	0.090855749	0.038208974
BC5	0.035791003	0.113230461	0.078447529	0.055879468

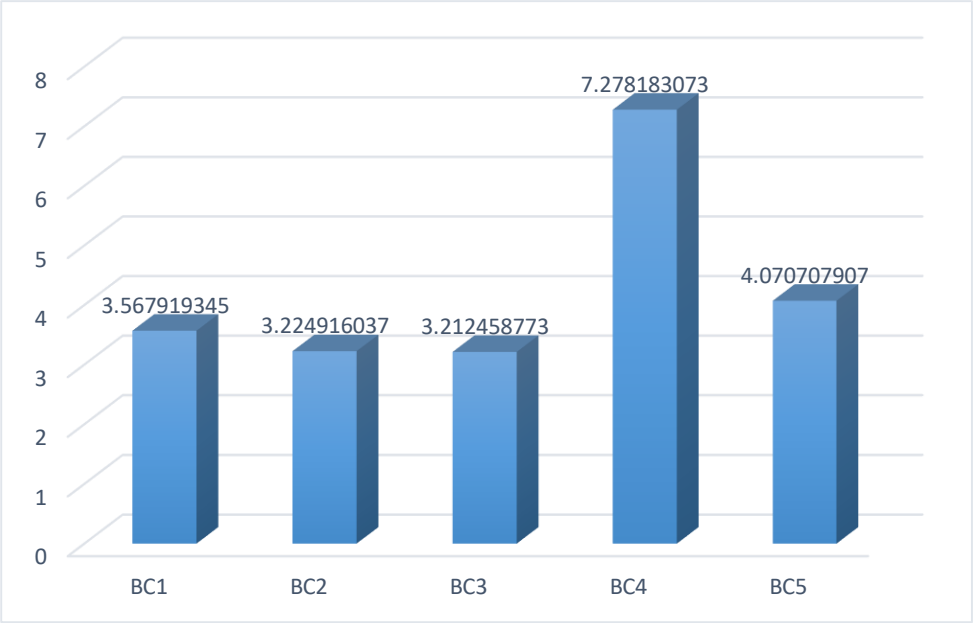


Fig 6. Final ranking for BC platforms

According to Proposition 2:

- Table 6 represents the normalized matrix according to Eq.(8).
- Table 7 for the weighted normalized matrix is generated based on Eq.(9).

Table 6. Normalized matrix

	A11	A22	A31	A42
BC1	0.404239135	0.452016567	0.288436709	0.420175361
BC2	0.546168684	0.518707536	0.315647719	0.539674775
BC3	0.360397023	0.44460646	0.439911333	0.462578379
BC4	0.471860019	0.358649211	0.597735192	0.318408118
BC5	0.430990254	0.447570503	0.516102162	0.465662235

Table 7. Weighted Normalized matrix

	A11	A22	A31	A42
BC1	0.031530653	0.041585524	0.04384238	0.050421043
BC2	0.042601157	0.047721093	0.047978453	0.064760973
BC3	0.028110968	0.040903794	0.066866523	0.055509405
BC4	0.036805082	0.032995727	0.090855749	0.038208974
BC5	0.03361724	0.041176486	0.078447529	0.055879468

According to Proposition 3:

- Table 8 represents the normalized matrix according to Eq.(8).

- Table 9 for the weighted normalized matrix is generated based on Eq.(9).

Table 8. Normalized matrix

	A12	A21	A31	A42
BC1	0.159831631	0.365028256	0.288436709	0.420175361
BC2	0.409092866	0.49539549	0.315647719	0.539674775
BC3	0.513744529	0.325193823	0.439911333	0.462578379
BC4	0.570827254	0.572167306	0.597735192	0.318408118
BC5	0.466175591	0.433833185	0.516102162	0.465662235

Table 9. Weighted Normalized matrix

	A12	A21	A31	A42
BC1	0.008151413	0.0335826	0.04384238	0.050421043
BC2	0.020863736	0.045576385	0.047978453	0.064760973
BC3	0.026200971	0.029917832	0.066866523	0.055509405
BC4	0.02911219	0.052639392	0.090855749	0.038208974
BC5	0.023774955	0.039912653	0.078447529	0.055879468

According to Proposition 4:

- Table 10 represents the normalized matrix according to Eq.(8).

- Table 11 for the weighted normalized matrix is generated based on Eq.(9).

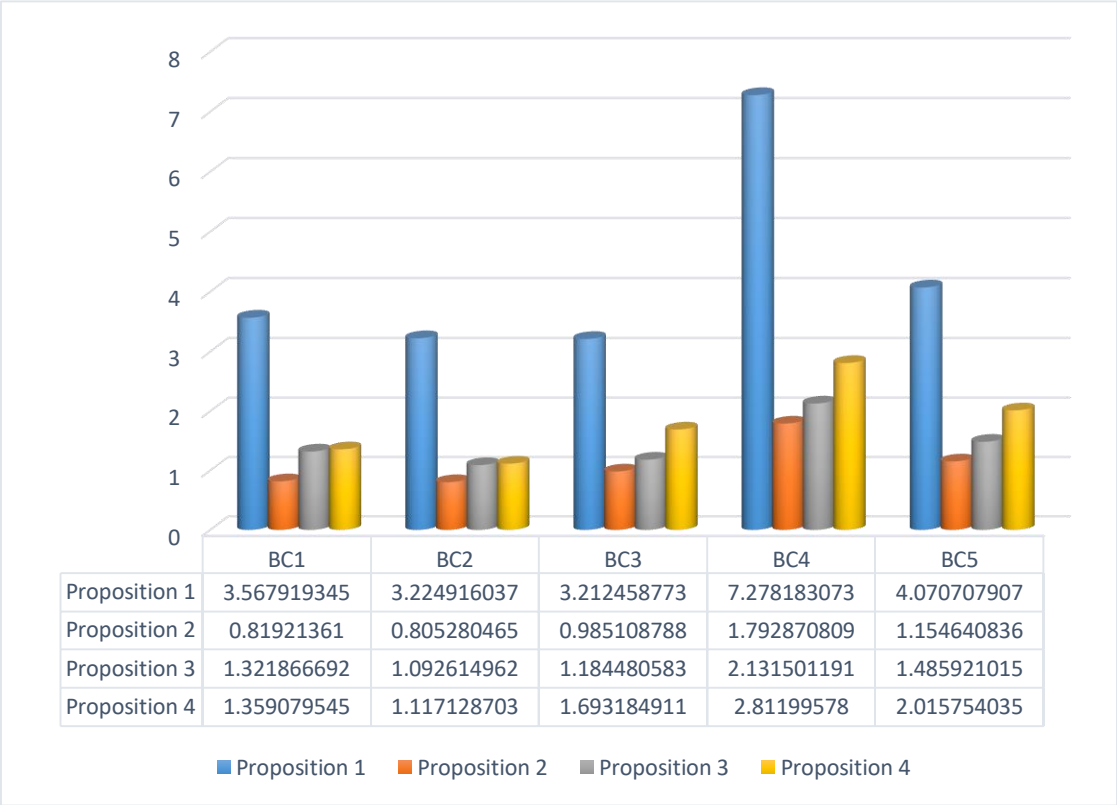
Table 10. Normalized matrix

	A12	A22	A31	A42
BC1	0.159831631	0.452016567	0.288436709	0.420175361
BC2	0.409092866	0.518707536	0.315647719	0.539674775
BC3	0.513744529	0.44460646	0.439911333	0.462578379
BC4	0.570827254	0.358649211	0.597735192	0.318408118
BC5	0.466175591	0.447570503	0.516102162	0.465662235

Table 11. Weighted Normalized matrix

	A12	A22	A31	A42
BC1	0.008151413	0.041585524	0.04384238	0.050421043
BC2	0.020863736	0.047721093	0.047978453	0.064760973
BC3	0.026200971	0.040903794	0.066866523	0.055509405
BC4	0.02911219	0.032995727	0.090855749	0.038208974
BC5	0.023774955	0.041176486	0.078447529	0.055879468

- After we applied the four propositions or four hypersoftsets, we concluded that BC5 is the most secure and appropriate for utilizing against any attack as shown in Fig 7.



	BC1	BC2	BC3	BC4	BC5
Proposition 1	3.567919345	3.224916037	3.212458773	7.278183073	4.070707907
Proposition 2	0.81921361	0.805280465	0.985108788	1.792870809	1.154640836
Proposition 3	1.321866692	1.092614962	1.184480583	2.131501191	1.485921015
Proposition 4	1.359079545	1.117128703	1.693184911	2.81199578	2.015754035

Fig 7. Final ranking for BC platforms based on various propositions

5 Conclusion

In this study, we attempt to solve the problem of attacks and exploiting vulnerabilities, especially in digital technologies. Hence, we focused on BC as one of the important technologies for many sectors Especially financial sectors and transactions that require customer information. Thus, fraudulent and dubious actions endanger financial establishments as well as people by corrupting and leaking data through encryption. Accordingly, LLMs can be harnessed to protect transactions and DL from any manipulation. through applying PaLM, BLOCKGPT, GPTu-tor….etc to scan smart contracts, detecting and recognizing unusual and abnormal activities as well, these models can develop secured smart contracts. Hence, we exhibit the importance of adopting LLMs in BC to make any business proactive and resilient against any crisis that is facing any sector.

Yet, stakeholders may face the problem of which BC platform can use. Hence, we constructed a soft opting model to aid them in recommending the most appropriate and secure BC. In these models, we applied for the first time SHS for supporting a set of propositions of sub-attributes.

Entropy is applied to generate weights for attributes and sub-attributes which are proposed by SHS to utilize in MOOSRA for recommending optimal BC based on LLMs.

The findings of a soft opting model indicated that BC 4 is the most secure platform to adopt in enterprises.

References

1. Ustundag, A., et al., *Overview of cyber security in the industry 4.0 era.* Industry 4.0: managing the digital transformation, 2018: p. 267-284.
2. Toussaint, M., S. Krima, and H. Panetto, *Industry 4.0 data security: A cybersecurity frameworks review.* Journal of Industrial Information Integration, 2024: p. 100604.
3. Weber, R.H. and E. Studer, *Cybersecurity in the Internet of Things: Legal aspects.* Computer Law & Security Review, 2016. **32**(5): p. 715-728.
4. Pandey, S., et al., *Cyber security risks in globalized supply chains: conceptual framework.* Journal of Global Operations and Strategic Sourcing, 2020. **13**(1): p. 103-128.
5. Ferrag, M.A., et al., *Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices.* IEEE Access, 2024.
6. Kaur, R., D. Gabrijelčič, and T. Klobučar, *Artificial intelligence for cybersecurity: Literature review and future research directions.* Information Fusion, 2023. **97**: p. 101804.
7. Hassanin, M. and N. Moustafa, *A Comprehensive Overview of Large Language Models (LLMs) for Cyber Defences: Opportunities and Directions.* arXiv preprint arXiv:2405.14487, 2024.
8. Salim, S., et al., *Deep federated learning-based threat detection model for extreme satellite communications.* IEEE Internet of Things Journal, 2023.
9. Farah, J.C., et al. *Impersonating chatbots in a code review exercise to teach software engineering best practices*. in *2022 IEEE Global Engineering Education Conference (EDUCON)*. 2022. IEEE.
10. Wu, J., *Literature review on vulnerability detection using NLP technology. arXiv 2021.* arXiv preprint arXiv:2104.11230, 2021.
11. Zhang, J., et al., *When llms meet cybersecurity: A systematic literature review.* arXiv preprint arXiv:2405.03644, 2024.
12. Touvron, H., et al., *Llama: Open and efficient foundation language models.* arXiv preprint arXiv:2302.13971, 2023.
13. Jiang, A.Q., et al., *Mixtral of experts.* arXiv preprint arXiv:2401.04088, 2024.
14. Team, G., et al., *Gemini: a family of highly capable multimodal models.* arXiv preprint arXiv:2312.11805, 2023.
15. Roziere, B., et al., *Code llama: Open foundation models for code.* arXiv preprint arXiv:2308.12950, 2023.
16. Li, R., et al., *Starcoder: may the source be with you!* arXiv preprint arXiv:2305.06161, 2023.
17. Lozhkov, A., et al., *Starcoder 2 and the stack v2: The next generation.* arXiv preprint arXiv:2402.19173, 2024.
18. Mao, Y., et al., *A Survey on LoRA of Large Language Models.* arXiv preprint arXiv:2407.11046, 2024.

19. Zhao, W.X., et al., *A survey of large language models.* arXiv preprint arXiv:2303.18223, 2023.
20. Hadi, M.U., et al., *A survey on large language models: Applications, challenges, limitations, and practical usage.* Authorea Preprints, 2023.
21. Gao, J. and C.-Y. Lin, *Introduction to the special issue on statistical language modeling*. 2004, ACM New York, NY, USA. p. 87-93.
22. Bengio, Y., R. Ducharme, and P. Vincent, *A neural probabilistic language model.* Advances in neural information processing systems, 2000. **13**.
23. Kombrink, S., et al. *Recurrent Neural Network Based Language Modeling in Meeting Recognition*. in *Interspeech*. 2011.
24. Vaswani, A., *Attention is all you need.* arXiv preprint arXiv:1706.03762, 2017.
25. Kaplan, J., et al., *Scaling laws for neural language models.* arXiv preprint arXiv:2001.08361, 2020.
26. Yang, J., et al., *Harnessing the power of llms in practice: A survey on chatgpt and beyond.* ACM Transactions on Knowledge Discovery from Data, 2024. **18**(6): p. 1-32.
27. Wei, J., et al., *Chain-of-thought prompting elicits reasoning in large language models.* Advances in neural information processing systems, 2022. **35**: p. 24824-24837.
28. Kalyan, K.S., *A survey of GPT-3 family large language models including ChatGPT and GPT-4.* Natural Language Processing Journal, 2023: p. 100048.
29. Sarker, I.H., et al., *Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures.* Internet of Things, 2024: p. 101110.
30. Ferrag, M.A., et al., *Generative AI and Large Language Models for Cyber Security: All Insights You Need.* arXiv preprint arXiv:2405.12750, 2024.
31. Yao, Y., et al., *A survey on large language model (llm) security and privacy: The good, the bad, and the ugly.* High-Confidence Computing, 2024: p. 100211.
32. Liu, Z. *A review of advancements and applications of pre-trained language models in cybersecurity*. in *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*. 2024. IEEE.
33. Devlin, J., et al., *BERT: Pre-training of deep bidirectional transformers for language understanding. NAACL HLT. 2019*. 1810.
34. Putzier, M., et al., *Implementation of cloud computing in the German healthcare system.* NPJ Digital Medicine, 2024. **7**(1): p. 12.
35. Gharib, M., F. Smarandache, and M. Mohamed, *CSsEv: Modelling QoS Metrics in Tree Soft Toward Cloud Services Evaluator based on Uncertainty Environment*. 2024: Infinite Study.
36. Ayyadapu, A.K.R., *Secure Cloud Infrastructures: A Machine Learning Perspective.* International Neurourology Journal, 2022. **26**(4): p. 22-29.
37. Cao, D. and W. Jun. *LLM-CloudSec: Large Language Model Empowered Automatic and Deep Vulnerability Analysis for Intelligent Clouds*. in *IEEE INFOCOM 2024-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2024. IEEE.
38. Desai, B. and K. Patil, *Secure and Scalable Multi-Modal Vehicle Systems: A Cloud-Based Framework for Real-Time LLM-Driven Interactions.* Innovative Computer Sciences Journal, 2023. **9**(1): p. 1− 11-1− 11.

39. Pal, S., et al., *A domain-specific next-generation large language model (LLM) or ChatGPT is required for biomedical engineering and research.* Annals of biomedical engineering, 2024. **52**(3): p. 451-454.
40. Smarandache, F., M. Mohamed, and M. Voskoglou, *Evaluating Blockchain Cybersecurity Based on Tree Soft and Opinion Weight Criteria Method under Uncertainty Climate.* HyperSoft Set Methods in Engineering, 2024. **1**: p. 1-10.
41. Peters, G.W. and E. Panayi, *Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money*. 2016: Springer.
42. He, Z., et al., *NURGLE: Exacerbating Resource Consumption in Blockchain State Storage via MPT Manipulation.* arXiv preprint arXiv:2406.10687, 2024.
43. Berdik, D., et al., *A survey on blockchain for information systems management and security.* Information Processing & Management, 2021. **58**(1): p. 102397.
44. Xu, H., et al., *Large language models for cyber security: A systematic literature review.* arXiv preprint arXiv:2405.04760, 2024.
45. Sun, Y., et al. *Gptscan: Detecting logic vulnerabilities in smart contracts by combining gpt with program analysis*. in *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. 2024.
46. Xia, S., et al., *AuditGPT: Auditing Smart Contracts with ChatGPT.* arXiv preprint arXiv:2404.04306, 2024.
47. Gai, Y., et al., *Blockchain large language models.* arXiv preprint arXiv:2304.12749, 2023.
48. Sahoo, S.K. and S.S. Goswami, *A comprehensive review of multiple criteria decision-making (MCDM) Methods: advancements, applications, and future directions.* Decision Making Advances, 2023. **1**(1): p. 25-48.
49. El-Henawy, I., et al., *Modeling Influenced Criteria in Classifiers' Imbalanced Challenges Based on TrSS Bolstered by The Vague Nature of Neutrosophic Theory*. 2024: Infinite Study.
50. Smarandache, F., *Foundation of the SuperHyperSoft Set and the Fuzzy Extension SuperHyperSoft Set: A New Vision.* Neutrosophic Systems with Applications, 2023. **11**: p. 48-51.
51. Feizi, F., A.A. Karbalaei-Ramezanali, and S. Farhadi, *FUCOM-MOORA and FUCOM-MOOSRA: new MCDM-based knowledge-driven procedures for mineral potential mapping in greenfields.* SN Applied Sciences, 2021. **3**: p. 1-19.

Received: April 1, 2024. Accepted: Aug 25, 2024