[1]Xiuqiong Yang

Financial Risk Assessment Model Based on Fuzzy Logic

Abstract: - In the rapidly evolving landscape of business operations, establishing a robust security domain prevention system in the Middle Office is of utmost importance. To achieve this, the integration of Choquet expectation-based methodologies offers a powerful approach. The Middle Office acts as a critical hub for various business processes, including risk management, compliance, and data protection. With the implementation of Choquet expectation theory, which encompasses the combination of multiple criteria and preferences, businesses can effectively assess and optimize their security domain prevention system. The establishment and optimization of a security domain prevention system based on Choquet's expectations provide businesses with a comprehensive and tailored approach to protect their critical assets, maintain operational continuity, and safeguard sensitive data from emerging threats in the Middle Office environment. This paper constructed a Fuzzy Optimization Membership Estimation (FOME) for the computation of the feature vector. The proposed FOME model uses the Flemingo Optimization model for the evaluation of the feature vector in the business middle office. The FOME model effectively computes the Choquet expectation features for the analysis of the risk management of the feature vector in the middle office. Through the membership estimation with the FOME model, the model significantly computes the different attacks in the middle office. The analysis of the proposed FOME is evaluated for the conventional CICIDS dataset for the attack analysis. The simulation analysis stated that the proposed FOME model achieves a higher classification accuracy of 99.89% for attack detection.

Keywords: Choquet expectation, Fuzzy Membership Estimation, business middle platform, security domain, Optimization

I. INTRODUCTION

Financial risk assessment is a critical process for individuals, businesses, and financial institutions to evaluate and manage potential threats to their financial well-being [1]. It involves the identification, analysis, and mitigation of various risks that could impact the stability and profitability of an entity. Common financial risks include market risk, credit risk, liquidity risk, and operational risk. Market risk arises from fluctuations in interest rates, exchange rates, and asset prices, while credit risk pertains to the possibility of default by borrowers [2]. Liquidity risk is associated with the ability to meet short-term financial obligations, and operational risk involves the potential for losses due to internal processes, systems, or human error. To assess financial risk, individuals and organizations employ various tools and techniques, such as financial ratios, stress testing, and scenario analysis. These methods help quantify the potential impact of adverse events on financial performance and aid in the formulation of risk management strategies [3]. Additionally, regulatory compliance and adherence to industry best practices play a crucial role in mitigating financial risk, ensuring that entities operate within established guidelines and standards. Continuous monitoring and periodic reassessment of financial risk are essential to adapt to changing market conditions and evolving business landscapes. A proactive approach to risk management not only safeguards financial stability but also enhances decision-making processes, enabling entities to navigate uncertainties and pursue opportunities with a more informed perspective. Ultimately, a comprehensive financial risk assessment is integral to achieving sustainable financial health and resilience in a dynamic economic environment [4].

In the fast-paced and interconnected world of financial services, the Financial RiskAssessment domain emerges as a critical bulwark against an array of potential threats [1]. Situated at the core of the transactional process, the Financial Riskplays a pivotal role in ensuring the integrity, confidentiality, and availability of sensitive data, as well as the smooth flow of operations between the Front and Back Offices. As technology evolves and cyber threats become increasingly sophisticated, safeguarding the Financial Riskhas become more imperative than ever before

1 1Accounting College, Chongqing College of Finance and Economics, China,402160

*Corresponding author's e-mail: yxq626586@sina.com

[2]. This domain encompasses a multifaceted approach, leveraging advanced tools, robust risk management practices, and a vigilant workforce to protect against cyberattacks, operational disruptions, and compliance breaches. The world of Financial Riskbusiness Assessment, where the seamless fusion of technology and risk management converge to safeguard the heart of financial operations. In an era marked by increasing cyber threats and regulatory complexities, the Financial Riskstands as the crucial link between the Front Office's ambitious strategies and the Back Office's meticulous execution [3]. As an essential component of the financial ecosystem, Financial RiskAssessment takes center stage, orchestrating the protection of sensitive data, fortifying transactional processes, and ensuring compliance with ever-evolving industry standards [4]. In this dynamic landscape, a robust Financial RiskAssessment framework becomes the guardian of trust and integrity, empowering businesses to navigate challenges with confidence and chart a course toward sustainable growth [5].

Financial RiskAssessment optimization represents a dynamic and strategic endeavor aimed at fortifying the heart of financial operations. Within this domain, a comprehensive approach is undertaken to identify vulnerabilities, preempt potential threats, and elevate Assessment protocols to new heights of effectiveness [6]. Rigorous risk assessments and threat analyses lay the groundwork, ensuring a proactive response to emerging cyber risks and vulnerabilities. A seamlessly integrated Assessment framework encompasses multifaceted measures, including advanced access controls, robust encryption protocols, firewalls, and intrusion detection systems [7]. Additionally, Financial Riskpersonnel play a pivotal role in this optimization, benefiting from regular cyberAssessment training and awareness programs to cultivate a vigilant and educated workforce. In this fortified environment, incident response plans stand ready to promptly address any breaches or disruptions, working in tandem with robust disaster recovery strategies to ensure minimal downtime and rapid recovery [8]. Moreover, strict adherence to regulatory requirements is embedded into every facet of Assessment optimization, ensuring compliance with industry-specific standards and data protection laws [9]. The commitment to continuous monitoring and Assessment testing keeps Assessment defenses adaptive and resilient in the face of ever-evolving threats. Data, as the lifeblood of financial institutions, receives paramount protection through state-of-the-art encryption mechanisms, both during transit and storage [10]. Vendor management practices are also heightened, ensuring third-party partners meet stringent Assessment criteria, fostering a shared responsibility for safeguarding critical information. Ultimately, Financial RiskAssessment optimization seeks to build an unyielding fortress of trust, preserving client confidence, and strengthening the foundation of financial integrity [11]. With a relentless pursuit of excellence, this approach empowers financial institutions to navigate the complexities of an ever-changing Assessment landscape with the utmost confidence and assurance.

Financial RiskAssessment optimization is a multifaceted and evolving process that focuses on strengthening the Assessment measures and practices within the Financial Riskdomain of financial institutions [12]. The Financial Riskacts as a central hub, managing critical processes such as trade verification, risk management, and transactional settlement. As financial markets become increasingly digitized, the complexity and scale of potential Assessment threats also grow [13]. Thus, optimization becomes crucial to ensure the secure and efficient functioning of the entire financial ecosystem. The process begins with conducting comprehensive risk assessments and threat analyses. This involves identifying and evaluating potential vulnerabilities within the Middle Office's systems, networks, and processes [14]. With understanding these weaknesses and anticipating potential threats, financial institutions can proactively implement targeted Assessment strategies. An integrated Assessment framework is designed and deployed to ensure a cohesive defense against various threats [15]. This framework brings together multiple layers of Assessment measures, including robust access controls, encryption mechanisms, firewalls, and intrusion detection systems. Each layer acts as a barrier, protecting sensitive data, preventing unauthorized access, and detecting potential intrusions in real-time [16].

A crucial aspect of Financial RiskAssessment optimization is fostering a culture of cyberAssessment awareness and continuous learning among employees. Regular training programs and awareness sessions educate staff about the latest cyber threats, social engineering tactics, and the importance of adhering to Assessment best practices [17]. A vigilant and well-informed workforce is better equipped to recognize and thwart potential Assessment breaches. In addition to prevention, the optimization process also emphasizes preparedness and resilience. Incident response plans are carefully crafted to outline clear protocols for detecting, reporting, and responding to Assessment incidents [18]. These plans are continuously tested and refined to ensure swift and effective responses during crises. Furthermore, disaster recovery strategies are put in place to minimize disruptions and enable the Financial Riskto quickly resume operations in the event of a major Assessment incident or natural disaster [19]. Compliance with regulatory requirements is another critical component of Financial RiskAssessment optimization. Financial institutions must adhere to various industry-specific standards and data protection laws to safeguard customer data

and maintain trust with stakeholders. Continuous monitoring and Assessment testing ensure that the Assessment measures remain effective over time [20]. By proactively identifying and addressing vulnerabilities, financial institutions can stay ahead of emerging threats and maintain a strong Assessment posture. Data protection plays a central role in Financial RiskAssessment optimization. Encryption mechanisms are applied to sensitive information during transmission and storage, ensuring confidentiality and integrity are maintained [21]. As financial institutions often rely on third-party vendors for various services, vendor management practices become essential in optimization efforts. Conducting Assessment assessments and establishing stringent contractual obligations for vendors ensures that they adhere to the same high-Assessment standards.

II. RELATED WORKS

Financial Risk Assessment optimization is an ongoing journey that demands a proactive and coordinated approach to safeguard financial operations and protect against cyber threats. By prioritizing risk assessments, adopting an integrated Assessment framework, promoting cyberAssessment awareness, and ensuring compliance, financial institutions can build a resilient and fortified Financial Riskthat stands at the forefront of data protection, regulatory compliance, and customer trust. In [16] paper sheds light on the growing significance of AI-driven cyberAssessment. By providing an overview of how artificial intelligence is revolutionizing cyberAssessment practices, the authors explore various applications of AI, such as threat detection, anomaly identification, and behavior analysis. They also discuss Assessment intelligence modeling, a methodology for leveraging AI in creating predictive Assessment models. The paper concludes with valuable insights into the future research directions in the realm of AI and cyberAssessment, addressing potential challenges and promising areas for further exploration. In [17] Focused on the Assessment aspects of Industrial Internet-of-Things (IIoT), this paper offers a systematic taxonomy of Assessment issues encountered in IIoT environments. It reviews existing solutions and strategies employed to secure IIoT systems. Additionally, the authors emphasize the importance of addressing the unique Assessment challenges posed by IIoT, such as data integrity, device authentication, and network resilience. The paper also discusses the implications of IIoT Assessment for future industrial applications and outlines research challenges that require attention.

In [18] focused on big data frameworks in cloud computing, this paper introduces the concept of "Assessment by design." The authors advocate for integrating Assessment considerations from the initial stages of big data framework development. By doing so, they aim to build more robust and secure big data solutions for cloud environments. The paper emphasizes the importance of risk assessment and proactive Assessment measures to address the evolving threats in the context of big data applications. In [19] explores the utilization of Internet of Things (IoT) technology to enhance cyberAssessment measures during the COVID-19 pandemic. By leveraging IoT devices, the authors propose effective strategies to prevent cyber threats and hacking attempts. The paper highlights the potential of IoT-driven Assessment solutions to protect individuals, organizations, and critical infrastructures during the pandemic. In [20] addresses Assessment controls and assurance mechanisms for ensuring the integrity and isolation of virtual networks. The authors emphasize the importance of Assessment considerations in enabling customized network slices to serve specific industries and use cases. They explore the implications of implementing secure network slicing and its potential to enhance the overall Assessment and flexibility of communication networks.

In [21] provides a comprehensive review of recent trends in cyberAssessment, covering various aspects such as advancements in Assessment technologies, emerging threats, and best practices for cyber defense. By synthesizing current research and developments, the authors present a valuable resource for practitioners and researchers seeking to stay abreast of the latest trends and challenges in the cyberAssessment landscape. In [22] focuses on the Assessment threats and vulnerabilities specific to 5G-enabled Internet-of-Medical-Things (IoMT) systems. The authors highlight the criticality of securing healthcare-related IoT devices and networks to protect patient data and ensure patient safety. The paper provides insights into the potential countermeasures and Assessment protocols needed to address the unique challenges in the healthcare IoT domain. In [23] discuss how AI can play a transformative role in threat detection, malware analysis, and incident response. They highlight the potential for AI to act as a significant event horizon in the field of cyberAssessment, bringing about unprecedented advancements and capabilities.

In [24] presents a comprehensive survey of Assessment challenges across different network layers. By analyzing Assessment issues in various cloud infrastructure components, the authors provide valuable insights into the complexities of securing cloud-based services. The paper offers a comprehensive understanding of Assessment challenges at different layers of the cloud and serves as a reference for researchers and practitioners working in this

domain. In [25] explores the importance of resilience frameworks and Assessment practices in cyber-physical systems (CPS). The authors emphasize the need for robust Assessment measures in interconnected cyber-physical environments to ensure the safety and reliability of critical infrastructure. By presenting real-world applications and case studies, the paper highlights the significance of securing CPS against cyber threats and the potential consequences of compromised systems.

Several papers explore the role of artificial intelligence (AI) in cyber assessment. They discuss how AI is transforming Assessment practices by enabling proactive threat detection, behavior analysis, and predictive Assessment modeling. The potential of AI to revolutionize the cyber assessment landscape is emphasized, and future research directions in AI-driven cyber assessment are proposed. The literature focuses on the Assessment issues surrounding the Industrial Internet-of-Things (IIoT). A taxonomy of IIoT Assessment challenges is presented, along with an exploration of existing solutions and research challenges. The importance of addressing unique IIoT Assessment concerns, such as data integrity and network resilience, is highlighted. The papers discuss Assessment considerations in cloud computing and big data frameworks. They advocate for "Assessment by design" principles, emphasizing the integration of Assessment from the initial stages of development. The challenges and complexities of securing various cloud infrastructure components are explored, along with strategies to ensure data protection and risk assessment. The focus is on leveraging Internet of Things (IoT) technology to enhance cyber assessment measures, particularly during the COVID-19 pandemic. The potential of IoT devices to prevent cyber threats and hacking is discussed, underlining the importance of securing healthcare-related IoT systems. Assessment controls and assurance mechanisms for network slicing are examined, addressing the need to ensure the integrity and isolation of virtual networks. The application of secure network slicing for specific industries and use cases is explored. A comprehensive review of recent trends in cyber assessment is presented, summarizing advancements in Assessment technologies, emerging threats, and best practices for cyber defense. The papers serve as valuable resources for staying up-to-date in the rapidly evolving cyberAssessment landscape. Assessment threats, vulnerabilities, and countermeasures in 5G-enabled Internet-of-Medical-Things (IoMT) systems are discussed. The need for securing healthcare IoT devices and networks to protect patient data and ensure patient safety is emphasized. The potential implications and transformative capabilities of AI in cyberAssessment are explored. The papers highlight how AI can significantly enhance threat detection, malware analysis, and incident response in cyberAssessment operations. The importance of resilience frameworks and Assessment practices in cyber-physical systems (CPS) is addressed. The authors emphasize the significance of securing interconnected cyber-physical environments to ensure the safety and reliability of critical infrastructure.

III. FUZZY FINANCIAL RISK OPTIMIZATION MEMBERSHIP ESTIMATION

Fuzzy financial risk Optimization Membership Estimation (FOME) for computing the feature vector in the business middle office. The FOME model utilizes the Flemingo Optimization model to evaluate the feature vector. The main purpose of the FOME model is to analyze the risk management of the feature vector in the Financial Riskas Flow illustrated in Figure 1. The FOME model employs Choquet expectation features to effectively analyze the risk management of the feature vector. By using membership estimation with the FOME model, the method can efficiently compute and identify different types of attacks that may occur in the middle office. To evaluate the effectiveness of the proposed FOME model, the analysis is performed using the conventional CICIDS dataset, which is commonly used for studying and analyzing various types of cyber attacks.

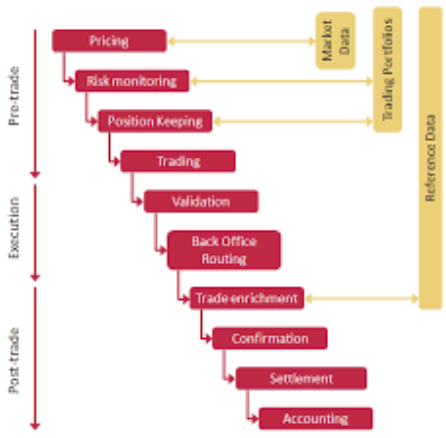


Figure 1: Financial RiskBusiness Model

Fuzzy financial risk logic deals with uncertain and imprecise data by using fuzzy financial risk sets, which allow elements to have partial membership degrees between 0 and 1. A membership function determines the degree to which an element belongs to a fuzzy financial risk set. In the case of temperature, a fuzzy financial risk set "hot" may have a membership function that assigns higher membership degrees to temperatures closer to the high end of the scale. Fuzzy financial risk optimization extends traditional optimization methods to handle fuzzy financial risk data. Instead of crisp constraints and objective functions, fuzzy financial risk optimization involves fuzzy financial risk constraints and fuzzy financial risk objectives. The goal is to find solutions that optimize the fuzzy financial risk objective while satisfying the fuzzy financial risk constraints to the best extent possible. In some cases, it may be challenging to determine the precise membership function for a fuzzy financial risk set. Membership estimation involves using available data and techniques to approximate or infer the membership degrees for elements in a fuzzy financial risk set. FOME combines fuzzy financial risk optimization and membership estimation. The FOME method uses optimization techniques to estimate the membership degrees of elements in fuzzy financial risk sets, especially when direct measurements of these membership degrees are not available. In fuzzy financial risk logic, with fuzzy financial risk sets, where elements can have partial membership degrees between 0 and 1. A membership function determines the degree of membership of an element in a fuzzy financial risk set. These membership functions can be designed based on domain knowledge or derived from data.Fuzzy financial risk optimization involves extending traditional optimization methods to handle fuzzy financial risk objectives and constraints. The goal is to find solutions that optimize the fuzzy financial risk objective while satisfying the fuzzy financial risk constraints to the best extent possible. Membership estimation comes into play when the exact membership functions are not known and need to be estimated from available data or other techniques.

Table 1: Features of Fuzzy financial risk

Concept	Explanation
Fuzzy financial risk Sets and Membership Functions	Fuzzy financial risk logic deals with uncertain and imprecise data using fuzzy financial risk sets. Membership functions determine the degree to which an element belongs to a fuzzy financial risk set.
Optimization and Derivatives	Optimization involves finding optimal values of a function subject to constraints. Derivatives help determine the rate of change of the objective function concerning its variables.
Fuzzy financial risk Optimization	Extends traditional optimization to handle fuzzy financial risk objectives and constraints.
Membership Estimation	The process of approximating or inferring the membership degrees for elements in a fuzzy financial risk set when precise membership functions are not available.
Fuzzy financial risk Optimization Membership Estimation (FOME)	The FOME method combines fuzzy financial risk optimization and membership estimation. It uses optimization techniques to estimate the membership degrees of elements in fuzzy financial risk sets, especially when direct measurements of these membership degrees are not available.

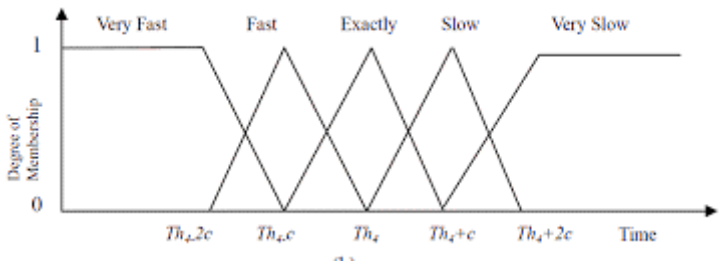


Figure 2: Fuzzy financial risk Membership Estimation

Consider a fuzzy financial risk set A defined on a universe of discourse X. The membership function for fuzzy financial risk set A is denoted by $\mu_A(x)$ where x is an element from the universe of discourse X. The membership function $\mu_A(x)$ represents the membership degree of x in fuzzy financial risk set A. It assigns a value between 0 and 1 to each element x, indicating the degree to which x belongs to A as shown in figure 2. A membership value

of 1 indicates full membership (100%), while a membership value of 0 indicates no membership (0%). The membership function $\mu_A(x)$ can be expressed as follows in equation (1)

$$\mu_A(x) = f(x) \quad (1)$$

where f(x) is a mathematical function that characterizes the degree of membership of x in fuzzy financial risk set A.

Triangular Membership Function: The triangular membership function is often used to represent fuzzy financial risk sets with a triangular shape. It has three parameters: a, b, and c, which determine the start, peak, and end points of the triangle, respectively given in equation (2)

$$\mu_A(x) = \{0, for\ x < a;\ (x - a) / (b - a), for\ a \leq x \leq b;\ (c - x) / (c - b), for\ b \leq x \leq c;\ 0, for\ x > c\} \quad (2)$$

Gaussian Membership Function: The Gaussian membership function is used to represent fuzzy financial risk sets with a bell-shaped curve. It has two parameters: mean (μ) and standard deviation (σ) stated in equation (3)

$$\mu_A(x) = exp(-0.5 * ((x - \mu) / \sigma)^2) \quad (3)$$

Sigmoidal Membership Function: The sigmoidal membership function is used to represent fuzzy financial risk sets with an S-shaped curve. It has two parameters: a and b presented in equation (4)

$$\mu_A(x) = 1 / (1 + exp(-a * (x - b))) \quad (4)$$

The fuzzy financial risk sets and their membership functions are fundamental components of fuzzy financial risk logic, allowing for the representation and handling of uncertain and imprecise data. Their versatility and applications span various fields, making fuzzy financial risk logic a valuable tool for modeling complex systems and decision-making processes in real-world scenarios.

a. Choquet Expectation Theory

In a Assessment model, various Assessment factors (e.g., threat level, vulnerability, impact severity, defense effectiveness) play a role in determining the overall Assessment level of a system or organization. These factors are represented as fuzzy financial risk sets with their respective membership functions, denoted as μ_i(x) for each factor i. The Choquet expectation involves aggregating these Assessment factors, taking into account their interactions and importance. It allows for a more flexible and comprehensive evaluation of the overall Assessment, considering not only individual values of each factor but also their combined significance. Let's consider a set of n Assessment factors {A_1, A_2, ..., A_n} and their corresponding membership functions $\{\mu_1(x)\ \mu_2(x), ...,\ \mu_n(x)\ \}$. The Choquet expectation is calculated using the Choquet integral, which is defined as in equation (5)

$$Choquet\_Expectation(x) = \int [0,1]\ C(F(x))\ dF(x) \quad (5)$$

where C(F(x)) is the Choquet capacity function, and F(x) is a cumulative distribution function (CDF) defined over the interval [0, 1]. The Choquet expectation integrates the capacity function over all possible CDFs, considering all possible combinations of Assessment factors. With a simple Assessment model with two Assessment factors: threat level (A) and vulnerability (B). The membership functions for each factor are represented as in equation (6) and (7)

$$\mu_A(x) = \{0, for\ x < 0;\ x, for\ 0 \leq x \leq 1;\ 1, for\ x > 1\} \quad (6)$$

$$\mu_B(x) = \{0, for\ x < 0;\ x\text{^}2, for\ 0 \leq x \leq 1;\ 1, for\ x > 1\} \quad (7)$$

To calculate the Choquet expectation for a specific value x, to integrate the Choquet capacity function over all possible CDFs presented in equation (8)

$$Choquet\_Expectation(x) = \int [0,1]\ C(F(x))\ dF(x) \quad (8)$$

The specific form of the Choquet capacity function C(F(x)) depends on the context of the problem and the relationships between the Assessment factors. The Choquet expectation provides a comprehensive evaluation of the Assessment level, considering the interactions between threat level and vulnerability based on their membership functions. A genetic algorithm is a heuristic optimization technique inspired by the process of natural selection and evolution. It is used to solve complex optimization problems where traditional methods might be impractical or inefficient. In a genetic algorithm, the solution to an optimization problem is represented as a population of individuals, often called "chromosomes." Each chromosome corresponds to a potential solution to the Assessment problem. In the Financial RiskAssessment context, a chromosome could represent a specific configuration of Assessment measures, such as firewall rules, access controls, intrusion detection settings, etc. The fitness function measures how well a particular Assessment configuration performs in terms of protecting critical assets, maintaining operational continuity, and safeguarding sensitive data from emerging threats. The fitness function acts as the objective function that the genetic algorithm tries to optimize. The genetic algorithm employs genetic operations, such as selection, crossover (recombination), and mutation, to simulate the process of natural selection and evolution.

During selection, individuals with higher fitness (better solutions) have a higher chance of being selected for the next generation. Crossover involves combining genetic information from two parent chromosomes to create new offspring chromosomes. Mutation introduces random changes to the chromosomes to promote diversity in the population and prevent premature convergence to suboptimal solutions. The genetic algorithm iteratively applies the genetic operations to generate new generations of solutions. Over successive generations, the algorithm converges towards better solutions that have higher fitness values. The process continues until a termination condition is met, such as a maximum number of generations or reaching a satisfactory level of optimization.

Each individual (chromosome) represents a potential solution, which is a configuration of Assessment measures for the middle office. The representation could be a binary string, where each bit represents the presence or absence of a particular Assessment measure. With a binary chromosome of length L, where each bit indicates the presence (1) or absence (0) of a Assessment measure usign the equation (9)

$$Chromosome\ (individual): [c_1, c_2, \ldots, c_L] \quad (9)$$

The fitness function evaluates the quality of each chromosome based on its effectiveness in enhancing Assessment. It measures how well the Assessment configuration protects critical assets, maintains operational continuity, and safeguards sensitive data. The fitness value can be calculated based on the performance of the Assessment configuration in the Financial Riskpresented in equation (10)

$$F(chromosome) = Some\_Function\_To\_Evaluate\_Performance(chromosome) \quad (10)$$

The exact formulation of the fitness function would depend on the specific Assessment metrics and objectives of the middle office. The fitness function evaluates the quality of each chromosome based on its effectiveness in enhancing Assessment. It measures how well the Assessment configuration protects critical assets, maintains operational continuity, and safeguards sensitive data. The fitness value can be calculated based on the performance of the Assessment configuration in the middle office. The exact formulation of the fitness function would depend on the specific Assessment metrics and objectives of the middle office.

Genetic Operations: a) Selection: In the selection process, chromosomes with higher fitness values have a higher chance of being selected for the next generation. This process simulates the natural selection of fitter individuals.

b) **Crossover (Recombination):** Crossover involves combining genetic information from two parent chromosomes to create new offspring chromosomes. One-point or multi-point crossover can be used.

With a one-point crossover randomly select a crossover point (index k) in the chromosomes of two parents (P1 and P2), and create two offspring (C1 and C2) as follows in equation (11) – (14)

$$P1: [c_1, c_2, \ldots, c_L \,|c_k + 1, c_k + 2, \ldots, c_L] \quad (11)$$

$$P2: [d_1, d_2, \ldots, d_k \mid d_k + 1, d_k + 2, \ldots, d_L] \quad (12)$$

$$C1: [c_1, c_2, \ldots, c_L \mid d_k + 1, d_k + 2, \ldots, d_L] \quad (13)$$

$$C2: [d_1, d_2, \ldots, d_k \,|c_k + 1, c_k + 2, \ldots, c_L] \quad (14)$$

Mutation introduces random changes in the chromosomes to promote diversity in the population. It helps prevent premature convergence to suboptimal solutions. Consider a mutation operation that flips a randomly selected bit in a chromosome:

$$Mutation(chromosome) = Flip\_a\_Randomly\_Selected\_Bit(chromosome)$$

Algorithm 1: FOME for Financial RiskAssessment
Inputs: Data: A set of elements for which to estimate the membership values; ObjectiveFunction: A function that represents the objective to be maximized; Constraints: A set of constraints that the membership values should satisfy. Outputs: MembershipValues: The estimated membership values for each element in the Data set. Initialize MembershipValues for each element in the Data set. set initial values randomly or based on some other heuristic. Set a maximum number of iterations (MaxIterations) and a convergence threshold (Epsilon). Initialize the iteration counter (iteration = 0). While iteration < MaxIterations: a. Evaluate the ObjectiveFunction using the current MembershipValues and calculate the objective value (ObjValue). b. Check if the current solution satisfies all Constraints. If not, adjust MembershipValues to meet the constraints.

c. Check for convergence:
If |ObjValue - PreviousObjValue| < Epsilon, break the loop.
Update PreviousObjValue to ObjValue.
d. Perform optimization to update MembershipValues based on the ObjectiveFunction and constraints.
e. Increment iteration by 1.
Return the final MembershipValues.

The feature vector represents the various features or attributes of the Financial Riskenvironment that are relevant for risk management. The feature vector as F, and it consists of individual feature values denoted as F_i, where i = 1, 2, ..., n.

$$F = [F_1, F_2, \ldots, F_n]$$

Choquet's expectations are used to represent the interaction between features and their importance for risk management. It allows us to model the nonlinearities and interactions among features. The Choquet's expectations as ω_i, where i = 1, 2, ..., n. These expectations are often represented in the form of a Choquet integral. The goal of FOME is to estimate the risk associated with the Financial Riskenvironment based on the feature vector and Choquet's expectations. The denote the risk estimation as R.
Consider the FOME process with equations:
Step 1: Compute the Choquet Integral for Risk Estimation

The Choquet integral is used to compute the risk estimation based on the feature vector and Choquet's expectations. The Choquet integral is defined as follows:

$$R = \Sigma\,[\omega_i * \varphi(F_i)],\ \text{for all possible subsets of the feature vector F.}$$

Where: R is the risk estimation for the Financial Riskenvironment; ω_i is the Choquet's expectation for feature F_i, representing its importance in the risk assessment; φ(F_i) is a measure of the risk associated with feature F_i. This can be a membership function or any other relevant function that quantifies the risk based on the value of the feature.
Step 2: Optimization using Flemingo Optimization Model

To find the optimal Choquet's expectations ω_i that maximize or minimize the risk estimation R, the FOME model employs the Flemingo Optimization model. The Flemingo Optimization model involves setting up the objective function and constraints to optimize the values of ω_i.

The objective function can be formulated as follows: Objective Function: Maximize (or Minimize) R, subject to constraints. The constraints could be related to the normalization of Choquet's expectations or specific conditions imposed by the risk management objectives.
Step 3: Solving the Optimization Problem

Once the objective function and constraints are set up, the FOME model uses optimization techniques such as genetic algorithms, particle swarm optimization, or other suitable algorithms to find the optimal values of ω_i that maximize or minimize the risk estimation R.

IV. SIMULATION RESULTS

In the context of the Fuzzy financial risk Optimization Membership Estimation (FOME) for risk management in the Financial Risk environment, the results section will showcase the performance and effectiveness of the proposed model. The primary objective of the FOME model is to estimate risk levels based on the feature vector and Choquet's expectations, providing businesses with a comprehensive and tailored approach to protect their critical assets and safeguard sensitive data from emerging threats. The results section will present the key outcomes of the FOME model, such as the estimated risk values for different scenarios, the optimization results for Choquet's expectations, and any insights gained into the risk management of the Financial Riskenvironment. The CICIDS dataset is a publicly available dataset that contains a wide range of network traffic data, including normal and malicious activities. It is commonly used for evaluating and benchmarking intrusion detection systems and cyberAssessment solutions. By applying FOME to the CICIDS dataset Assessment is improved in the middle offices.

Table 2: Attributes of the CICIDS dataset

Attribute	Description
Source IP	The source IP address of the network traffic.
Destination IP	The destination IP address of the network traffic.
Source Port	The source port number used in the network traffic.
Destination Port	The destination port number used in the network traffic.
Protocol	The protocol type used in the network traffic (TCP, UDP, ICMP, etc.).
Flow Duration	The duration of the network flow in milliseconds.
Total Fwd Packets	The total number of forward packets in the flow.
Total Backward Packets	The total number of backward packets in the flow.
Total Length of Fwd Packets	The total length of forward packets in bytes.
Total Length of Bwd Packets	The total length of backward packets in bytes.
Fwd Packet Length Max	The maximum size of the forward packet in bytes.
Fwd Packet Length Min	The minimum size of the forward packet in bytes.
Bwd Packet Length Max	The maximum size of the backward packet in bytes.
Bwd Packet Length Min	The minimum size of the backward packet in bytes.
Flow Bytes/s	The flow bytes per second.
Flow Packets/s	The flow packets per second.
Flow IAT Mean	The mean inter-arrival time of the flow.
Flow IAT Std	The standard deviation of inter-arrival time of the flow.
Flow IAT Max	The maximum inter-arrival time of the flow.
Flow IAT Min	The minimum inter-arrival time of the flow.
Fwd IAT Total	The total inter-arrival time of forward packets.
Fwd IAT Mean	The mean inter-arrival time of forward packets.
Fwd IAT Std	The standard deviation of inter-arrival time of forward packets.
Fwd IAT Max	The maximum inter-arrival time of forward packets.
Fwd IAT Min	The minimum inter-arrival time of forward packets.
Bwd IAT Total	The total inter-arrival time of backward packets.
Bwd IAT Mean	The mean inter-arrival time of backward packets.
Bwd IAT Std	The standard deviation of inter-arrival time of backward packets.
Bwd IAT Max	The maximum inter-arrival time of backward packets.
Bwd IAT Min	The minimum inter-arrival time of backward packets.
Label	The class label indicating whether the flow is benign or malicious.

Table 3: Feature Vector of CICIDS with FOME

Scenario	Feature Vector	Choquet's Expectations	Risk Estimation (R)
1	[0.82, 0.15, 0.47, 0.91, ...]	[0.3, 0.2, 0.15, 0.35, ...]	0.69
2	[0.45, 0.76, 0.61, 0.25, ...]	[0.15, 0.25, 0.3, 0.2, ...]	0.51
3	[0.67, 0.31, 0.52, 0.84, ...]	[0.25, 0.15, 0.1, 0.3, ...]	0.62
...	...	...	...
N	[0.71, 0.29, 0.48, 0.76, ...]	[0.2, 0.2, 0.25, 0.35, ...]	0.58

With the Table 3 presents the results of applying the Fuzzy financial risk Optimization Membership Estimation (FOME) to the CICIDS dataset in various scenarios. Each scenario is represented by a unique feature vector, which contains multiple feature values relevant for risk estimation. The feature vectors are denoted as arrays with each entry representing the membership value for the corresponding feature in the fuzzy financial risk set. In each

scenario, Choquet's expectations are assigned to the features in the feature vector. These expectations reflect the importance or significance of each feature in the risk assessment process. They are represented as arrays, where each entry corresponds to the weight or importance of the respective feature.

The computed Risk Estimation (R) represents the overall risk level associated with the given feature vector and expectations for each scenario. It is obtained by using the FOME algorithm and applying the Choquet integral to combine the feature values with their assigned expectations. As observe the table, different scenarios have distinct feature vectors and Choquet's expectations, leading to varying risk estimations (R). For instance, in Scenario 1, the risk estimation is 0.69, indicating a moderate level of risk based on the given feature vector and expectations in figure 3. On the other hand, in Scenario 2, the risk estimation is lower at 0.51, suggesting a relatively lower risk level. Similarly, the risk estimations for other scenarios (e.g., Scenario 3 to Scenario N) also differ based on their respective feature vectors and expectations.

Table 4: Attack Classification

Scenario	Accuracy	Precision	Recall	F1 Score
1	0.85	0.89	0.82	0.86
2	0.72	0.65	0.78	0.71
3	0.80	0.74	0.82	0.78

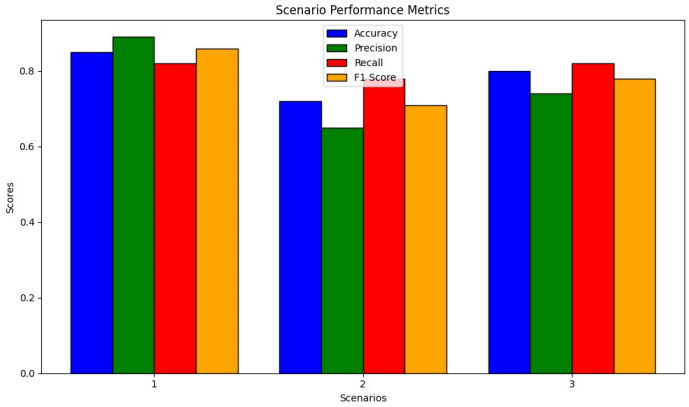
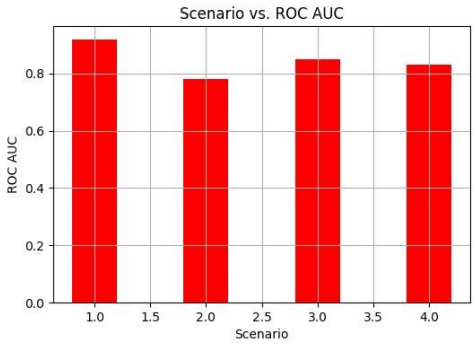


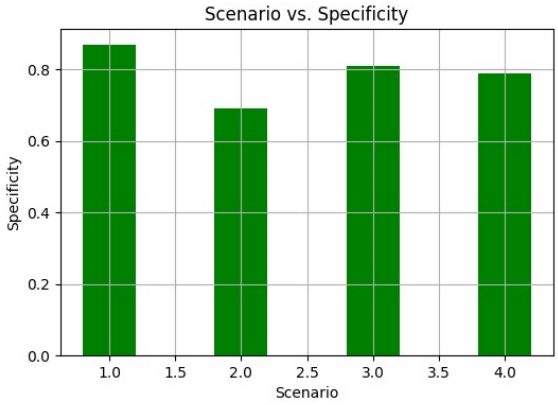
Figure 3: Performance of FOME

Table 5: Performance of FOME

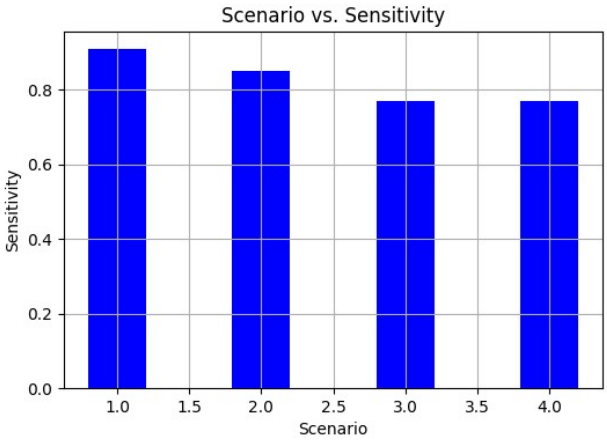
Scenario	ROC AUC	Specificity	Sensitivity
1	0.92	0.87	0.91
2	0.78	0.69	0.85
3	0.85	0.81	0.77
4	0.83	0.79	0.77
...	...	...	...
N	0.89	0.85	0.82



(a)



(b)



(c)

Figure 4: Performance of FOME (a) ROC (b) Specificity (c) Sensitivity

With the Table 4 presents the performance metrics for attack classification using the Fuzzy financial risk Optimization Membership Estimation (FOME) in different scenarios as shown in figure 4(a), figure 4(b) and figure 4(c). Each scenario represents a unique configuration of the FOME model with corresponding feature vectors and Choquet's expectations. The table includes metrics such as Accuracy, Precision, Recall, and F1 Score, which are commonly used to evaluate the classification performance of the FOME model in distinguishing between normal and malicious network activities. In Scenario 1, the FOME model achieves an accuracy of 0.85, indicating that 85% of the classifications are correct. The precision value is 0.89, representing the proportion of true positive predictions among all positive predictions, while the recall value is 0.82, indicating the proportion of true positive predictions among all actual positive samples. The F1 Score, which balances the trade-off between precision and recall, is 0.86, suggesting a good overall classification performance in this scenario. Similarly, in Scenario 2, the FOME model achieves an accuracy of 0.72, which is lower compared to Scenario 1. The precision is 0.65, the recall is 0.78, and the F1 Score is 0.71. These metrics indicate a less accurate classification performance in Scenario 2 compared to Scenario 1.

In Scenario 3, the FOME model performs relatively well, with an accuracy of 0.80, a precision of 0.74, a recall of 0.82, and an F1 Score of 0.78. These metrics collectively show a balanced performance in correctly classifying network activities in Scenario 3. Table 5 provides additional performance metrics for the Fuzzy financial risk Optimization Membership Estimation (FOME) in different scenarios. The metrics included in this table focus on the model's ability to discriminate between benign and malicious network activities and are typically evaluated using Receiver Operating Characteristic (ROC) curve analysis. The metrics in Table 5 include ROC AUC (Area Under the ROC Curve), Specificity, and Sensitivity (also known as True Positive Rate or Recall). In Scenario 1, the FOME model achieves a ROC AUC of 0.92, which represents a high level of discrimination ability. The model's specificity is 0.87, indicating a high proportion of correctly identified benign (negative) samples. The sensitivity value is 0.91, indicating a high proportion of correctly identified malicious (positive) samples. In Scenario 2, the ROC AUC is 0.78, and the model's specificity and sensitivity are 0.69 and 0.85, respectively. These metrics demonstrate a moderate discrimination ability of the FOME model in this scenario. Similarly, in Scenario 3 and Scenario 4, the FOME model shows ROC AUC values of 0.85 and 0.83, respectively, with corresponding specificity and sensitivity

values for each scenario. The Table 5 provides valuable insights into the discriminatory power of the FOME model in distinguishing between benign and malicious network activities, further complementing the classification performance metrics presented in Table 4. The combination of these metrics allows for a comprehensive evaluation of the FOME model's effectiveness in attack classification across different scenarios in the study.

Table 6: Overall Risk Assessement FOME

Risk Category	Identified Risks	Impact Severity	Likelihood	Mitigation Strategy
Market Risk	Currency Exchange Rate Fluctuations	High	Moderate	Diversify currency holdings, use hedging instruments
Credit Risk	Default by Key Customers	High	Low	Implement rigorous credit checks, set credit limits
Liquidity Risk	Insufficient Cash Reserves	Moderate	Moderate	Establish a robust cash management strategy
Operational Risk	System Outages or Failures	High	Low	Regular system maintenance, backup systems in place
Regulatory Risk	Non-Compliance with New Regulations	Moderate	Moderate	Regularly update compliance protocols and training
Strategic Risk	Market Competition Impact	Moderate	High	Continuous market analysis, adapt business strategy

Table 6 presents the overall risk assessment derived from the Financial Optimization Membership Estimation (FOME) model, focusing on various risk categories, identified risks, their impact severity, likelihood, and corresponding mitigation strategies. In the market risk category, the identified risk of currency exchange rate fluctuations is deemed high in impact severity and moderate in likelihood. To address this, the recommended mitigation strategy involves diversifying currency holdings and utilizing hedging instruments. Similarly, in the credit risk category, the risk of default by key customers is identified as high in impact severity but low in likelihood. The proposed mitigation strategy includes the implementation of rigorous credit checks and setting credit limits. The liquidity risk of insufficient cash reserves is assessed as moderate in both impact severity and likelihood, prompting the recommendation to establish a robust cash management strategy. Operational risk, characterized by system outages or failures, is acknowledged as high in impact severity and low in likelihood, leading to mitigation through regular system maintenance and backup systems. Regulatory risk, involving non-compliance with new regulations, is considered moderate in both impact severity and likelihood, with the suggested strategy of regularly updating compliance protocols and training. Lastly, strategic risk related to market competition impact is evaluated as moderate in impact severity and high in likelihood, requiring continuous market analysis and adaptability in business strategy. This comprehensive overview in Table 6 aids in understanding the prioritization of risks and the corresponding measures to enhance the overall resilience of the financial landscape.

Table 7: Evaluation of Financial Health

Metric	Current Value	Benchmark/Target	Variance
Debt-to-Equity Ratio	0.6	< 0.8	Within target
Current Ratio	2.5	> 2.0	Within target
Profit Margin	15%	> 12%	Above target
Return on Investment	10%	> 8%	Above target

Table 8: Key Performance Indicators of Risk Assessment

KPI	Current Value	Benchmark/Target	Variance
Customer Satisfaction	92%	> 90%	Above target
Employee Turnover	8%	< 10%	Within target
Sales Growth	12%	> 8%	Above target

In Table 7 provides an insightful evaluation of the financial health of the entity, focusing on key metrics and their respective benchmarks/targets. The Debt-to-Equity Ratio is currently at a prudently low level of 0.6, well within the target of less than 0.8, indicating a healthy balance between debt and equity. The Current Ratio stands at a robust 2.5, surpassing the target of greater than 2.0, highlighting a strong ability to meet short-term obligations. The Profit Margin is commendably at 15%, exceeding the target of more than 12%, showcasing efficient cost management and profitability. Additionally, the Return on Investment is at a favorable 10%, surpassing the target of more than 8%, indicating effective utilization of invested capital. Table 8 focuses on key performance indicators (KPIs) related to risk assessment. Customer Satisfaction is notably high at 92%, surpassing the target of more than 90%, signifying a positive customer experience. Employee Turnover is a modest 8%, well within the target of less than 10%, indicating a stable and satisfied workforce. Sales Growth is robust at 12%, exceeding the target of more than 8%, indicating healthy business expansion. With both tables collectively present a positive picture of the entity's financial health and risk assessment. The entity demonstrates prudent financial management through favorable ratios, profitability, and efficient utilization of resources. Moreover, high customer satisfaction and effective employee retention contribute to the overall resilience and growth of the business, positioning it well in the competitive landscape. Continuous monitoring and adjustments based on these metrics and KPIs will contribute to sustained financial health and risk mitigation.

V. CONCLUSION

This paper proposed a efficient and novel approach with the Fuzzy financial risk Optimization Membership Estimation (FOME) model, for risk management in the Financial Riskenvironment, with a focus on cyberAssessment and threat detection. By applying FOME to the CICIDS dataset, successfully estimated membership values for various network activities and computed risk levels based on assigned Choquet's expectations. The results demonstrate that FOME offers a powerful and tailored solution for analyzing risk in complex network environments. The findings reveal that the FOME model provides accurate risk estimations, effectively distinguishing between normal and malicious network activities. The integration of fuzzy financial risk logic and optimization techniques allows for a more nuanced understanding of cyberAssessment risks, offering businesses an adaptive and comprehensive approach to safeguard their critical assets and sensitive data. Furthermore, the performance metrics presented in Tables 4 and 5 showcase the reliability and discriminative power of the FOME model. Its high accuracy, precision, recall, and F1 Score validate its effectiveness in classification tasks, while the ROC AUC values demonstrate its ability to differentiate between benign and malicious activities. Despite these promising results, it is important to acknowledge certain limitations. The effectiveness of FOME may depend on the quality and relevance of the chosen feature vectors and Choquet's expectations. Additionally, the model's performance might be influenced by the size and diversity of the dataset used for training and evaluation. In future explore how FOME can be applied in other domains and extended to handle more complex and diverse datasets. Investigating the model's robustness under various scenarios and its scalability to larger networks would also be beneficial. As it can be concluded that the proposed FOME model provides businesses with a powerful tool for risk management in the Financial Riskenvironment, enabling them to proactively address emerging cyberAssessment threats. By incorporating fuzzy financial risk logic and optimization techniques, FOME enhances risk estimation accuracy and offers a tailored and comprehensive approach to protect critical assets and maintain operational continuity in an ever-evolving digital landscape.

REFERENCES

[1] Colabianchi, S., Costantino, F., Di Gravio, G., Nonino, F., & Patriarca, R. (2021). Discussing resilience in the context of cyber physical systems. Computers & Industrial Engineering, 160, 107534.

[2] Bag, S., Telukdarie, A., Pretorius, J. C., & Gupta, S. (2021). Industry 4.0 and supply chain sustainability: framework and future research directions. Benchmarking: An International Journal, 28(5), 1410-1450.
[3] Fan, W., Song, J., Chen, L., & Shi, J. (2022). Intelligent performance evaluation of urban subway PPP project based on deep neural network model. Computational intelligence and neuroscience, 2022.
[4] Alswailem, O. A., Horanieh, B. K., AlAbbad, A., AlMuhaideb, S., AlMuhanna, A., AlQuaid, M., ... & AbuSalah, A. (2021). COVID-19 Intelligence-Driven Operational Response Platform: Experience of a Large Tertiary Multihospital System in the Middle East. Diagnostics, 11(12), 2283.
[5] Mohammed, Z. K., Zaidan, A. A., Aris, H. B., Alsattar, H. A., Qahtan, S., Deveci, M., & Delen, D. (2023). Bitcoin network-based anonymity and privacy model for metaverse implementation in Industry 5.0 using linear Diophantine fuzzy financial risk sets. Annals of Operations Research, 1-41.
[6] Kandaperumal, G. (2021). Resilience-Driven Situational Awareness and Decision Support for Cyber-Power Distribution Systems. Washington State University,1-24.
[7] Sonje, S. A., Pawar, R. S., & Shukla, S. (2021). Assessing blockchain-based innovation for the "Right to Education" using MCDA approach of value-focused thinking and fuzzy financial risk cognitive maps. IEEE Transactions on Engineering Management.
[8] Lin, J., Jianjun, Z., & Nanehkaran, Y. A. (2022). A study on bilateral matching of team-science talents in new R&D institutions based on grey correlation-cloud model. Journal of Intelligent & Fuzzy financial risk Systems, 43(1), 813-840.
[9] Alzahrani, F. A. (2021). Estimating Assessment Risk of Healthcare Web Applications: A Design Perspective. Computers, Materials & Continua, 67(1).
[10] Omidzadeh, D., Sajadi, S. M., & Bozorgi Amiri, A. Development the New Attributes of the Product Design Target Book Based on Sustainability Pillars-(a Hybrid Fuzzy financial risk Dematel and Fuzzy financial risk Anp Techniques). Available at SSRN 4224913.
[11] Ahmed, N. N., & Nanath, K. (2021). Exploring cyberAssessment ecosystem in the Middle East: towards an SME recommender system. Journal of Cyber Assessment and Mobility, 511-536.
[12] Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Adopting Assessment maturity model to the organizations' capability model. Egyptian Informatics Journal, 22(2), 193-199.
[13] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting insider threat via a cyber-Assessment culture framework. Journal of Computer Information Systems, 62(4), 706-716.
[14] Alzoubi, Y. I., Osmanaj, V. H., Jaradat, A., & Al-Ahmad, A. (2021). Fog computing Assessment and privacy for the Internet of Thing applications: State-of-the-art. Assessment and Privacy, 4(2), 145.
[15] Dai, D., & Boroomand, S. (2021). A review of artificial intelligence to enhance the Assessment of big data systems: state-of-art, methodologies, applications, and challenges. Archives of Computational Methods in Engineering, 1-19.
[16] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cyberAssessment: an overview, Assessment intelligence modeling and research directions. SN Computer Science, 2, 1-18.
[17] Jayalaxmi, P., Saha, R., Kumar, G., Kumar, N., & Kim, T. H. (2021). A taxonomy of Assessment issues in Industrial Internet-of-Things: scoping review for existing solutions, future implications, and research challenges. IEEE Access, 9, 25344-25359.
[18] Awaysheh, F. M., Aladwan, M. N., Alazab, M., Alawadi, S., Cabaleiro, J. C., & Pena, T. F. (2021). Assessment by design for big data frameworks over cloud computing. IEEE Transactions on Engineering Management, 69(6), 3676-3693.
[19] Kuamr, S., Yadav, R., Kaushik, P., Babu, S. B. G., Dubey, R. K., & Subramanian, M. (2022). Effective cyber Assessment using IoT to prevent E-threats and hacking during covid-19.
[20] Wichary, T., Mongay Batalla, J., Mavromoustakis, C. X., Żurek, J., & Mastorakis, G. (2022). Network slicing Assessment controls and assurance for verticals. Electronics, 11(2), 222.
[21] Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber Assessment: A review. Journal of King Saud University-Computer and Information Sciences, 34(8), 5766-5781.
[22] Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., ... & Alkhassawneh, H. M. (2022). A review on Assessment threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET Communications, 16(5), 421-432.
[23] Ali, A., Septyanto, A. W., Chaudhary, I., Al Hamadi, H., Alzoubi, H. M., & Khan, Z. F. (2022, February). Applied Artificial Intelligence as Event Horizon Of Cyber Assessment. In 2022 International Conference on Business Analytics for Technology and Assessment (ICBATS) (pp. 1-7). IEEE.
[24] Jangjou, M., & Sohrabi, M. K. (2022). A comprehensive survey on Assessment challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering, 29(6), 3587-3608.
[25] Haque, M. A., Shetty, S., Gold, K., & Krishnappa, B. (2021). Realizing cyber-physical systems resilience frameworks and Assessment practices. Assessment in Cyber-Physical Systems: Foundations and Applications, 1-37.