10.24425/acs.2025.157144

Archives of Control Sciences
Volume 35(LXXI), 2025
No. 4, *pages 713–728*

A hybrid cybersecurity model inspired by Chakravyuh formation using chaos theory and fuzzy logic

Kavita GUPTA

In this paper, a cybersecurity problem where the security team faces the challenge of preventing the hacker from breaching the multiple security layers is studied. The cybersecurity challenge mirrors the Chakravyuh, an ancient battlefield formation described in the Indian epic Mahabharata. The multi-layered complex structure of Chakravyuh, designed to trap the enemy, serves as an analogy for modelling the cybersecurity model of the digital economy. A hybrid model that integrates chaos theory and fuzzy logic is developed to enhance the defense mechanism in digitalization process. It is shown that the chaos theory approach can tackle the non-linear dynamics and unpredictable behavior of the hacker. On the other hand, fuzzy logic provides a more structured and adaptive defense mechanism. Monte Carlo simulations are used to analyze hacker's breaching probability across security layers. Further, the Binary search algorithm is applied to optimize security layers dynamically while maintaining computational efficiency. This study integrates ancient wisdom with modern computational techniques to effectively mitigate cybersecurity threats.

Key words: chaos theory, Monte Carlo simulation, cybersecurity, fuzzy approach, Chakravyuh

1. Introduction

The growing complexity of cyberattacks and the increased dependence on digital infrastructure necessitate the strengthening of cybersecurity defense mechanisms. This research draws inspiration from the Chakravyuh, which is a multi-layered complex battlefield formation as described in the great Indian epic Mahabharata. Chakravyuh is an advanced war strategy deployed by Kauravas against Pandavas during the 18-day- long war in Kurukshetra. This complex structure is nearly invincible even for a skilled warrior. Only Arjuna knew the strategy of penetrating this multi-layered complex structure, but in his absence, his son

K. Gupta (e-mail: gupta_kavita31@kmc.du.ac.in) is with Department of Mathematics, Kirori Mal College, University of Delhi, Delhi, India.

Received 14.08.2025.

Abhimanyu entered this Chakravyuh, but unfortunately, he could not come back safely. None of the existing literature addresses the inner details of this military formation or the skills involved in beating it. This paper is an attempt to create a bridge between ancient Indian text and mathematics together with resolving this mystery of beating Chakravyuh. This concept of Chakravyuh can be connected to the real-life problem of cybersecurity, where attackers and defenders engage in a dynamic system of penetration and defense. Motivated by the Chakravyuh analogy, this study provides a hybrid approach to develop a security system that prevents the attackers from penetrating into multiple security layers.

Chakravyuh is a complex spiral-like military arrangement of warriors that is strategically designed to trap the enemy in its intricate concentric layers. It is highly organized internally but appears as chaotic to opponents. The structure consists of seven layers of soldiers placed strategically at different positions in each of the layers depending on their defensive strength. Soldiers in the inner layer have higher defensive strength as compared to the soldiers in the outer layer. Higher defensive strength indicates a more skilled warrior, the use of sophisticated weapons, a huge army, the physical strength of the warrior, etc. Warriors are positioned in such a way as to maximize the damage caused to enemy warriors or to maximize the defensive strength to defend against the attacks from the highly skilled opponent. During the Mahabharata, the infantry was placed on the outer layers while armored chariots and elephant cavalry formed the inner layers of the Chakravyuh. The innermost layer was comprised of the strongest warriors with a relatively higher density than that of the outer layers. The commander-in-chief, *Dronacharya*, was positioned at the core of the Chakra. Each layer has a shrouded entrance that is densely protected by highly skilled soldiers and their troops. The soldiers of the outer layer conceal this entry of enemy warriors into the inner layer. If a layer breaks down, the soldiers at the outer layer conceal further entrances but do not assault the warriors who have already breached the layer. The whole arrangement has a well-defined mechanism of synchronous rotation about its axis. This Chakravyuh formation aligns with the modern cybersecurity challenge where the hacker attempts continuously to breach the multiple defensive layers to reach the core where important and sensitive data is kept. The security team is posed with the challenge of tightening the security at each layer to prevent the hacker from penetrating into the system. The objective of the hacker is to determine the minimum defensive strength of each layer, such that the hacker with a given initial strength finds it nearly impossible to breach.

Kumar [10] put emphasis on teaching Indian knowledge systems to our upcoming generations, through which they can seek the solutions to the contemporary challenges faced by human societies. Biswas et al. [2] have discussed that chaos theory finds its applications in social sciences, the stock market, the

human body, engineering, robotics, circuits, literature, etc. Bhalla and Suresh [1] connect the teachings of Vedic scriptures like Bhagavad Gita and Srimad Bhagawatam with the concept of relativity. Chakravyuh, a complex battle formation, has remained nearly invincible even for skilled warriors due to its infinite ways of rearrangement. Dutta [4] has shown that advancement in computer hardware and visualization systems enables scientists and modern mathematicians to decipher complex puzzles like Chakravyuh and unravel the inherent mystery of ancient wisdom.

Pieczywok [13] describes modern society as a risky society where cyberspace poses threats such as cyberbullying, cyber violence, cyber protests, cyber conflicts, etc. He suggested that this undesirable phenomenon can be tackled with the proper training of the staff in an organization. Klein and Zwilling [8] studied the increase in cyberattacks during the COVID-19 pandemic. They have shown that educating the employees about different defensive techniques can significantly reduce cybercrime. Khoroshko et al. [7] studied multi-criteria optimization problem of cybersecurity and information security, focusing on evaluating the authenticity of the decisions made. Digital transformation is the need of the hour for an organization to meet the competition level in today's digital economy [3]. This can be achieved through interactions between environmental uncertainty and resource orchestration. Kostelic [9] has integrated the technique for order of preference by similarity to the ideal solution with Saaty's criteria for evaluating employee cybersecurity risk across five criteria such as knowledge, risky behaviors, attitudes, compliance, and training. Evre and Ciylan [5] evaluated the effectiveness of cybersecurity strategies with a scorecard based on risk analysis. Strang [14] uses cognitive computing design and machine learning techniques to analyze employee behavior data from a multinational fintech company. Zanakis et al. [15] proposed several methods for solving multi-attribute decision-making problems. They compared the performance of eight methods, including ELECTRE, TOPSIS, MEW, SAW, and four versions of AHP, and analyzed the results using twelve different measures. They show that the methods' weights become stronger in problems with few alternatives, but the final rankings vary more in problems with many alternatives.

According to Zimmermann [16], fuzzy set theory has been widely applied in mathematical programming, allowing flexibility in constraints and fuzziness in objective functions. These models have been used to offer computationally efficient approaches for solving vector maximum problems, and this paper surveys major models and theories. Oliveira et al. [12] proposed that the complexity of resource discovery and selection is influenced by uncertainties in customer preferences due to growing Internet-connected resources. They use interval-valued fuzzy logic to model imprecision in classifying resources in IoT. Mahuve and

Tarime [11] proposed a fuzzy-based continuous travel impedance function which can measure spatial accessibility of service points and water points in a floating catchment area. Karnik and Mendel [6] developed the centroid and generalized centroid of a type-2 fuzzy set, both of which are essential for implementing a type-2 fuzzy logic system. It provides an exact computation procedure for interval type-2 sets and approximation for both.

Many researchers have used the fuzzy approach and chaos theory approach to deal with uncertainties, but no literature is available on relating the cybersecurity issue to the ancient Chakravyuh formation. The objective of this paper is to determine the minimum defensive strength of each security layer needed to prevent the hacker with a given initial strength from breaching the system. Existing literature does not address the chaotic and unpredictable behavior of hackers. The methodology developed in this study will assist the cybersecurity teams in developing the robust defense mechanism while considering the uncertainty in hackers' attempts. This paper bridges the gap between ancient wisdom and modern science by addressing cybersecurity issues using fuzzy and chaos theory, a novel approach that addresses uncertainties in ancient Chakravyuh formation.

2. Methodology

The proposed methodology integrates a chaos theory approach and a fuzzy approach to develop a robust cybersecurity defense mechanism.

2.1. Chaotic theory approach to Chakravyuh

The Chakravyuh, being a highly intricate and evolving battle formation, represents a dynamic system where chaos, unpredictability, and ordered structure coexist simultaneously. It can be explained as follows.

Structure of Chakravyuh: The complex structure of Chakravyuh is like systems in chaos theory, as one can observe fractal patterns and dynamic complexity in it. The concentric circular layers of the Chakravyuh show self-similarity and recursive designs, which give rise to fractal patterns. Dynamic complexity includes the continuous movement of soldiers within the Chakravyuh that creates an impression of chaos for the opponent but follows an underlying set of rules.

Emergence of chaos and order: The Chakravyuh appears chaotic and unpredictable to an opponent as its dynamic structure makes it hard to understand or penetrate through it. However, the soldiers follow the strict underlying set of patterns and rules within the formation, thereby creating an organized system of defense. This indicates how order occurs from chaos. Not only this, but this military formation also resulted in chaos from order. When Abhimanyu could

enter the Chakravyuh but could not exit out of it, it resulted in chaos and disorder, which illustrates sensitivity to initial conditions. Hence, order and chaos are interdependent.

Sensitivity of initial conditions: In chaos theory, we deal with the situations where small changes can lead to highly unpredictable outcomes. There are many entry points in Chakravyuh. Selection of the entry point is very critical. The wrong selection of an entry point can lead to destabilization of the whole military formation. So, these entry points act as initial conditions, and Abhimanyu's action inside layers is highly sensitive to these initial conditions.

Fractal nature of Chakravyuh: The design of Chakravyuh consists of concentric circles that are interconnected, resulting in a spiral-like structure. These self-similar patterns in seven layers of Chakra repeat at different scales. This ensures the fractal nature of Chakravyuh.

Feedback loops and dynamics of Chakravyuh: The position of soldiers' changes with respect to every move of Abhimanyu. This change in the position of warriors is unpredictable. Moreover, Abhimanyu's death resulted in the collapse of the whole dynamical system. This demonstrates the non-linear nature of complex systems.

2.2. Chaos theory approach in cybersecurity

The Chakravyuh problem can be applied in cybersecurity, where hackers act as Abhimanyu, and positions of warriors at different places in different layers of Chakravyuh play the role of defenders of cybersecurity. The hacker uses his skills to penetrate the dynamic system and break the firewalls to reach the innermost layer containing the important data.

Structure of cybersecurity: A network firewall is organized and structured with various layers of defense. Outer layers consist of general protection systems like antivirus software, anti-malware, anti-adware, intrusion detection systems, etc. Inner layers are hard to penetrate as they consist of encrypted databases, secure tunnels, multifactor authentication, etc. In this way, this multi-layered structure of cybersecurity resembles the intricate structure of Chakravyuh.

Emergence of chaos and order: The chaos and order co-exist as a cybersecurity problem. The hacker cracks the weak password and enters the outermost layer of security. His entry into the system leads to disturbance, and a state of chaos is generated as he progresses from one layer to another. The interaction between the hacker and security layers will eventually stabilize, with either success or failure of the hacker. Therefore, the chaos that has occurred will finally lead to order.

Sensitivity to initial conditions: The weak password, weak encryption, breaking the one-time password, etc., by the hacker can lead to catastrophic consequences. This makes the system highly sensitive to initial conditions. This can be mitigated by setting strong passwords, robust encryption, etc., leading to the minimization of chaos.

Feedback loops: Hacker's move into the dynamical system from one layer to another produces alarms, countermeasures, and adaptive learning by the defense systems. This resembles the introduction of feedback loops with each broken layer of safety. The network firewall uses these feedback loops to adapt dynamically by creating self-correcting systems. This allows the defensive security layers to adapt and counteract new attacks.

Fractal nature: The layers of defense in cybersecurity are fractals. The first layer blocks unauthorized access. The second layer monitors suspicious activity, the third layer might involve the anomaly detection, such as IP blocking and so on. These security layers have a common goal of providing friction to the hacker from penetrating into the core of the system where sensitive data is saved. These layers are self-similar structures giving rise to fractals.

Dynamics of cybersecurity system: The network firewall is a non-linear dynamical system. If the hacker is stopped at the first point by setting strong passwords, the large-scale important data available at the innermost layer is saved. But if the hacker can crack the various security walls and reach the core of the system, the security system can deploy non-linear responses such as locking the database and activating the backup system to protect the sensitive data. The security team can monitor the chaotic patterns in the attack behavior of the hacker and can dynamically adjust the security layers to neutralize the chaos.

2.3. Mathematical formulation of breaching the cybersecurity system

Let the cybersecurity system consist of n layers of security that a hacker will breach to reach the innermost core where the sensitive data is saved. Each layer has a probability of being breached depending upon the skills of the hacker or the tight security level set up in the cybersecurity system. For instance, the probability of cracking the weak password is higher than that of the strong password. Each layer has its own defensive strength that decreases with the hacker's success in entering the successive layers.

Notations

n – number of layers in the security system,

p_i – probability of penetrating the layer i, $i = 1, 2, 3, \ldots, n$,

d_i – defensive strength of layer i, $i = 1, 2, 3, \ldots, n$,

h_0 – initial strength of the hacker,

h_i – hacker's strength at any layer i, $i = 1, 2, 3, \ldots, n$.

Assumptions:

1. Higher value of p_i means weaker defense system, such as weak passwords, less effective antivirus software, etc.
2. As the hacker progresses from the outer layer towards the inner layer, his strength reduces proportionally to its effectiveness.
3. The hacker's success of reaching the core depends on his own strength, breaching probability, and feedback loops between the layers.
4. Feedback between different security layers depends on the hacker's residual strength and the security system's ability to adapt to the response generated with every move of the hacker.

Our objective is to simulate the hacker's progress and determine whether the hacker will be able to reach the innermost layer or not. Now, the mathematical formulation of the problem under consideration is as follows:

1. **Hacker's strength at layer $i + 1$:** The hacker loses its strength as he progresses from i-th layer to $(i+1)$-th layer. The loss in strength is proportional to $d_i(1 - p_i)$. Moreover, the system adapts itself with every move of the hacker which adds a feedback term $f(h_i, d_i, p_i)$ to his strength. Hence, a hacker's strength at $(i+1)$-th layer is given by:

$$h_{i+1} = h_i - d_i(1 - p_i) + f(h_i, d_i, p_i).$$

2. **Feedback function:** For simplicity, we model the feedback as a non-linear function given by:

$$f(h_i, d_i, p_i) = k h_i^2 - \alpha d_i$$

where k is the amplification constant for chaos and α is the scaling factor for security effectiveness.

3. **Stability condition:** The hacker is successful in reaching the core where important data is kept if $h_n > 0$ otherwise the system stabilizes, and the security system remains intact. Determine the minimum strength required by the hacker to breach the layers and access the sensitive data by applying the Monte Carlo Simulation technique described below.

Monte Carlo simulation

The technique of iterative simulation can be used to analyze the system's chaotic behavior as follows.

1. **Initialization:** Set the initial strength of the hacker h_0, breach probability of each layer p_i and defensive strength of each layer d_i. Initialize the feedback parameters k and α.
2. **Hacker's strength update:** Compute h_{i+1} iteratively for each layer using the equation

$$h_{i+1} = h_i - d_i(1 - p_i) + f(h_i, d_i, p_i) \quad \text{where} \quad f(h_i, d_i, p_i) = k h_i^2 - \alpha d_i \, .$$

3. **Sensitivity to the initial conditions:** Vary initial conditions h_0 or parameters (d_i, p_i, k, α) to observe changes in outcomes.
4. **Visualization of chaos:** Plot the hacker's strength h_i with layers $i = 1, 2, 3, \ldots, n$ to observe the non-linear dynamics and sensitivity.

3. Illustrating cybersecurity problem by chaos theory approach

Let the system consist of five layers with defensive strengths as 20, 30, 35, 50, and 60 and the probabilities of breaching different layers are 0.7, 0.6, 0.4, 0.3, 0.1 from the outermost layer to the innermost layer successively. Let the amplification constant be $k = 0.01$ and the scaling factor $\alpha = 0.5$. Vary the initial strength of the hacker with which he enters the system to determine up to which layer he can reach and whether he would be successful in reaching the innermost layer. Use the Monte Carlo simulation technique to estimate the minimum initial strength that a hacker must have to reach the core of the security system and access the sensitive data. Further, fix the minimum strength and simulate the defensive strength of each layer, which stops the hacker from reaching the core.

Solution:

Table 1 shows the resulting strength of the hacker after each layer if he enters the Chakravyuh (security system) with initial strength h_0 varying between 10 and 50. He would be able to reach till that layer where his strength is positive. The layer at which its strength becomes negative would result in failure at that layer. He would be successful in reaching the innermost core if he is able to breach all layers. It is clear from Table 1 that he requires an initial strength of 50 to access the sensitive data available at the core of the security system. Figure 1 shows how the hacker's strength evolves as he progresses through layers for each initial strength. Apply the Monte Carlo simulation technique on the computing software MATHEMATICA to estimate the minimum value of the initial strength required by the hacker to successfully breach all layers and reach the core to access the security system. Initial strength is varied randomly between 10 and 180, and the hacker's progress through the layers is simulated to check whether he breaches

all layers. Then we find the minimum value of h_0 that ensures success with 95% probability. Figure 2 displays the change in the probability of success with initial strength. It is found by the Monte Carlo simulation that the hacker should have a minimum strength of 50 to breach all layers. This value of minimum strength can be used by the security team to estimate the defensive strength of each layer, which makes the security system difficult to breach. Monte Carlo Simulation is used to simulate a hacker's progress when defensive strength ranges between 20 and 100. This gives us that the minimum defensive strength from the outermost layer to the innermost core should be 21,34,40,49, and 64. Table 2 shows the hacker's strength after each layer if his initial strength is fixed at 50 and the defensive strength of each layer is 21, 30, 40, 49, and 64. We observe that the hacker's strength at the innermost layer is negative, which means that he would not be able to reach the core. In this way, the security team can tighten the security of system, which is nearly impossible to breach.

Table 1: Results at different Initial Strength

Initial strength %	Hacker's strength at layers 1 to 5	Layers breached	Outcome
10	$\{-5, -31.75, -60.1694, -83.9658, -97.4632\}$	None	Fail
20	$\{8, -18.36, -53.4891, -84.8783, -96.8351\}$	Only outermost layer	Fail
30	$\{23, 1.29, -37.1934, -83.3599, -97.8712\}$	First and second layers	Fail
40	$\{40, 29, -1.09, -61.0781, -107.773\}$	First and second layers	Fail
50	$\{59, 66.81, 72.9458, 66.1566, 25.9236\}$	All layers	Pass

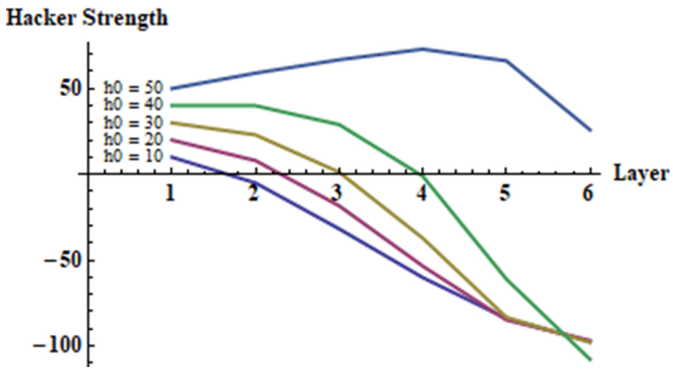

Figure 1: Hacker's strength at different layers

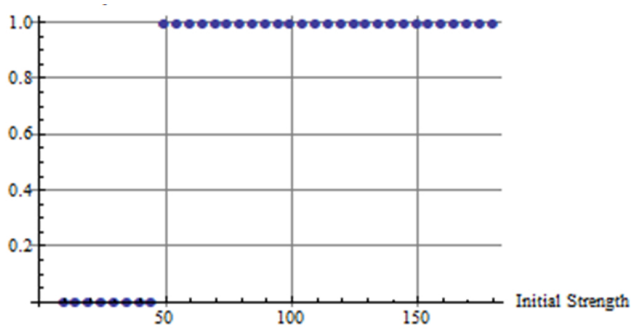

Figure 2: Monte Carlo estimation of minimum hacker strength

Table 2: Hacker's strength

Layer i	Defensive strength (d_i)	Breach probability (p_i)	Hacker's strength after layer i	Outcome
1	21	0.7	58.2	Pass
2	34	0.6	61.4724	Pass
3	40	0.4	55.261	Pass
4	49	0.3	26.9987	Pass
5	64	0.1	-55.312	Fail

4. Fuzzy approach to cybersecurity problem

The fuzzy approach can be used to deal with the uncertainty in a hacker's strength, the defensive strength of each layer, and breach probabilities. The fuzzy model so developed will adapt dynamically to different security conditions. This ensures that the cybersecurity strategies can be optimized, subject to the least possible defensive strength while maintaining security.

Membership function for hacker's strength (h_0)

Uncertainty in hacker's strength can be categorized as weak $(h_0 \leqslant 60)$, moderate $50 \leqslant h_0 \leqslant 120$; strong $(h_0 \geqslant 120)$. Weak hackers have full membership for $h_0 \leqslant 50$ and as their strength increases, membership declines linearly. Moderate hackers have membership in the middle range (50–120) whereas strong hackers

have a high initial strength with increasing membership.

$$\mu_{\text{weak}}(h_0) = \begin{cases} 1, & h_0 \leqslant 50, \\ \dfrac{60 - h_0}{10}, & 50 < h_0 \leqslant 60, \\ 0, & h_0 > 60; \end{cases}$$

$$\mu_{\text{mod}}(h_0) = \begin{cases} 0, & h_0 \leqslant 50 \text{ or } h_0 \geqslant 120, \\ \dfrac{h_0 - 50}{70}, & 50 < h_0 < 120; \end{cases}$$

$$\mu_{\text{strong}}(h_0) = \begin{cases} 0, & h_0 \leqslant 120, \\ \dfrac{h_0 - 120}{80}, & 120 < h_0 \leqslant 200, \\ 1, & h_0 > 200. \end{cases}$$

Membership function for defensive strength at each layer (d_i)

Membership functions used to effectively model uncertainty in defensive strength has been categorized into low ($d_i \leqslant 30$), medium ($30 \leqslant d_i \leqslant 70$); high ($d_i \geqslant 70$). Low category of defensive strength is strongest at $d_i \leqslant 30$ but declines by 50. Medium defense is active between 30 and 70. High defensive strength starts increasing at 70 and reaches its maximum at 100.

$$\mu_{\text{low}}(d_i) = \begin{cases} 1, & d_i \leqslant 30, \\ \dfrac{50 - d_i}{20}, & 30 < d_i \leqslant 50, \\ 0, & d_i > 50; \end{cases}$$

$$\mu_{\text{medium}}(d_i) = \begin{cases} 0, & d_i \leqslant 30 \text{ or } d_i \geqslant 70, \\ \dfrac{d_i - 30}{40}, & 30 < d_i \leqslant 70; \end{cases}$$

$$\mu_{\text{high}}(d_i) = \begin{cases} 0, & d_i \leqslant 70, \\ \dfrac{d_i - 70}{30}, & 70 < d_i \leqslant 100, \\ 1, & d_i > 100. \end{cases}$$

Membership function for breach probability (p_i)

Three categories for breach probabilities are low ($p_i \leqslant 0.4$), medium ($0.4 < p_i < 0.7$), high ($p_i \geqslant 0.7$). Low breach probability is highest when $p_i \leqslant 0.4$ and declines as p_i increases. Medium breach probability ranges between 0.4 and 0.7.

High breach probability rises above 0.7 and fully activates beyond 0.9.

$$\mu_{\text{low}}(p_i) = \begin{cases} 1, & p_i \leqslant 0.4, \\ \dfrac{0.7 - p_i}{0.3}, & 0.4 < p_i \leqslant 0.7, \\ 0, & p_i > 0.7; \end{cases}$$

$$\mu_{\text{medium}}(p_i) = \begin{cases} 0, & p_i \leqslant 0.4 \text{ or } p_i \geqslant 0.7, \\ \dfrac{p_i - 0.4}{0.3}, & 0.4 < p_i < 0.7; \end{cases}$$

$$\mu_{\text{high}}(p_i) = \begin{cases} 0, & p_i \leqslant 0.7, \\ \dfrac{p_i - 0.7}{0.2}, & 0.7 < p_i \leqslant 0.9, \\ 1, & p_i > 0.9. \end{cases}$$

Fuzzy rules:

1. If the initial strength of the hacker (h_0) is weak and defensive strength (d_i) is high then breach probability (p_i) is very low.
2. For moderate hacker strength and medium defensive strength, the breach probability is medium.
3. Strong hacker's strength and low defensive strength results in higher breach probability.
4. Moderate (h_0) and high (d_i) gives low breach probability.
5. If defensive strength is greater than 70, set breach probability to 0.01. This is the safe condition.
6. Otherwise, use a smooth function to reduce breach probability based on defensive strength.

The above fuzzy rules are framed to ensure smooth reduction in breach probability so that the search does not overshoot to 100. This means that as defensive strength increases, the breach probability decreases gradually rather than making abrupt changes.

Iterative defensive strength adjustment:

In cybersecurity, the defensive measures are continuously evaluated and improved to effectively counterattack the evolving threats. This makes the cybersecurity system dynamic. This necessitates continuous assessment and improvement in security protocols. In the problem under study, the defensive strength is adjusted using a binary search algorithm. This algorithm determines the optimal defensive strength, which keeps the breach probability below a specified threshold (0.01).

Binary search algorithm:

1. Set the lower bound of defensive strength to 20 and the upper bound to 100.
2. Calculate the midpoint of the lower and upper bounds.
3. Compute the breach probability using the fuzzy rules with the current mid value for defensive strength.
4. If $p_i < 0.01$, adjust the upper bound to the mid value but if $p_i \geqslant 0.01$, adjust the lower bound to mid value.
5. Continue the above process until the difference between upper and lower bounds is minimal, ensuring convergence to the optimal defensive strength.

Defuzzification:

The fuzzy breach probabilities for all security layers are converted into a single crisp value by using the centroid method defined below

$$p_{\text{final}} = \frac{\sum_i \mu_i p_i}{\sum_i \mu_i}.$$

Centroid method is the most common technique of defuzzification. The weighted sum of all fuzzy membership values μ_i and their corresponding breach probabilities p_i represents that breach probability with higher membership values contribute more to the final value. Dividing the weighted sum by the sum of all memberships ensures that the result remains within a valid range. This justifies the choice of centroid method for defuzzification.

Algorithm to solve cybersecurity problem by using Fuzzy approach:

1. Defining the membership functions for hacker's strength, defensive strength of security layers and breach probabilities.
2. Designing the fuzzy rules that reduce breach probability when defensive strength is higher.
3. Adjusting the defensive strength iteratively by using fuzzy rules until the overall breach probability is less than 0.01.
4. Use centroid method of defuzzification to find the actual breach probability.
5. Computing software MATHEMATICA is used for applying the fuzzy approach to determine the minimum defensive strength of each security layer to ensure that breach probability is less than 1%.

On applying the above algorithm of Fuzzy model on Mathematica to cybersecurity problem under consideration, it is found that optimal defensive strength of each layer is 70.

5. Results and analysis

The cybersecurity problem is studied with two different approaches: The chaos theory and the fuzzy approach.

5.1. Chaos theory simulations

Monte Carlo simulations in the chaos theory approach revealed that if the hacker with initial strength 50 enters the system, then the estimated defensive strength of security layers should be 21, 34, 40, 49, and 64 to prevent him from reaching the core of the system.

5.2. Fuzzy approach simulations

Fuzzy approach provides an estimated defensive strength of 70 for each security layer to ensure that the breach probability remains below 0.1% if the hacker enters the system with initial strength 50.

6. Conclusions

In this paper, a cybersecurity problem is modelled as a Chakravyuh, where a hacker attempts to breach the security layers, much like a warrior as Abhimanyu in the Mahabharata. He is trying to penetrate the concentric rings where warriors of different defensive strengths are positioned at different places. The goal is to reach the innermost core of the system where sensitive data is kept. Our objective is to determine the minimum defensive strength of each layer that prevents the hacker with a given initial strength to reach the core. A hybrid approach consisting of chaos theory and a fuzzy approach is used to optimize the cybersecurity defenses. The two approaches cater to different aspects of the problem. The chaos theory approach deals with the unpredictability of hacking attempts and is highly sensitive to initial conditions. The chaos theory approach analyzes the non-linear dynamics of cybersecurity attacks and requires extensive use of simulation techniques such as Monte Carlo simulation. On the other hand, the fuzzy approach is practical for the real-world scenarios in cybersecurity since it accounts for uncertainty and dynamically adjusts defenses. The fuzzy approach is probabilistic and provides optimal defensive strength using structured and adaptive mechanism without requiring extensive simulations. Hence, we can say that the hybrid approach developed in this paper is useful for solving cybersecurity

issues. Chaos theory models the unpredictable nature of cyberattacks while fuzzy logic ensures a robust defense mechanism that continuously evolves against potential threats. As future work is intended, machine learning algorithms such as decision trees, random forest, reinforcement learning can be incorporated with the fuzzy model to predict hacking patterns and adjust security mechanisms dynamically. Real-world testing can be done by implementing the developed model in a real cybersecurity environment to compare the practical performance against actual cyber threats.

References

[1] S. Bhalla and R. Suresh: Concept of Relativity in Light of Vedic Scriptures. *Science and Spiritual Quest*, (2010), 55–59.

[2] H.R. Biswas, M.M. Hasan and S.K. Bala: Chaos theory and its applications in our real life. *Barishal University Journal. Part 1*, **5**(1-2), (2018), 123–140.

[3] H. Chen and Z. Tian: Environmental uncertainty, resource orchestration and digital transformation: A fuzzy-set QCA approach. *Journal of Business Research*, **139**, (2022), 184–193, DOI: 10.1016/j.jbusres.2021.09.048

[4] K. Dutta: Dynamics of an invincible troop formation in ancient open battlefields. *Interdisciplinary Description of Complex Systems*, **19**(1), (2021), 146–159, DOI: 10.7906/indecs.19.1.12

[5] O.G. Evre and B. Ciylan: Measurement of the cybersecurity strategy effectiveness with a scorecard based on risk analysis. *Gazi University Journal of Science Part C: Design and Technology*, **11**(4), (2023), 1116–1130, DOI: 10.29109/gujsc.1345984

[6] N.N. Karnik and J.M. Mendel: Centroid of a type-2 fuzzy set. *Information Sciences*, **132**(1-4), (2001), 195–220, DOI: 10.1016/S0020-0255(01)00069-X

[7] V. Khoroshko, M. Brailovskyi and M. Kapustian: Multi-criteria assessment of the correctness of decision-making in information security tasks. *Computer Systems and Information Technologies*, **4** (2023), 81–86, DOI: 10.31891/csit-2023-4-11

[8] G. Klein and M. Zwilling: The weakest link: Employee cyber-defense behaviors while working from home. *Journal of Computer Information Systems*, **64**(3), (2023), 408–422, DOI: 10.1080/08874417.2023.2221200

[9] K. Kostelic: TOPSIS-based framework for evaluating employee cybersecurity risk. *Croatian Operational Research Review*, **16**(1), (2025), 31–44, DOI: 10.17535/crorr.2025.0003

[10] M.J. Kumar: Forging connections: Integrating Indian knowledge systems in higher education. *IETE Technical Review*, **41**(3), (2024), 271–273, DOI: 10.1080/02564602.2024.2342625

[11] F.E. Mahuve and B.C. Tarimo: Integrating fuzzy set function into floating catchment area measures: A determination of spatial accessibility of service points. *Annals of GIS*, **28**(3), (2022), 307–323, DOI: 10.1080/19475683.2022.2026477

[12] L. Oliveira, A. Argou, R. Dilli, A. Yamin, R. Reiser and B. Bedregal: Exploring fuzzy set consensus analysis in IoT resource ranking. *Engineering Applications of Artificial Intelligence*, **109**, (2022), 104617, DOI: 10.1016/j.engappai.2021.104617

[13] A. Pieczywok: Training employees on risks in the area of cybersecurity. *Cybersecurity and Law*, **7**(1), (2022), 261–271, DOI: 10.35467/cal/151832

[14] K.D. Strang: Cybercrime risk found in employee behavior big data using semisupervised machine learning with personality theories. *Big Data and Cognitive Computing*, **8**(4), (2024), DOI: 10.3390/bdcc8040037

[15] S.H. Zanakis, A. Solomon, N. Wishart and S. Dublish: Multi-attribute decision making: A simulation comparison of select methods. *European Journal of Operational Research*, **107**(3), (1998), 507–529, DOI: 10.1016/S0377-2217(97)00147-1

[16] H.J. Zimmermann: Applications of fuzzy set theory to mathematical programming. *Information Sciences*, **36**(1-2), (1985), 29–58, DOI: 10.1016/0020-0255(85)90025-8