A Fuzzy Logic and Deep Learning for a Knowledge-Driven Modeling-Based Recommendation System

Najma Imtiaz Ali * , Imtiaz Ali Brohi , AllahRakhio Junejo , Allah Bachayo Brohi

Posted Date: 21 February 2025

doi: 10.20944/preprints202502.1674.v1

Keywords: Fuzzy logic (FL); hybrid fuzzy detection (HFD) deep learning (DL); recommendation system model

Article

A Fuzzy Logic and Deep Learning for a Knowledge-Driven Modeling-Based Recommendation System

Najma Imtiaz Ali [1,*], Imtiaz Ali Brohi [2], AllahRakhio Junejo [3] and Allah Bachayo [2]

[1] Institute of Mathematics and Computer Science, University of Sindh
[2] Department of Computer Science, GC University Hyderabad
[3] Department of Information Technology, GC University Hyderabad
* Correspondence: najma.channa@usindh.edu.pk

Abstract: The fuzzy- logic (FL) based recommendation system is a research subject that studies and develops technological systems capable of solving complex tasks typically requiring human intelligence, as well as creating intelligent recommendation systems. Fuzzy logic (FL) and deep learning (DL) are techniques for handling variables that allow multiple values to be processed through the same variable. To resolve issues with an open, inexact spectrum of information that makes it feasible to obtain an array of specific. Our proposed model is a FL based recommendation system, characterized by a hybrid fuzzy detection (HFD) and loss computation model. Furthermore, the FL based model is developed using DL, along with a FL algorithm designed for detecting and preventing attacks. Configuration techniques results such as positive and negative attacks, which are attributed to the type of attack or normal behavior. The frequency results are attributed to the type of attack or normal behavior. Evolution analysis refers to the description and modeling of regularities or trends for objects whose count changes over time. The distribution includes a positive peak of 77 and a negative peak of over 100 categories, forming the foundation of the FL based recommendation system. In engineering finding the proposed FL and DL recommendation system has the potential to provide valuable support and help users achieve their financial goals.

Keywords: Fuzzy logic (FL); hybrid fuzzy detection (HFD) deep learning (DL); recommendation system model

1. Introduction

Many researchers believe that Fuzzy logic (FL) based intelligent systems provide effective solutions to real-world problems. Enhancing the capabilities of FL-based recommendation systems and evolutionary computation is a research area focused on developing technological systems that solve complex tasks in ways that would typically require human intelligence.

The FL based recommendation system is a research area that focuses on developing technological systems to solve complex tasks using methods that would traditionally require human intelligence and create smart recommendation systems. The FL-based recommendation system is used for aid of a self-propagating growth of era that acquiring new functionality from the virtual enterprise and information and acquiring new functionality from the virtual enterprise and information and conversation era. In this area of FL based recommendation system, DL has advanced high-quality progress over the last decades.

The FL based recommendation systems and evolutionary computation and technique for variable dealing out that permits for more than one value to be processed via the identical variable. In this paper we are using FL-based recommendation systems that perform specialized functions that humans perform through their power of reasoning and decision-making. The FL also helps

 doi:10.20944/preprints202502.1674.v1

technology to self-propagate its growth, moving on to acquire new functionalities from the digital enterprise, information, and communication technology Jiang [1], Biswas [2].

FL is a method of handling variables that allows for multiple values for the same variable. It aims to solve problems using open, imprecise spectra of information that facilitate the realization of a range of specific outcomes. Developing solutions to FL problems often requires an examination of human techniques and consideration of how to scale these solutions to have a comprehensive impact on society Singh [3]. FL and DL-based recommendation systems are valuable for dealing with uncertainty and imprecision, making them suitable for complex tasks that require human-like reasoning. When combined with DL, these systems effectively process and interpret ambiguous data. DL techniques, such as neural networks, benefit from FL by incorporating fuzzy inputs and outputs, enhancing the model's ability to generalize from imprecise data. It's important to develop criteria to evaluate the effectiveness of your FL based recommendation system compared to traditional methods, using metrics like precision, recall, and user satisfaction Fang [4], Jameson [5].

The present development overcomes the problems related. FL and DL for a knowledge-driven modeling-based recommendation system. And reputation device with the use of a FL based recommendation system by using DL. The HFD and loss computation proposed model recovers neighborhood's descriptors.

- Our proposed model is a FL based recommendation system, characterized by a hybrid fuzzy detection (HFD) and loss computation model.
- Furthermore, the FL based model is developed using DL, along with a FL algorithm designed for detecting and preventing attacks. Configuration techniques results such as positive and negative attacks, which are attributed to the type of attack or normal behavior. The frequency results are attributed to the type of attack or normal behavior.
- Evolution analysis refers to the description and modeling of regularities or trends for objects whose count changes over time. The distribution includes a positive peak of 77 and a negative peak of over 100 categories, forming the foundation of the FL based recommendation system. In engineering finding the proposed FL and DL recommendation system has the potential to provide valuable support and help users achieve their financial goals.

2. Experimental Designs

2.1. The FL-Based Recommendation System

The FL-based recommendation system combines factor of studying, variation, the progression that are all intently linked to system learning-to allow one to create, in a few experiences intelligent packages as shown in Figure 1**.**

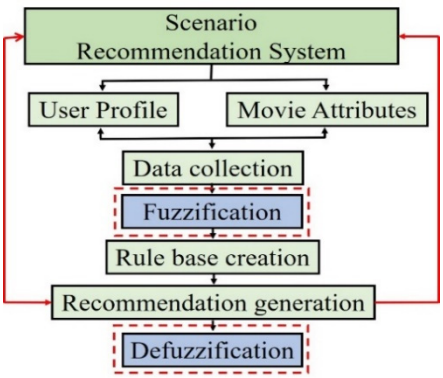

Figure 1. The HFD and loss computation model.

 doi:10.20944/preprints202502.1674.v1

2.2. FL-Based Recommendation System

The Data Collection: collect user data (preferences, behaviors, demographics) and item data (attributes, ratings). Fuzzification: Convert crisp user preferences and item attributes into fuzzy sets. Rule Base Creation: Develop a comprehensive set of fuzzy rules based on domain knowledge and data analysis. For instance, if a user rates action movies highly, rules is adjusted to recommend similar genres. Recommendation Generation: Use the Fuzzy Inference System (FIS) to generate recommendations by matching fuzzy user profiles with fuzzy item descriptions. Defuzzification: Convert the FL output back into a ranked list of recommendations for the user.

2.3. Using Deep Learning

The recommendation system model by using DL as characteristic set that is extract and selects from a given fact set use strategies including records mining as shown in Figure 2.

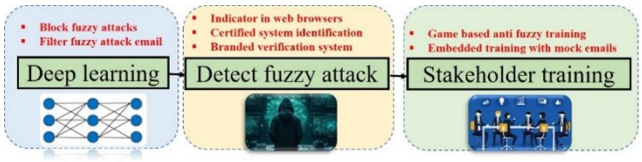

Figure 2. FL-based recommendation system by using DL.

The model combines FL-based recommendation system with DL. To effectively combat fuzzy attacks, three components must be in place: DL, detection of fuzzy attacks, and stakeholder training, as shown in Figure 2. The FL based recommendation system has far surpassing classifier skills and is in wide use in many fields related to scientific studies. This is because it is easy, and its implementation is straightforward. the data showing its main characteristics, making a count of the numerical data and each column's type of data as shown in Table 1. Furthermore, selected the two main attributes, the most valued in the selection ranking, and visualized [6].

Table 3. The number of the fuzzy attacks.

Total Attacks	Positive Attacks	Negative
10000	50000	10000
5000	1000	2000
2500	500	250
1500	200	100
2000	1000	800
250	50	500
300	20	300
350	10	200
400	55	10
450	58	50
500	250	220

The HFD and loss computation model proposed by [6,7] which state the use of three modules as risk analysis, loss estimation and risk mitigation. FL-based recommendation system combines factors of studying, variation, the progression that are all intently linked to system DL and computational intelligence.

Train employees to recognize scams is help them to stop the attacks in case neither of the preventing measures such as firewall and Intrusion Prevention Systems (IPS) could not detect and stop the attack. The FL- based recommendation system has far surpassing classifier skills and is in wide use in many fields related to scientific studies. This is because it is easy, and its implementation is straightforward. the data showing its main characteristics, making a count of the numerical data

 doi:10.20944/preprints202502.1674.v1

and each column's type of data. Use two-step verification. The attacker surely not know the organization is using two-factor authentication, in case the employee has been finished, if doesn't receive the PIN or code that confirm the change of his credentials, it's known that victim of fuzzy and report it to the appropriate department for corrective actions. Have regular security evaluation checks. Many fuzzy emails carry malware, reliable anti-virus software detect and remove all those malwares or any backdoor. A Demilitarized Zone (DMZ) network which host servers that are not only accessed for the internal network but also from the internet. Apart from that, the IPS/IDS is installed on the firewall and the internal router; the internal network has other server that are exclusively used on the intranet for internal use [8].

2.2. Algorithm for the Fuzzy Attacks

The given equation is *(log_2(x) = 3)*. This means we are looking for a number *(x)* such that when 2 is raised to the power of *3*, the result is *(x)*.

To find *(x)*, rewrite the logarithmic equation in its exponential form. The general form of a logarithmic equation *(log_b(a) = c)* rewritten as *(a = b^c)*.

So, *(log_2(x) = 3)* can be rewritten as:

[x = 2^3]

Now calculate *(2^3)*:

[2^3 = 2 times 2 times 2 = 8]

[x = 8]

Logarithmic and exponential Relationship

The logarithm of a number is the exponent to which the base must be raised to produce that number. In the equation *(log_2(x) = 3)*, *2* is the base, *(x)* is the number, and *3* is the exponent. By converting the logarithmic form to the exponential form (x = 2^3), calculate the value of *(x)*.

[1] Solve the logarithmic equation *(log_5(x) = 2)*.

[2] Convert the exponential equation *(10^4 = x)* to its logarithmic form.

[3] Find the value of *(x)* in the equation *(log_{10}(x) = -1)*.

The equation *(log_2(x) = 3)* tells us that *(x)* is the number such that when *2* (the base of the logarithm) is raised to the power of *3*, it equals *(x)*. In other words, *(2^3 = x)*.

- $\mathbb{Q}$: the set of rational numbers
- $\mathbb{Z}$: the rational integers
- θ: a real algebraic integer of degree $n \geq 2$
- $K \coloneqq \mathbb{Q}(\theta)$
- $M(n, \mathbb{Z})$: The *n-th* integer square matrices
- $GL(n, \mathbb{Z})$: the *n-th* unimodular square matrix group
- $a_{ij}, b_{ij}\alpha_i, \beta_i$ Express respectively Energy consumption of storage, computation, communication and VMs resources.
- det (M): The determinant of a matrix M.
- $\sigma_i (i = 1, .., n)$: isomorphisms which transfer θ to another conjugate of θ, where σ_1 is the identify map
- $\beta_i * \beta_j \coloneqq \sum_{k=2}^{n} b_{ik} b_{jk}$
- $\{\alpha_i\}$:a column vector of K, where $i = 1, \dots, n$ and $\alpha_1 = 1$
- $\{\alpha_i\}_\sigma$: the n-square matrix which (i, j) elements is $\sigma_j(\alpha_i)$
- $\{a_{ij}\}$: the n square matrix of which (i, j) element equals to a_{ij} where $i, j = 1, \dots, n$
- $\{b_{ij}\}'$:the $n - 1$ square matrix of which (i, j) element equals to b_{ij} where $i, j = 2, \dots, n$
- $||\chi|| = \prod_{i=1}^{n} \sigma_i(\chi)$ for $\chi \in K$
- $D \coloneqq \{\theta^{(i-1)}\}_\sigma$
- $\mathbb{Q}$: the set of rational numbers
- $\mathbb{Z}$: the rational integers
- θ: a real algebraic integer of degree $n \geq 2$
- $K \coloneqq \mathbb{Q}(\theta)$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2025 doi:10.20944/preprints202502.1674.v1

- $M(n,\mathbb{Z})$: The n-th integer square matrices
- $GL(n,\mathbb{Z})$: the n-th unimodular square matrix group
- $a_{ij}, b_{ij}\alpha_i, \beta_i$ Express respectively Energy consumption of storage, computation, communication and VMs resources.
- det (M): The determinant of a matrix M.
- $\sigma_i(i = 1,..,n)$: isomorphisms which transfer θ to another conjugate of θ, where σ_1 is the identify map
- $\beta_i * \beta_j \coloneqq \sum_{k=2}^{n} b_{ik} b_{jk}$
- $\{\alpha_i\}$:a column vector of K, where $i = 1, \dots, n$ and $\alpha_1 = 1$
- $\{\alpha_i\}_\sigma$: the n-square matrix which (i,j) elements is $\sigma_j(\alpha_i)$
- $\{a_{ij}\}$: the n square matrix of which (i,j) element equals to a_{ij} where $i,j = 1, \dots, n$
- $\{b_{ij}\}'$:the $n-1$ square matrix of which (i,j) element equals to b_{ij} where $i,j = 2, \dots, n$
- $||\chi|| = \prod_{i=1}^{n} \sigma_i(\chi)$ for $\chi \in K$
- $D \coloneqq \{\theta^{(i-1)}\}_\sigma$

3. Model Design

The fuzzy attacks based on model for an organization to protect itself effectively from fuzzy attacks as shown in Figure 3.

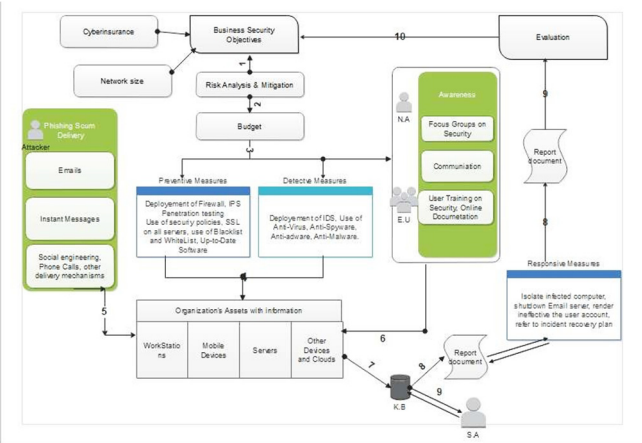

Figure 3. Preventive and detective model for fuzzy attacks.

3.1. Fuzzy Attacks Steps

Train employees to recognize scams: This is helping tostop the attacks in case neither of the preventing measures such as firewall and IPS could not detect and stop the attack.

Use two-step verification: The attacker is surely not knowing the organization is using two-factor authentication, in case the employee has been phished, if doesn't receive the PIN or code that confirm the change of his credentials, he/she will know that she/he is victim of Fuzzy and report it to the appropriate department for corrective actions Ranjan [9].

Have regular security evaluation checks: Performing security evaluation regularly helps the organization to discover the security holes but also to assess the attacks that hit the organization and see what could be done to prevent the occurrence of similar attacks.

Continually update software: Some fuzzy attack, such as malware attacks exploit vulnerabilities or install backdoors on the systems, update of software is the effective remediation against these attacks.

Secure the application browsers: Updated browsers are using SSL/TLS that provide a layer of security from the previous version of browsers and limit the abilities of casual hackers to impersonate the trusted web site.

 doi:10.20944/preprints202502.1674.v1

Use different password: The use of one password is too dangerous in case a hacker gets a hand on it, he has access to all the systems accessed using the password. Some software such as LastPass, help in the management of passwords and users can be advised to use them.

Hold mock drills for Fuzzy attacks: The security team can use mock emails to test the ability of employees to recognize fuzzy emails. It also helps in determine the state of security software such anti-virus and firewall on end-hosts.

Install reliable anti-virus software: Many Fuzzy emails carry malware; reliable anti-virus software will detect and remove all those malwares or any backdoor. Users should be taught on how to active and update them regularly.

Never click on link in emails: Most of Fuzzy emails contain links to fake web sites. User should be train on this issue and should avoid clicking on this link. Instead, they can open another window and access the intended site from there.

Report Fuzzy attacks: The organization should have a mean for reporting Fuzzy attacks in the organization Biswas [10].

Fuzzy Scum Delivery: This shows the different means used by attackers to deliver the payload to their victims. This includes email, instant messages on social media such as Facebook, WhatsApp, LinkedIn, Instagram etc. and even SMS or phone calls when the hacker want to increase the level of confidence of the victim. Social engineering is also used to convince the user to do want the hacker want.

Organization's assets with information or has access to information: These are all the devices that have access to information kept by the organization. They include workstations, mobile devices owned by the organization or by individual employees and servers that store that information.

Business Security Objectives (BSO): These are objectives set by the organization even before any security measures are applied in the company. Each organization must have objectives so that it can budget how much it is willing to spend on the security aspect of its information. This process involves also knowing the exact size of the network, if possible, also to apply to a cyber-insurance company and most importantly to perform the risk analysis to know well the vulnerabilities so that they can know what security measures to put in place.

Preventives measures (PM): The organization should put in place measures to prevent Fuzzy link to reach users; if the payload doesn't reach its destination, there is 80% of chance for the user to not open it and read it which will prevent the attack from occurring. Organizations can accomplish this by deploying on their network well configured firewalls, intrusion prevention system, email filtering using whitelist for allowed addresses and blacklist for blocking addresses that are already recognized as vector for Fuzzy, the use SSL on their critical server systems, the use of security policies, penetration testing and auditing, use of preventive algorithm that have been developed and prove themselves on the market. These measures can be extended according to the capability of the organization.

Detective measures (DM): Organizations should also put in place detective measures to detect earlier the scum that might successes to lure the preventive measures. A detected Fuzzy scum can reduce by 90% the chance of a fuzzy attack to take place. The detective measures that can be put in place are but not limited to Intrusion Detection Systems both Network-based and Host-based, anti-virus software, anti-spyware software and other anti-malware software, detective algorithm that have been developed and prove themselves on the market.

Awareness Measures (AM): The biggest weakness to security is users. Preventives and Detectives measures are effective enough only if end-users can also do their part; and the only way they can do it is if they are aware of what they are supposed to do. This is done through communication, user training, security campaign, focus group on security and many more. Network Administrators and security officers should tell the users how important security of information is and that they are responsible for it. They should train them on how to verify basic security utilities on their personal host such firewalls, HIDS and IPS and ant-malwares, so that they know if they are running before

 doi:10.20944/preprints202502.1674.v1

they can connect to the internet or open their email. Security campaign and focus groups on security should also be organized to refresh the awareness of users about security.

Responsive measures (RM): In case the user is unable to detect a Fuzzy email, and the hacker get her/ his credentials, or the virus get spread on the network, responsive measures should be put in place to contain the propagation of the virus or to prevent the hacker to use the credential he/she has stolen. This can be done by defining clearly the responsibilities of individuals in the Business Continuity Plan in case such incident occurs, it is isolating the infected computer from others on the network, shutting down the mail server if the fuzzy email were numerous, and other measures. In case of stolen credential, the user should communicate with the system administrator who should change the user's credentials immediately or render ineffective the user's account.

Report Document: After the responsive measures have been applied and the attack contained and resolved, the attack and all the processes and measures took to resolved it must be documented and kept in the knowledge base of the organization. A copy of the report can be sent to security practitioners who are responsible for the development of security tools.

Knowledge Base (KB)L: This is the database that keeps all the virus, malware, or any attack that the organization is aware of and have been subject to. It is populated by the organizations' experiences on security but also by other organization and security practitioners.

Evaluation: Evaluation is done after a security attack have been resolved. It is also done periodically to make sure that the security mechanisms used by the organization are effective. If they are not effective or when new update from security practitioners have been released, the organization has to apply them.

Security Authority (SA): These are security practitioners who develop security tools. Add data to the organization's knowledge base and the organization can also supply them with new that when are faced with a new attack. To solve for (x), we convert the logarithmic equation to its exponential form. The general logarithmic form (log_b(a) = c) can be rewritten as (a = b^c).

Table 2. Provides the detailed information for each data entry.

Fuzzy state	Fuzzy system	Installment	Log Annual Inc	DTI	FICO	Days with Line	Revolving	Revolving Utilization
Fuzzy sulfidation	0.1189	829.1	11.3504	19.48	737	5639.958	28854	52.1
Fuzz card	0.1071	228.22	11.0821	14.29	707	2760	33623	76.7
Fuzzy consolidation	0.1357	366.86	10.3735	11.63	682	4710	3511	25.6
Fuzzy consolidation	0.1008	162.34	11.3504	8.1	712	2699.958	33667	73.2
Fuzzy_ditcard	0.1426	102.92	11.2997	14.97	667	4066	4740	39.5

3.2. Conversion Leverages the Definition of Logarithms

[log_b(a) = c if a = b^c]
So, for (log_2(x) = 3):
[x = 2^3]
Next, we calculate (2^3):

 doi:10.20944/preprints202502.1674.v1

[2^3 = 2 times 2 times 2 = 8]
Thus, (x = 8).
[x = 8]

Logarithmic and Exponential Relationship

The logarithm of a number answers the question: To what power must the base be raised, to produce this numbers. The equation (log_2(x) = 3) means that we need to raise the base 2 to the power 3 to get (x).

The exponential form (x = 2^3) is derived from this definition:

- Base (b) = 2
- Exponent (c) = 3
- Result (a) = (x)

By converting from logarithmic to exponential form, we use the property that the logarithm base (b) of (a) is the power (c) to which (b) must be raised to equal (a).

Solve the logarithmic equation (log_5(x) = 2).**

- Convert to exponential form: (x = 5^2)
  - Calculate: (5^2 = 25)
  - Final answer: (x = 25)

Convert the exponential equation (10^4 = x) to its logarithmic form.**

- Using the definition: (log_{10}(x) = 4)
- Final answer: (log_{10}(x) = 4)

Find the value of (x) in the equation (log_{10}(x) = -1).**

- Convert to exponential form: (x = 10^{-1})
- Calculate: (10^{-1} = 0.1)
- Final answer: (x = 0.1)

The Table 3 provides the detailed information for each data entry, covering aspects like credit policy, interest rate, instalment amount, annual income, debt-to-income ratio, FICO score, days with detect fuzzy and stakeholder training in the delinquencies and public records, and whether the loan was not fully paid Ding [11].

4. Results

The attacker does not know the organization is using two-factor authentication, in case the user has been phished, if receive the PIN or code that confirm the change of his credentials, user know that is victim of Fuzzy and report it to the appropriate department for corrective actions. The FL based recommendation system model by using DL have regular security evaluation checks. Many fuzzy emails carry malware, reliable anti-virus software detect and remove all those malwares or any backdoor. The only parameter set to the model was which indicates the minimum number of samples required to split an internal tree node, which we gave the value of 100. As shown in the Jupiter Notebook, after loading the KDD99 dataset complete with Pandas, we proceeded to indicate the name of the 31 columns (attributes) relevant to our predictive model of the (DL) Kim [12], Li [13].

We have also made several changes to the CNN 99% data set based on the initial version of the code. in case the employee has been phished, if he/she doesn't receive the PIN or code that confirm the change of his credentials, he/she will know that she/he is victim of Fuzzy and report it to the appropriate department for corrective actions. Detect fuzzy and Stakeholder training. The fuzzy based recommendation system model by using DL have regular security evaluation checks. In Figure 4, he designed system test and performance evaluation formula Mei [14], Kim [15].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2025 doi:10.20944/preprints202502.1674.v1

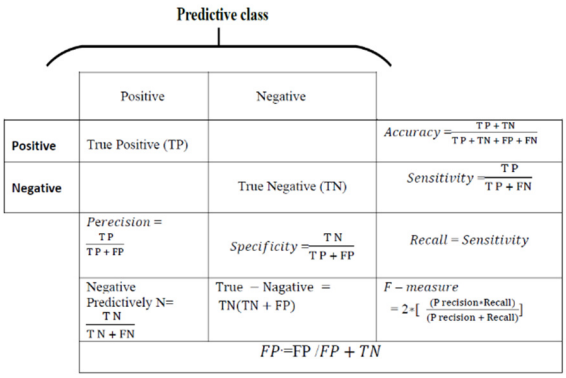

Figure 4. The designed system test and performance evaluation formula.

Table 4. The count attribute, divided into positive and negative categories.

Count	Positive	Negative
0	50000	10000
50	1000	2000
100	500	1500
150	200	1000
200	100	800
250	50	500
300	20	300
350	10	200
400	5	100
450	2	50
500	1	270000

The positive and negative common metrics calculated from the confusion matrix are precision and accuracy as shown in Figure 5

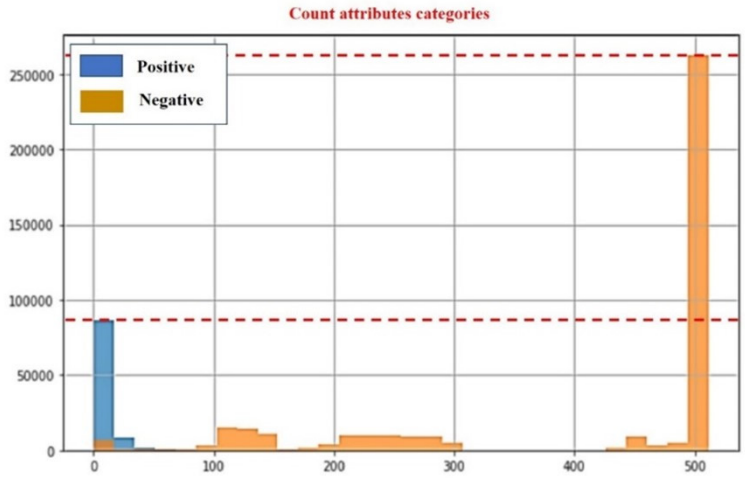

Figure 5. The frequency result attribute to the type of attack.

One data set was loaded in memory as made a quick visualization of the data showing its main characteristics, making a count of the numerical data and each column's type of data as shown in Figure 6.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2025 doi:10.20944/preprints202502.1674.v1

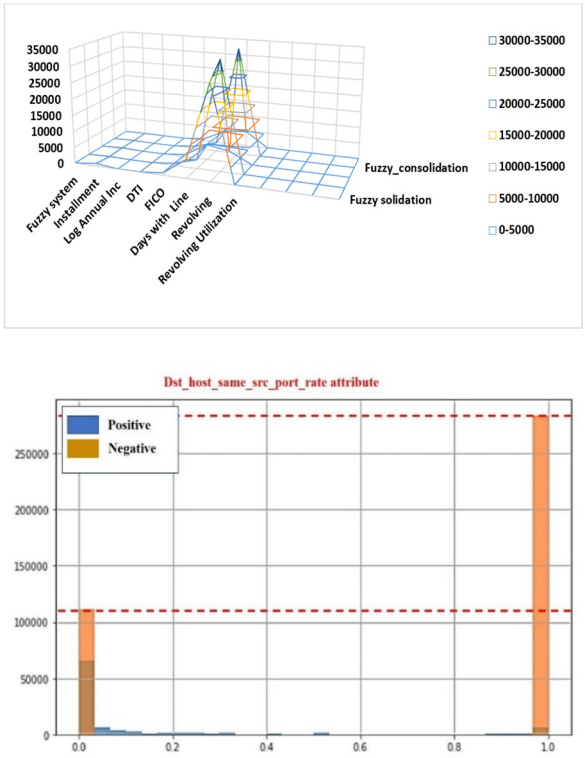

Figure 6. Public records, of the fuzzy based recommendation system.

The Figure 7 provides the detailed information for each data entry, covering aspects like fuzzy policy, DTI, FICO score, days with Line, and Revolving Utilization with showing its main characteristics, making a count of the numerical data, revolving utilization, inquiries in the last 6 months, delinquencies in the last 2 years, public records, of the fuzzy based recommendation system.

Figure 7. The frequency result attribute to the type of attack or normal.

The elect two main attributes, the most valued in the selection ranking, and visualized them in a frequency histogram according to the attack or normal, as shown in the following Figure 2, and 3, 4. As it corresponds to this DL algorithm type, proceeded to code the categorical attributes and scaling the data in the range to values between 0 and 1 using the Min-Max function contained in the Scikit-Learn library. Once the necessary normalization and scaling transformations of the dataset attributes were done and divided it into two train and test subsets and then trained our model using the Scikit-Learn decision tree Mei [17], J Su [21].

FL based recommendation generated system from sample attack detection show in the Figure 9.

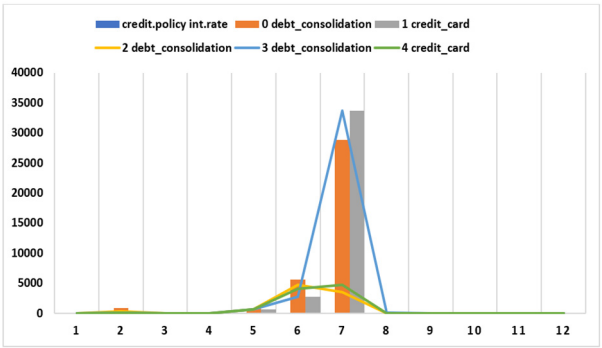

Figure 9. DL has advanced high-quality progress over the last decades.

The Figure 4, and Figure 5 foundation of the FL-based recommendation system is the characteristic and structure of neural networks whose building blocks are neurons. The FL-based

 doi:10.20944/preprints202502.1674.v1

recommendation system is aid of a self-propagating growth of era that acquiring new functionality from the virtual enterprise and information and conversation era. In this area of FL and DL has advanced high-quality progress. Figure **10.** Displays the frequency distribution of an attribute, divided into positive and negative categories

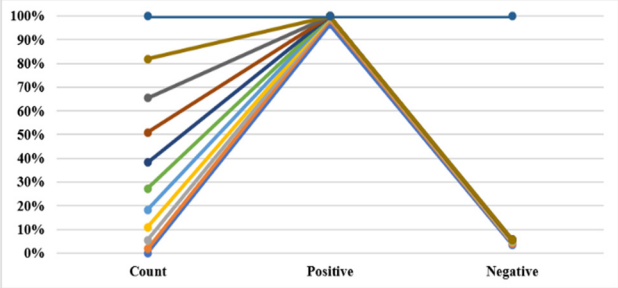

Figure 10. Displays the frequency distribution of an attribute, divided into positive and negative categories .

The Figure 10, show DL used for construct progress in any actual-international hassle the DL 99% data set based on the initial version.

5. Conclusion

We used Intel core i7-4790 CPU @3.60GH, RAM 16 GB, and 64-bit OS type. Our research focuses on a model that helps in the prevention and detection of fuzzy attacks aimed at individuals and organizations. The proposed model utilizes organizational processes, technological factors, and the human factor to address the threats posed by fuzzy attacks. We believe that it effectively helps reduce their impact on organizations. The fuzzy-based intelligent system is part of the self-propagating growth of an era that acquires new functionality from the virtual enterprise and the information and communication age. The FL and DL are techniques for handling variables that allow multiple values to be processed through the same variable. To resolve issues with an open, inexact spectrum of information makes it feasible to obtain an array of specific. Our proposed model is a FL based recommendation system, characterized by a HFD and loss computation model. Furthermore, the FL based model is developed using DL, along with a FL algorithm designed for detecting and preventing attacks. Configuration techniques results such as positive and negative attacks, which are attributed to the type of attack or normal behavior. The frequency results are attributed to the type of attack or normal behavior. Evolution analysis refers to the description and modeling of regularities or trends for objects whose count changes over time. The distribution includes a positive peak of 77 and a negative peak of over 100 categories, forming the foundation of the FL based recommendation system. In engineering, finding the proposed FL and DL recommendation system has the potential to provide valuable support and help users achieve their financial goals. here.

References

1. Jiang, Yiming, Chenguang Yang, and Hongbin Ma. "A Review of Fuzzy Logic and Neural Network Based Intelligent Control Design for Discrete-Time Systems." Discrete Dynamics in Nature and Society 2016, no. 1 (2016): 7217364.
2. Cherroun, Lakhmissi, and Mohamed Boumehraz. "Intelligent systems based on reinforcement learning and fuzzy logic approaches," Application to mobile robotic"." In 2012 International Conference on Information Technology and e-Services, pp. 1-6. IEEE, 2012.
3. Singh, Harpreet, Madan M. Gupta, Thomas Meitzler, Zeng-Guang Hou, Kum Kum Garg, Ashu MG Solo, and Lotfi A. Zadeh. "Real-life applications of fuzzy logic." Advances in Fuzzy Systems 2013 (2013): 3-3.
4. Fang, Hui, Danning Zhang, Yiheng Shu, and Guibing Guo. "Deep learning for sequential recommendation: Algorithms, influential factors, and evaluations." ACM Transactions on Information Systems (TOIS) 39, no. 1 (2020): 1-42.

 doi:10.20944/preprints202502.1674.v1

5. Jameson, Anthony, Martijn C. Willemsen, Alexander Felfernig, Marco De Gemmis, Pasquale Lops, Giovanni Semeraro, and Li Chen. "Human decision making and recommender systems." Recommender systems handbook (2015): 611-648.
6. Biswas, Siddhartha, Basudeb Mukhopadhyay, and Soumen Shaw. "Rayleigh surface wave propagation in orthotropic thermoelastic solids under three-phase-lag model." Journal of Thermal Stresses 40, no. 4 (2017): 403-419.
7. Biswas, Siddhartha, Basudeb Mukhopadhyay, and Soumen Shaw. "Thermal shock response in magneto-thermoelastic orthotropic medium with three-phase-lag model." Journal of Electromagnetic waves and Applications 31, no. 9 (2017): 879-897.
8. Yung –nien Sun, Yi-Ying Wang, Shao-Chien Chang, Li-wha Wu, and Sen – tien Tsai, "Color-based tumor segmentation for the automated estimation of oral cancer parameters", Microscopy Research and Technique, Vol. 73, Issue. 1, pp 5- 13, 2010.
9. Ranjan Rashmi Paul, Anirban Mukherjee, Pranab K. Dutta, Swapna Banerjee, Mousumi, Pal, Jyotirmoy Chatterjee, and Keya Chaudhuri, "A novel wavelet neural network-based pathological stage detection technique for an oral, precancerous condition", Journal of Clinical Pathology, Vol.58, Issue.9, pp 932 – 938,2024.
10. Biswas, B., & Mukhopadhyay, A. (2017). Phishing Detection and Loss Computation Hybrid Model A Machine-learning Approach. ISACA JOURNAL, 20-29.
11. Ding, J., & Sun, S. (2019). Integrative analysis of gene expression and methylation data for breast cancer cell lines. Biodata mining, 11(1), 13.
12. Kim, I., Choi, S., & Kim, S. (2019). BRCA-Pathway: a structural integration and visualization system of TCGA breast cancer data on KEGG pathways. BMC bioinformatics, 19(1), 42.
13. Li, C., Lee, J., Ding, J., & Sun, S. (2019). Integrative analysis of gene expression and methylation data for breast cancer cell lines. Biodata mining, 11(1), 13.
14. Mei, Y., Yang, J. P., Lang, Y. H., Peng, L. X., Yang, M. M., Liu, Q., ... & Li, C. Z. (2018). Global expression profiling and pathway analysis of mouse mammary tumor reveals strain and stage specific dysregulated pathways in breast cancer progression. Cell Cycle, 1-11.
15. Kim, I., Choi, S., & Kim, S. (2019). BRCA-Pathway: a structural integration and visualization system of TCGA breast cancer data on KEGG pathways. BMC bioinformatics, 19(1), 42.
16. Li, C., Lee, J., Ding, J., & Sun, S. (2019). Integrative analysis of gene expression and methylation data for breast cancer cell lines. Biodata mining, 11(1), 13.
17. Mei, Y., Yang, J. P., Lang, Y. H., Peng, L. X., Yang, M. M., Liu, Q., ... & Li, C. Z. (2018). Global expression profiling and pathway analysis of mouse mammary tumor reveals strain and stage specific dysregulated pathways in breast cancer progression. Cell Cycle, 1-11.
18. Kim, I., Choi, S., & Kim, S. (2019). BRCA-Pathway: a structural integration and visualization system of TCGA breast cancer data on KEGG pathways. BMC bioinformatics, 19(1), 42.
19. Li, C., Lee, J., Ding, J., & Sun, S. (2019). Integrative analysis of gene expression and methylation data for breast cancer cell lines. Biodata mining, 11(1), 13.
20. Zhang, Z Zhang, Z Li, and Y Qiao, “Joint Face Detection and Alignment Using Multi-Task Cascaded Convolutional Networks,” IEEE Signal Process Lett, 2016.
21. J Su, L Gao, W Li, Y Xia, N Cao, and R Wang, “Fast face tracking-by-detection algorithm for secure monitoring,” Appl Sci, 2019.