Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.034589
Article

Tech Science Press

Anomaly Detection Based on Discrete Wavelet Transformation for Insider Threat Classification

Dong-Wook Kim[1], Gun-Yoon Shin[1] and Myung-Mook Han[2,*]

[1]Department of Computer Engineering, Gachon University, Seongnam-si, 13120, Korea
[2]Department of AI Software, Gachon University, Seongnam-si, 13120, Korea
*Corresponding Author: Myung-Mook Han. Email: mmhan@gachon.ac.kr
Received: 21 July 2022; Accepted: 30 September 2022

Abstract: Unlike external attacks, insider threats arise from legitimate users who belong to the organization. These individuals may be a potential threat for hostile behavior depending on their motives. For insider detection, many intrusion detection systems learn and prevent known scenarios, but because malicious behavior has similar patterns to normal behavior, in reality, these systems can be evaded. Furthermore, because insider threats share a feature space similar to normal behavior, identifying them by detecting anomalies has limitations. This study proposes an improved anomaly detection methodology for insider threats that occur in cybersecurity in which a discrete wavelet transformation technique is applied to classify normal *vs.* malicious users. The discrete wavelet transformation technique easily discovers new patterns or decomposes synthesized data, making it possible to distinguish between shared characteristics. To verify the efficacy of the proposed methodology, experiments were conducted in which normal users and malicious users were classified based on insider threat scenarios provided in Carnegie Mellon University's Computer Emergency Response Team (CERT) dataset. The experimental results indicate that the proposed methodology with discrete wavelet transformation reduced the false-positive rate by 82% to 98% compared to the case with no wavelet applied. Thus, the proposed methodology has high potential for application to similar feature spaces.

Keywords: Anomaly detection; cybersecurity; discrete wavelet transformation; insider threat classification

1 Introduction

Cybersecurity threats in an organization can arise internally or externally. Although most defense systems focus on protecting resources against external attackers, many breaches of security data and privacy are caused by internal attackers. Internal attackers, such as employees and corporate partners that can legitimately connect to an organization's computer systems, pose a more lethal threat than external attackers [1]. Internal attackers have an understanding and knowledge of the organizational system and, unlike outsiders, they can possess all the necessary authorities and privileges to carry out a successful attack. These characteristics can make insider attacks look like normal tasks, which threatens the

principles of information protection for confidentiality, integrity, and availability in organizational networks and systems.

Researchers have long studied intrusion detection systems using machine learning methods to detect internal threats in the cybersecurity field. The machine learning methods used can be divided into signature-based detection methods that learn and classify normal and malicious behavior patterns, and anomaly detection outside a certain category by learning normal behavior [2]. The signature-based detection approach can perform detection only after learning the unique patterns of normal and malicious behavior. Furthermore, it loses functionality if malicious internal patterns cannot be continuously collected [3]. Most internal threat detection is performed using the anomaly detection approach; however, it is difficult to represent a clear normal category in the learning classes, thus leading to high false-positive rates. This occurs because malicious internal behavior is hidden in normal behavior, as the normal and malicious behaviors have similar patterns owing to the nature of internal threats.

This study proposes a methodology that applies discrete wavelets to improve anomaly detection performance based on the characteristics of insider threats. The proposed strategy involves removing noise belonging to the "normal category" of the training data and constructing a normal category similar to the existing one to overcome the limitations of the anomaly detection methodology while considering the characteristics of insider threats. This similar normal category is reconstructed such that approximations are obtained through the constant function in the existing normal category. This removes innocuous anomalies belonging to the normal profile in the training data, and the learning boundary is reconstructed by compressing the distance between data points scattered in the learning space [4]. This approach makes it possible to understand the class patterns of normal and malicious events for insider threats and reduces the false alarm rate, thus improving the anomaly detection performance.

We contribute to the detection of insider threats similar to normal patterns by first introducing the characteristics and types of insider threats in cybersecurity. Next, we address the limitations and problems associated with the machine learning taxonomy for anomaly detection in the area of insider threat detection and propose a way to overcome them with discrete wavelet transformation. Finally, we compare and evaluate the learning performance resulting from utilizing discrete wavelet transforms in anomaly detection algorithms.

The remainder of this paper is organized as follows. Section 2 describes insider threat characteristics and the limitations of anomaly detection. Section 3 details the dataset, discrete wavelet transformations, and machine learning algorithms used by the proposed method. Section 4 outlines the experiments conducted and analyzes the results obtained. Finally, Section 5 presents concluding remarks.

2 Literature Review

This section introduces anomaly detection methodologies and limitations related to insider threats in cybersecurity. Unlike external attacks, because insider threats behave based on an understanding of the organizational system, it is difficult to identify such malicious behavior. Therefore, this study defines the types and characteristics of insiders and explains the limitations of anomaly detection mechanisms in this regard.

2.1 Types and Characteristics of Insider Threats

Insider threats are defined as behaviors that can adversely impact an organization through malicious or unintentional use by an individual with authorized access and privileges over the organization's assets [5]. According to this definition, the types of insider threats can be divided into "unintentional" due to system misuse, "traitor" due to dissatisfaction within the organization, and "masquerader" who conceals their identity and engages in threat behavior [6]. Traitors are legitimate users who are granted access rights to systems and information resources but who violate policies or negatively impact the confidentiality, integrity, or availability of some information assets [7]. Traitors use their own legitimate credentials to

perform malicious acts. Masqueraders, a representative example of insiders, have the malicious objective of stealing and intercepting authorized access and pretending to be a legitimate user [6]. Masqueraders use compromised computers belonging to legitimate users through intercepted credentials to infiltrate information communication technology systems, so they are clearly malicious users in terms of intention.

In one type of insider threat, individuals can cause unintentional malicious behavior without even being aware of it; this is malicious behavior that threatens an organization through a legitimate user's unintentional mistake. For example, an employee can lose their work device, accidentally disclose sensitive company information on a social network, or fall prey to phishing or other disguised software attacks [8].

Insider threats are composed of complex elements that can occur in any cyber threat. Because traitors, masqueraders, and unintentional attacks do not violate the policies in defense systems and have characteristics that can be avoided, they show similar patterns to normal behavior [9]. Although normal users show activity sequences that reflect regular or normal behavior such as repetitive commands and system calls, there are potential internal threats that deviate from normal sequences based on the user's motives [10]. Hence, identifying insider threats requires defining a user's normal behavior and constructing potential patterns and sequences of their observed behavior. Solving this problem requires generating several characteristics for various potential patterns of users and including timings such as the start and end of the event. Event data for this study are available from Carnegie Mellon University's Computer Emergency Response Team (CERT) Insider Threat Center, which provides insider threat scenarios that have been used in numerous studies [11]. This research institute provides education on various scenarios and the prevention of insider threat behavior, and proposes mitigation measures through policies, culture, and education based on real cases, from the motives of users' abnormal behavior to the characteristics of human psychological factors.

2.2 Limited Anomaly Detection

In cybersecurity, complex and intelligent attacks like those by insiders consist of new attacks, anomalous attacks, and stealth attacks depending on the attacker's capabilities and objectives. The anomaly detection approach using machine learning typically employs a normal profile for model training with data belonging to general classes. However, because the abnormal data generated by most applications are either unlabeled or composed of unbalanced classes, the normal data may be mixed with a small amount of abnormal data [12].

In insider threats, even normal users always show unexpected behavior, which causes a wide category of "normal" patterns and makes the classification of potential internal threats unreliable. This leads to excessive false positives for "abnormal" behavior. Because a wide-ranging normal user data sample is much larger than the attack sample, it is difficult to detect threat events, and a single anomaly data instance is considered an anomaly when it differs from the rest of the normal pattern; however, it is sometimes considered an anomaly pattern if it occurs along with other data instances [13,14]. This issue can arise when the range of the normal data distribution is wide or sparse [15].

An obvious shortcoming of the anomaly detection strategy is that it requires an appropriate "normal" profile to be defined and a learning process. However, as in the related problem, creating a normal profile is a complex challenge, and creating an inappropriate normal profile can reduce performance or make it time-consuming to maintain the profile. Because the anomaly detection strategy involves finding anomaly events rather than attacks, it is impacted by false alarms. A false alarm occurs when the intrusion detection system reports a legitimate network activity as an intrusion event. The system may fail to detect real attacks or malicious activities because of their seemingly normal patterns. Accordingly, a key element of the latest anomaly detection systems is to resolve problems with modules that support correlation for these alarms. Nevertheless, owing to the typically high false alarm rates of anomaly detection systems, it is very difficult to associate a specific alarm with the event that triggered it, and

malicious users of the anomaly detection system can train the system to accept malicious behavior as normal by gradually poisoning it [16].

Other problems include the collection of real samples that did not occur and the detection of attacks due to delays in the detection process. As an active learning strategy to solve these problems, researchers have proposed methods for generating new data distributed around or in the low-density region of a real data manifold [17,18]. This strategy is designed so that detecting a new data distribution that did not occur can generate similar data from the distribution of existing training data. Low-density sections in the real data distribution are detected to generate similar data, for which a generative model is used.

Another strategy is to approximate the normal state of the input data to detect anomalies. This approach involves removing unnecessary noise according to each state and reconstructing new patterns in the process of characterizing normal and abnormal states. The approach applies wavelet transformation, which is typically used in signal processing. This approximation methodology enables sparsity or compression after applying signal transformation (e.g., Fourier, wavelet) as a compression and sampling theorem to the data sample [19]. The compressed sensing technique leverages the fact that a sparse signal has only a few important components and many unimportant components [20]. Characteristics that can indicate the boundary between insider misuse and normal behavior can be critical in this strategy [21].

3 Proposed Method

This study proposes an anomaly detection methodology for detecting malicious behavior events in each insider threat environment (see Fig. 1). Because a normal distribution of the input data is required to detect anomalies, the data are preprocessed, which includes scaling, removing meaningless values, and a statistical analysis. Next, discrete wavelet transformation is applied, which reduces the noise of the normal distribution and reconstructs it into a form with approximate values to the existing normal distribution. As the results widely vary with the parameters required for wavelet transformation, to compose a distribution with optimal fit, a coefficient that determines the fuzziness according to the fuzzy C-means clustering algorithm is used to evaluate separation according to class. Based on a partition coefficient value between 0 and 1, anomaly detection using machine learning is performed on the wavelet functions with high class separation. One-class support vector machine (SVM), a semi-supervised learning approach, is applied for the machine learning technique to classify normal and malicious users and anomalies, and the performance is evaluated and compared.

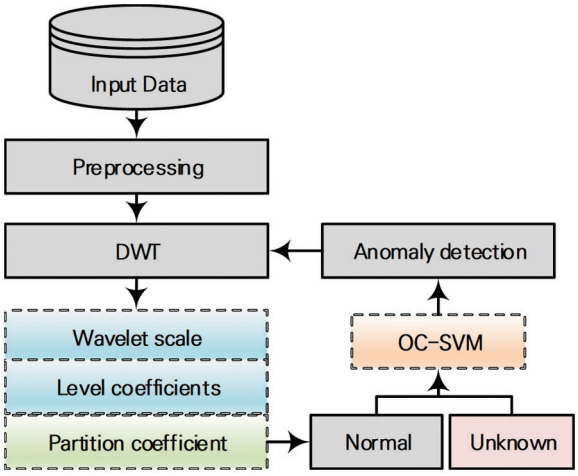


Figure 1: Overall process of the proposed insider threat detection method. (DWT: Discrete wavelet transformation; OC-SVM: One-class support vector machine)

3.1 Insider Threat Dataset

For the insider threat dataset, this study used a publicly available dataset for insider threat mitigation, approaches, development, and testing. Specifically, the CERT dataset, which contains over 1000 real cases of internal threats, was used. As shown in Table 1, the data comprise information on the user's computer activities, including logon/logoff, emails, websites, files, and removable drive connections, as well as organizational structure and user information.

Table 1: Configuration of the Computer Emergency Response Team (CERT) insider threat dataset

Activities file	Fields
logon	id, date, user, pc, activity (Logon/Logoff)
device	id, date, user, pc, activity
file	id, date, user, pc, filename, content
http	id, date, user, pc, url, content
email	id, date, to, from, size, attachment_count, content
psychometric	employee_name, user_id, O, C, E, A, N

The device file indicates whether a removable drive was used, the logon file indicates whether the user was logged in during working hours, holidays, etc., and according to the relationship of the device file and changes in operation time, the PC status can be determined using the logoff of the user's PC. The http file shows the URL of accessed domains, allowing one to determine whether the user visited a malicious web page. It has also been suggested that text analysis can be conducted assuming that the words in the URL are highly related to the web page. The email file contains records of the number of emails sent by the user per day and the email recipients. Employees and non-employees can be distinguished. The "file" file comprises headers including the file extension, and the normality or abnormality of file copies can be analyzed through data figures. The psychometric file shows external figures about the user, and O, C, E, A, and N indicate information related to the user's personality.

Based on these items, preprocessing is conducted to generate a dataset for machine learning, as shown in Fig. 2. Through a statistical analysis, activity frequency analysis, and organizational information analysis of the user for each file, data instances of the user's daily activities are generated. Regarding user activity creation, data from different sources are analyzed based on the user ID, and features such as time and number of operations are extracted to generate numerical vectors. With reference to Le et al. [22], 508 detailed features were constructed, including statistical features (e.g., mean, median, and standard deviation of the data) and email attachment size, file size, and number of words of websites visited. These generated data contained a total of three threat scenarios, including normal and malicious users, over a period of 72 weeks (18 months), and 330,452 data instances were generated for the daily activity period.

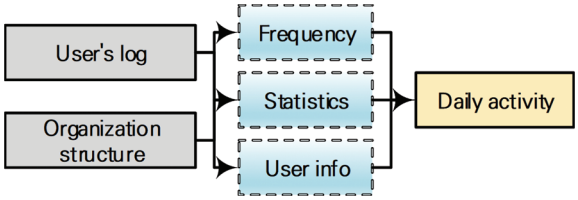


Figure 2: User preprocessing

3.2 Discrete Wavelet Transform

Wavelet transform, a time–frequency analysis tool, is utilized in numerous fields—including signal processing, computer graphics, neuroscience, sampling theorems, quantum mechanics, and medicine—and is mainly used to extract the abnormalities of signals whose characteristics change within a specific time. Wavelet analysis has functions similar to Fourier analysis but possesses the advantage of extracting specific frequencies that vary with time and frequency.

For the decomposition of abnormal sections using wavelet transformation, how the frequency varies over time can be identified by analyzing signals comprising high- and low-pass components of the time–frequency decomposition, a feature of the wavelet transform [23].

To represent the frequencies of signals with various magnitudes, the wavelet transform in Fig. 3 projects the discrete signal into two spaces, approximation coefficients (low-pass) and detail coefficients (high-pass).

$$y_{low}[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n-k] \tag{1}$$

$$y_{high}[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n-k] \tag{2}$$

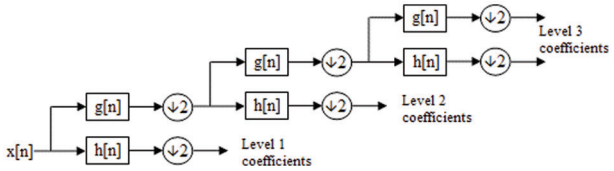


Figure 3: Discrete wavelet transform decomposition representation

The decomposition level can be selected based on the entropy and appropriate criteria according to the signal properties. The wavelet selection is then evaluated by comparing the reconstructed signal with the existing one or by calculating qualitative parameters for the decomposed coefficients. Various basic wavelet functions can be used for wavelet transformation, and the result may be influenced by the selected wavelet function. Seven representative wavelet functions that can be used are Haar, Daubechies (db), Biorthogonal (bior), Reverse Biorthogonal (rbior), Coiflets (coif), Symlets (sym), and Discrete Meyer (dmey) [24].

The data distribution caused by wavelet transformation is evaluated with the membership value by applying fuzzy C-means clustering, which can measure cohesion and separation through clustering analysis [25,26]. With the goal of generating a minimized distribution, the fuzzy partition coefficient (FPC) values are compared and analyzed with respect to parameter m, which determines the fuzziness of the clustering partitions and two clusters.

3.3 Anomaly Detection Algorithms

This study uses one-class SVM (OC-SVM), the basis of the decision boundary estimator, as the method to detect anomalies. OC-SVM divides the hyperplane based on the margin between the support vectors; however, unlike the standard SVM, it is based on the origin. Consequently, regardless of the amount and type of data, there can be only one class [27]. Therefore, OC-SVM can process datasets containing only patterns of a single target class [28]. OC-SVM classification seeks to distinguish one class of a target sample from all other classes, for which it must learn the minimum volume contour that encloses most of the data in a given dataset. This characteristic is used to find other data in the training dataset and is suitable for detecting anomalies. Through this approach, data corresponding to an attack is defined as

negative and that corresponding to normal is defined as positive, and 2-class classification is performed. Thus, OC-SVM classification is utilized to identify a specific class and classify all others as abnormal. For both labeled and unlabeled data, it is possible to reconstruct a learning framework to utilize the information [29].

4 Experimental Evaluation

The performance items of the proposed tasks were taken from the CERT insider threat dataset. From this dataset, through statistical, activity frequency, and organizational information analyses of the users, data instances of the users' daily activities were generated. The goal of the experiment was to classify the instances of normal and malicious users. Because normal and malicious users share similar characteristics, an experiment was performed to classify them.

The dataset used comprised the number of instances corresponding to insider scenarios, as shown in Table 2. As normal scenarios comprised 99.7% of the total number of instances, the dataset was highly unbalanced. Under these conditions, normal state learning was performed on the items of only 100 random users out of 930 normal users. Of these 100 random users, training data were used only for users confirmed to be normal users for 72 weeks who did not change into malicious users. Malicious Scenarios 1, 2, and 3 were synthesized and used for anomalies in the test data, and we analyzed how similar the activities of malicious users were to normal users through performance based on the false-positive rate.

Table 2: Number of instances by insider threat scenario

Scenario	Number of users	Number of instances
Normal	930	329,486 (99.71%)
Malicious scenario 1	30	85 (0.03%)
Malicious scenario 2	30	861 (0.26%)
Malicious scenario 3	10	20 (0.01%)
Total	1,000	330,452

In the experiments, we applied discrete wavelet transformations to insider scenarios. The representative wavelet functions were Haar, Daubechies (db), Biorthogonal (bior), Reverse Biorthogonal (rbior), Coiflets (coif), Symlets (sym), and Discrete Meyer (dmey). Each wavelet function analyzed the clustering distribution based on the decomposition level.

First, three-level denoising was performed through discrete wavelet transformation. For the scenarios of normal and malicious users, we modeled the reconstructed normal category according to the scale decomposition and coefficients of characteristic values with similar features. Table 3 compares the FPC values, which indicate how well separation was performed using fuzzy C-means by applying wavelets for known attacks of normal users used in the training data. "None," which denotes the non-application of wavelet transformation, has an FPC value of 0.50. In the wavelet family, "Daubechies" yielded the highest FPC and "Haar" yielded the lowest, but the difference was very insignificant at ±0.01. The FPC value for "None" is much lower than when wavelet transformation is applied, indicating that the data instances belonging to the cluster were spread over the entire feature space. This is one factor that hinders learning performance with noise from various data patterns. This performance is compared through the following classification performance.

Table 3: Fuzzy partition coefficient (FPC) comparison of wavelet transformation in insider threat scenarios

Wavelet family	Wavelet scale	FPC
None	None	0.500314
Biorthogonal	bior6.8	0.942403
Coiflets	coif17	0.943435
Daubechies	db32	0.945733
Discrete Meyer	dmey	0.943516
Haar	haar	0.939913
Reverse Biorthogonal	rbio5.5	0.942598
Symlets	sym19	0.943348

Next, OC-SVM was applied as the anomaly detection algorithm. Precision, recall, and F1-score were used as the evaluation metrics for user classification and anomaly detection for malicious activity was measured with the false-positive rate. Regarding the parameters of OC-SVM, *nu*, which adjusts the tolerance for misclassification, was set to (number of anomaly samples)/(total number of training data samples), and gamma, which defines the learning boundary, was set to 0.7 and 0.1. The classification performance of OC-SVM was then evaluated with these settings.

Table 4 shows the anomaly classification results for a gamma value of 0.7 was applied. Overall, the F1-score, which indicates that a normal scenario was detected as normal, was 97% on average. In terms of model performance, the area under the curve (AUC) of "None" (no wavelet applied) was very poor at 56.2%, whereas the other results with wavelet application yielded very good performance, with an average AUC of 94.6%. AUC is an indicator of the binary classifier's performance, where values of at least 0.5 can be regarded as good performance. In terms of the anomaly detection results for malicious scenarios, "None" showed a value of 82.7%, meaning that almost no malicious scenarios were detected, whereas db32 achieved the best performance at 0.104%. This corresponds to one misclassification out of 966 total anomalies. Haar yielded the worst performance, with 47 misclassifications out of 966 anomalies.

Table 4: Insider one-class support vector machine (SVM) (gamma = 0.7) classification. (AUC: area under the curve; FPR: false-positive rate; FNR: false-negative rate)

Wavelet	Precision	Recall	F1-score	AUC	FPR	FNR
None	0.929185	0.952311	0.940606	0.562594	0.827122	0.047688
bior6.8	0.99228	0.957953	0.974815	0.937051	0.08385	0.042046
coif17	0.995868	0.953537	0.974243	0.954512	0.044513	0.046462
db32	0.999903	0.953813	0.976314	0.976389	0.001035	0.046186
dmey	0.996148	0.951881	0.973512	0.955236	0.041407	0.048118
haar	0.988223	0.957309	0.97252	0.914472	0.128364	0.04269
rbio5.5	0.990207	0.958229	0.973956	0.925802	0.106625	0.04177
sym19	0.996651	0.958505	0.977206	0.961136	0.036231	0.041494

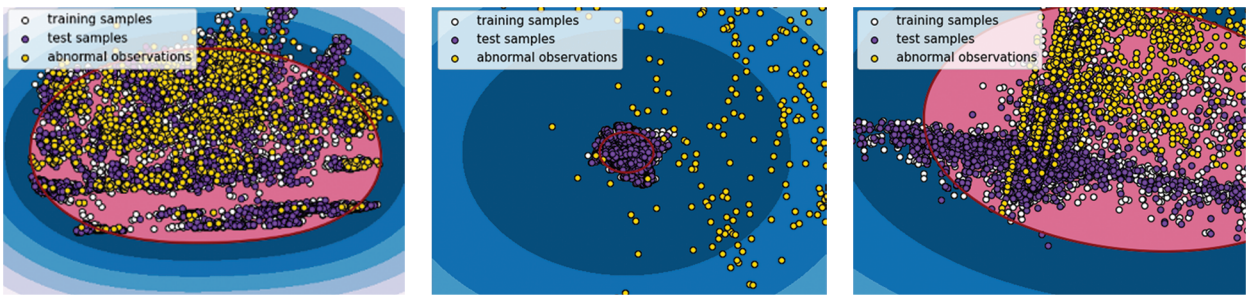
Table 5 shows the anomaly classification results when a gamma value of 0.1 was applied. The F1-score was 97.1% on average; however, the AUC of "None" was very low at 48.5%. The other results with a wavelet applied exhibited a much higher AUC, with an average of 95.6%. In particular, in terms of the anomaly detection results for malicious scenarios, "None" showed a value of 98.6%, indicating that it failed to classify malicious scenarios. db32 yielded the best performance at one misclassification out of 966 anomalies, and haar exhibited the worst performance at 299 misclassifications out of 966 anomalies.

Table 5: Insider one-class SVM (gamma = 0.1) classification

Wavelet	Precision	Recall	F1-score	AUC	FPR	FNR
None	0.918831	0.957401	0.93772	0.485429	0.986542	0.042598
bior6.8	0.985649	0.958836	0.972058	0.898673	0.16149	0.041163
coif17	0.998228	0.958031	0.977716	0.969181	0.019668	0.041968
db32	0.999906	0.958568	0.978801	0.978766	0.001035	0.041431
dmey	0.992588	0.958747	0.975374	0.937965	0.082815	0.041252
haar	0.972756	0.955346	0.963972	0.822911	0.309523	0.044653
rbio5.5	0.983288	0.958299	0.970633	0.884946	0.188405	0.0417
sym19	0.991924	0.956241	0.973756	0.933089	0.090062	0.043758

In conclusion, a very large difference can be confirmed by comparing the differences in the results of not applying the wavelet function. The reason is that in the case of "None," i.e., without the wavelet function, the data are very sparsely scattered and not concentrated on the learning boundary. The characteristics of OC-SVM can prove this well, and learning data patterns according to learning boundaries can explain this. We present a visual representation of applying a wavelet function along the learning boundaries below.

The wavelet transformation results are visually expressed in Fig. 4, in which the anomalies according to the learning boundary can be confirmed. First, Fig. 4a, which has no wavelet transformation (i.e., "None"), shows a form containing malicious instances due to its wide learning distribution spread. In db32 of Fig. 4b, because the training data are dense, the model clearly detects anomalies of malicious instances. Meanwhile, in the haar wavelet function of Fig. 4c, the training data have a scattered distribution, such that the distribution mixed with malicious users lead to disparity in the false-negative rate (FNR) results. Hence, if the space for learning the normal state has a high density, then the detection rate of anomalies in the test data is high.



(a) gamma = 0.1 "None" (b) gamma = 0.1 "db32" (c) gamma = 0.1 "haar"

Figure 4: Comparison of anomaly detection by learning boundary

When the normal data category is widely distributed like in insider threat scenarios, it is difficult to detect similar attack scenarios. However, the classification results can be improved by approximating the normal data category to a specific range. This study used OC-SVM, a representative anomaly detection algorithm, to analyze the evaluation of anomalies. db32, a wavelet function that can remove noise and increase the density of the training data, yielded the best performance and favorable classification results even with the shared characteristics between normal and malicious users.

However, although discrete wavelet transformations were applied to generate a normal anomaly detection profile, it was confirmed that the difference varies depending on the wavelet function. Calculating many wavelet functions is costly. Accordingly, more research is needed to optimize the appropriate parameters required for discrete wavelet conversion or to simplify them.

5 Conclusions

Insider threats are complex cyberattacks that have various threat motives depending on the user. These users typically maintain normal activities but may deviate from their normal behavior owing to potential motives. As these characteristics may appear similar to normal behavior, detecting them requires a function that can distinguish this behavior even in new patterns. The anomaly detection methodology learns a normal distribution for one class and identifies instances that deviate from this distribution as anomalies. However, this methodology can fail if the normal distribution contains potential threats and anomalies.

Accordingly, this study proposed a methodology for detecting potential threat behavior within normal behavior patterns such as insider threats. The experimental results showed that the best anomaly detection performance was obtained using a method that applies wavelet transformation for feature decomposition and denoising to construct the normal behavior distribution. With this methodology, we expect that discrete wavelet transformation techniques can contribute to various anomaly detection algorithms in data preprocessing. However, there are areas that need to be improved. For example, because wavelet transformations require decomposition levels and wavelet functions, appropriate optimization must be performed. In the future, relevant mechanisms will be added to achieve this.

Funding Statement: This work was supported by the Research Program through the National Research Foundation of Korea, NRF-2022R1F1A1073375.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici and M. Ochoa, "Insight into insiders and IT," *ACM Computing Surveys*, vol. 52, no. 2, pp. 1–40, 2020.

[2] N. Sultana, N. Chilamkurti, W. Peng and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493–501, 2018.

[3] M. Sevri and H. Karacan, "Two stage deep learning based stacked ensemble model for web application security," *KSII Transactions on Internet and Information Systems*, vol. 16, no. 2, pp. 632–657, 2022.

[4] M. Salagean and I. Firoiu, "Anomaly detection of network traffic based on analytical discrete wavelet transform," in *2010 8th Int. Conf. on Communications*, Bucharest, Romania, pp. 49–52, 2010.

[5] M. C. Theis, R. F. Trzeciak, D. L. Costa, A. P. Moore, S. Miller *et al., Common Sense Guide to Mitigating Insider Threats*, Pittsburgh, Pennsylvania, USA: Carnegie Mellon University, 2019. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540644.

[6] D. Cappelli, A. Moore and R. Trzeciak, "The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud)," in *SEI Series in Software Engineering*, Boston, USA: Addison-Wesley, pp. 23–127, 2012.

[7] M. B. Salem, S. Hershkop and S. J. Stolfo, "A survey of insider attack detection research," in *Insider Attack and Cyber Security*, vol. 39, Boston, USA: Springer, pp. 69–90, 2008.

[8] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese *et al.,* "Understanding insider threat: A framework for characterising attacks," in *2014 IEEE Security and Privacy Workshops*, San Jose, CA, USA, pp. 214–228, 2014.

[9] B. Sharma, P. Pokharel and B. Joshi, "User behavior analytics for anomaly detection using LSTM autoencoder-insider threat detection," in *Proc. of the 11th Int. Conf. on Advances in Information Technology*, New York, NY, USA, pp. 1–9, 2020.

[10] P. Parveen and B. Thuraisingham, "Unsupervised incremental sequence learning for insider threat detection," in *2012 IEEE Int. Conf. on Intelligence and Security Informatics*, Washington, DC, USA, pp. 141–143, 2012.

[11] J. Glasser and B. Lindauer, "Bridging the gap: A pragmatic approach to generating insider threat data," in *2013 IEEE Security and Privacy Workshops*, San Francisco, CA, USA, pp. 98–104, 2013.

[12] J. Kong, W. Kowalczyk, S. Menzel and T. Bäck, "Improving imbalanced classification by anomaly detection," in *Parallel Problem Solving from Nature–PPSN XVI. Springer International Publishing*, vol. 12269, Berlin/Heidelberg, Germany: Springer, pp. 512–523, 2020.

[13] M. Ahmed, A. Naser Mahmood and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.

[14] M. Hosseinzadeh, A. M. Rahmani, B. Vo, M. Bidaki, M. Masdari *et al.,* "Improving security using SVM-based anomaly detection: Issues and challenges," *Soft Computing*, vol. 25, no. 4, pp. 3195–3223, 2020.

[15] X. Liu, J. Ren, H. He, Q. Wang and S. Sun, "A novel network anomaly detection method based on data balancing and recursive feature addition," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 7, pp. 3093–3115, 2020.

[16] A. Paudice, L. Muñoz-González, A. Gyorgy and E. C. Lupu, "Detection of adversarial training examples in poisoning attacks through anomaly detection," arXiv preprint arXiv:1802.03041, pp. 1–10, 2018.

[17] D. Hendrycks and K. Gimpel, "A baseline for detecting misclassified and out-of-distribution examples in neural networks," arXiv preprint arXiv:1610.02136, Toulon, France, pp. 1–12, 2016.

[18] N. Goernitz, M. Kloft, K. Rieck and U. Brefeld, "Toward supervised anomaly detection," *Journal of Artificial Intelligence Research*, vol. 46, pp. 235–262, 2013.

[19] M. M. Abo-Zahhad, A. I. Hussein and A. M. Mohamed, "Compressive sensing algorithms for signal processing applications: A survey," *International Journal of Communications, Network and System Sciences*, vol. 8, no. 6, pp. 197–216, 2015.

[20] A. Moon, X. Zhuo, J. Zhang and S. W. Son, "AD2: Improving quality of IoT data through compressive anomaly detection," in *2019 IEEE Int. Conf. on Big Data (Big Data)*, Los Angeles, CA, USA, pp. 1662–1668, 2019.

[21] J. Hunker and C. W. Probst, "Insiders and insider threats-an overview of definitions and mitigation techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 1, pp. 4–27, 2011.

[22] D. C. Le, N. Zincir-Heywood and M. I. Heywood, "Analyzing data granularity levels for insider threat detection using machine learning," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 30–44, 2020.

[23] Ł. Saganowski, T. Andrysiak, R. Kozik and M. Choraś, "DWT-based anomaly detection method for cyber security of wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 15, pp. 2911–2922, 2016.

[24] P. K. de Macedo Machado Freire, C. A. G. Santos and G. B. L. da Silva, "Analysis of the use of discrete wavelet transforms coupled with ANN for short-term streamflow forecasting," *Applied Soft Computing*, vol. 80, pp. 494–505, 2019.

[25] F. L. Gaol, S. Yi and F. Deng, "Research of network intrusion detection system based on data mining," in *Recent Progress in Data Engineering and Internet Technology*, vol. 157, Berlin/Heidelberg, Germany: Springer, pp. 141–148, 2012.

[26] L. Duan, W. Wang and B. Han, "A hybrid recommendation system based on fuzzy C-means clustering and supervised learning," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 7, pp. 2399–2413, 2021.

[27] O. A. Alzubi, J. A. Alzubi, A. M. Al-Zoubi, M. A. Hassonah and U. Kose, "An efficient malware detection approach with feature weighting based on Harris Hawks optimization," *Cluster Computing*, vol. 25, no. 4, pp. 2369–2387, 2021.

[28] R. K. Malaiya, D. Kwon, J. Kim, S. C. Suh, H. Kim *et al.,* "An empirical evaluation of deep learning for network anomaly detection," in *2018 Int. Conf. on Computing, Networking and Communications (ICNC)*, Maui, HI, USA, pp. 893–898, 2018.

[29] C. Scott and G. Blanchard, "Novelty detection: Unlabeled data definitely help," in *Proc. of the Twelfth Int. Conf. on Artificial Intelligence and Statistics*, Clearwater Beach, Florida, USA, pp. 464–471, 2009.