International Journal of Service and Knowledge Management
International Institute of Applied Informatics
2025, Vol. 9, No. 1, IJSKM929

Proactive Internal Fraud Detection Strategies Utilizing UX Data Based on Multiple Sensors

Shigeaki Tanimoto [*], Yuta Takagi [†], Takashi Hatashima [‡], Atsushi Kanai [§]

Abstract

The COVID-19 pandemic forced companies to change how they work, promoting a work style unbound by time or location, such as teleworking. While convenient, this remote approach has been linked to increased internal fraud risks due to alienation, perceived unfairness, and reduced compliance awareness. In 2023, Japan's Information-technology Promotion Agency (IPA) ranked "information leaks due to internal misconduct" as the fourth most critical information security threat. Internal fraud is categorized into carelessness/negligence (60%) and intentional misconduct (40%), with the latter costing 1.34 times more to address, leading to significant financial losses. This paper explores user experience (UX) environments utilizing sensors to collect non-cyber information, such as facial expressions, to counter intentional fraud. A theoretical analysis indicates that combining two sensor types—environmental and biometric—offers the most cost-effective solution, significantly improving fraud detection rates. While adding more sensor types enhances accuracy, cost-effectiveness declines beyond three types. Additionally, the detection of *rationalization* remains consistently low, highlighting the need for complementary methods like text and speech analysis or long-term behavioral monitoring. These findings underscore the effectiveness of UX-based non-cyber information and its potential as an innovative approach to mitigating intentional internal fraud.

Keywords: Internal fraud detection, Sensor, User experience, Fraud pentagon theory

1 Introduction

The COVID-19 Pandemic significantly reshaped corporate work environments. In particular, many companies accelerated the adoption of remote workstyles, such as telework, which enable employees to work flexibly regardless of time and location [1]. While this shift offers greater convenience, it has also been pointed out that such work arrangements may increase the psychological predisposition to internal fraud, driven by factors such as a sense of isolation, perceived unfairness, and declining adherence to rules. In fact, the "Top 10 Information Security Threats 2023" report published by Japan’s Information-Technology Promotion Agency (IPA) ranks "Information leakage due to internal fraud" as the 4th biggest threat and "Attacks targeting new

[*] Japan International University, Ibaraki, Japan
[†] Chiba Institute of Technology, Chiba, Japan
[‡] NTT Social Informatics Laboratories, Tokyo, Japan
[§] Hosei University, Tokyo, Japan

normal workstyles such as telework" as the 5th biggest threat [2]. This underscores the growing security risks posed by internal fraud, which has become a major concern [3]. A breakdown of internal fraud cases reveals that approximately 60% result from negligence or carelessness, while 40% are intentional [4]. Although unintentional incidents constitute the majority, the cost of countermeasures against intentional fraud is approximately 1.34 times higher than that against negligence and carelessness [5]. In other words, when considering prevention costs quantitatively, intentional internal fraud results in greater financial losses for companies.

Meanwhile, the use of UX (User Experience) in conjunction with sensor technology has been proposed as a method to prevent psychological states that lead to internal fraud in advance [6]. However, measures to prevent intentional internal fraud utilizing UX have not been thoroughly examined.

In this paper, we aim to contribute to preventing intentional internal fraud by visualizing psychological and other internal states, which have traditionally been difficult to assess. Specifically, we focus on a UX environment that enables the collection of non-cyber information, such as user facial expressions. More concretely, we analyze and visualize real-time data on user facial expressions and other information obtained from multiple sensors as non-cyber information and propose and evaluate internal fraud countermeasures on the basis of these insights.

The rest of this paper is as follows. Section 2 discusses the current state and challenges of internal fraud. Section 3 provides an overview of existing internal fraud prevention theories, including the Fraud Triangle Theory, as well as related research. Section 4 builds on the internal fraud prevention theories discussed in Section 3 and proposes and evaluates a proactive internal fraud detection strategy based on utilizing UX data from sensors as a new internal fraud prevention approach focusing on the UX environment. Section 5 presents the conclusion and future challenges.

2 Current State and Issues of Internal Fraud

2.1 Current State of Internal Fraud

Internal fraud refers to fraudulent activities in which an organization’s current or former members steal, leak, or delete critical information. These fraudulent acts include not only intentional actions, such as those driven by financial motives, but also unintentional mistakes caused by negligence. According to the "Guidelines for Preventing Internal Fraud in Organizations" published by the IPA, internal fraud encompasses not only illegal acts but also violations of internal information security regulations, even if they do not strictly constitute criminal offenses [3].

Specific examples of internal fraud include theft, unauthorized removal, leakage, deletion, or destruction of valuable information assets or information systems. Additionally, disclosing confidential information obtained during employment after resignation is also classified as internal fraud [3]. Notably, incidents of information leakage caused by employees misusing their access to personal data continue to occur frequently. In fact, the "Top 10 Information Security Threats" report, published annually by the IPA, has ranked internal fraud-related information leaks in the top 10 threats for more than a decade, placing it 4th in 2023 [2].

Furthermore, the rapid expansion of telework that started during COVID-19 Pandemic has become a significant factor contributing to increased internal fraud risks. Employees working from home or other remote locations are outside the direct supervision of colleagues and superiors, making it more difficult for organizations to ensure compliance with internal regulations. The Cabinet Office of Japan has identified "difficulty in casual consultations and reporting within the company" and "lack of communication relying solely on screen-based interactions" as key disadvantages of telework, which in turn increase employee stress levels [7].

A stressful work environment can negatively impact employees' mental and physical well-being, lower their motivation, and lead to growing dissatisfaction with their organization. If left unaddressed, this can result in a decline in compliance awareness and an increased risk of internal fraud motivation. The IPA's "Guidelines for Preventing Internal Fraud in Organizations" also highlight that feelings of isolation and perceived unfairness among teleworking employees can weaken their commitment to rules, making them more psychologically inclined to commit internal fraud [3].

Thus, in telework environments, the physical separation of employees makes it harder for them to seek advice and support, potentially leading to increased stress and concerns that may act as a trigger for internal fraud.

2.2 Issues of Internal Fraud

According to a survey conducted by the IPA [4], approximately 40% of respondents who had engaged in internal fraud did so intentionally, as shown in Fig. 1. The survey revealed several reasons for such behavior, including the following: "Work was too busy, and I needed to take data home to complete tasks," "There were rules in place, but since others repeatedly violated them, I followed suit," and "I wanted to monetize the information or equipment I took." These issues can potentially be prevented through educational and training programs aimed at improving information ethics and IT literacy, as well as through stricter technical measures, such as enhanced access control management.

On the other hand, internal fraud motivated by "dissatisfaction with salary or treatment," "the desire to leverage stolen information or equipment for a new job or startup," or "holding a grudge against the company, organization, or superiors" is less likely to be effectively addressed through education and training alone. Additionally, it has been reported that about 50% of individuals who engaged in internal fraud were system administrators, indicating that even strict access control measures cannot completely prevent internal fraud.

Furthermore, according to a survey conducted by the IPA on the current state of internal fraud prevention frameworks [8], the following measures were identified as the top responses in the questionnaire asking, "Are there internal fraud prevention measures in place for teleworking employees?":

- Restricting the handling of sensitive information in telework environments to prevent information leakage.
- Educating and enforcing internal regulations and legal requirements related to telework.
- Collecting and analyzing activity logs from company-provided telework PCs to enhance early detection and post-incident response to internal fraud.

However, these top three measures have implementation rates below 40%, indicating that the current level of countermeasures is insufficient. Notably, less than 20% of companies reported implementing measures to ensure adequate communication with teleworking employees. This suggests that a lack of communication in telework environments reduces interactions among employees, potentially creating conditions that facilitate internal fraud.

These findings evidently show that, despite the increasing adoption of new normal workstyles such as telework, internal fraud prevention measures remain inadequate. Addressing this issue should be regarded as a critical challenge moving forward.

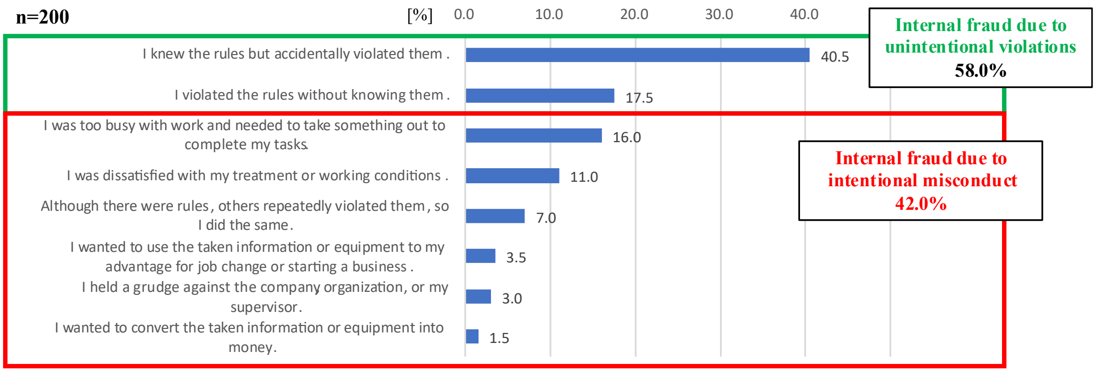


Figure 1: Survey on reasons for committing internal fraud, conducted by IPA [4]

3 Theories and Related Work on Internal Fraud

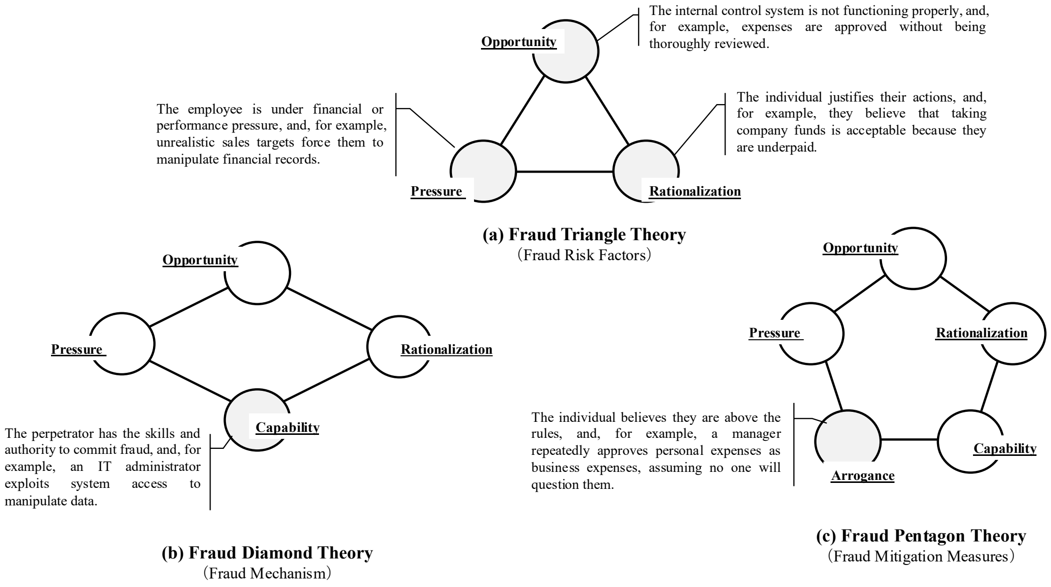
3.1 A Multidimensional Model of Fraud

One of the most influential prior studies on the factors leading employees to commit internal fraud is the Fraud Triangle Theory proposed by Donald Cressey, an American organizational crime researcher [9]. This theory was developed on the basis of empirical analysis of prisoners convicted of embezzlement. Cressey argued that three key elements contribute to fraudulent behavior: Pressure (Motivation), Opportunity, and Rationalization (Fig. 2(a)) [9][10].

- Pressure (Motivation): Personal factors such as financial pressure.
- Opportunity: Weak internal controls and inadequate audits.
- Rationalization: A psychological process in which individuals justify their fraudulent actions.

Beyond the Fraud Triangle Theory, Wolfe, D. T., et al. introduced the Fraud Diamond Theory, which incorporates a fourth element: Capability (Fig. 2(b)) [10]. This theory considers individual traits (such as knowledge, skills, and position) of the fraudster, providing a crucial perspective for evaluating the feasibility of fraud execution. Furthermore, the Fraud Pentagon Theory extends this framework by adding Arrogance as a fifth factor (Fig. 2(c)) [11]. This theory focuses on the sense of power and entitlement of fraud perpetrators, particularly analyzing the increased risk of fraud among executives and managerial personnel

In the past few years, with the widespread adoption of telework that started during the COVID-19 Pandemic, concerns have been raised that employees may become more psychologically prone to committing internal fraud due to feelings of isolation, perceived unfairness, and a decline in rule compliance awareness [3]. Therefore, to comprehensively assess internal fraud risks, it is crucial to integrate the Fraud Triangle Theory, which explains the causes and psychological factors behind fraud, the Fraud Diamond Theory, which considers fraud structures and feasibility, and the Fraud Pentagon Theory, which includes the influence of organizational culture and leadership.



The internal control system is not functioning properly, and, for example, expenses are approved without being thoroughly reviewed.

The employee is under financial or performance pressure, and, for example, unrealistic sales targets force them to manipulate financial records.

The individual justifies their actions, and, for example, they believe that taking company funds is acceptable because they are underpaid.

(a) Fraud Triangle Theory
(Fraud Risk Factors)

The perpetrator has the skills and authority to commit fraud, and, for example, an IT administrator exploits system access to manipulate data.

(b) Fraud Diamond Theory
(Fraud Mechanism)

The individual believes they are above the rules, and, for example, a manager repeatedly approves personal expenses as business expenses, assuming no one will question them.

(c) Fraud Pentagon Theory
(Fraud Mitigation Measures)

Figure 2: Multidimensional model of fraud [9] - [11]

3.2 Related Work

3.2.1 Existing Studies on Internal Fraud Prevention

Numerous studies have been conducted on countermeasures for preventing internal fraud. One of the key studies is a systematic literature review on insider threats by P. Singh et al., which classifies and analyzes factors such as insider types, access privileges, motivations, profiling, and attack methods [12]. Additionally, D. Maimon et al. leveraged insights from research on deviant workplace behavior and workplace incivility to propose a classification system for insider threats [13].

Furthermore, N. Mehrnezhad et al. proposed a unified framework for insider threat prevention, incorporating technical, psychological, behavioral, and cognitive factors [14]. Meanwhile, J. R. C. Nurse et al. developed a framework for understanding and identifying insider threats, which clarifies insider threat characteristics on the basis of case studies and psychological theories [15].

These studies primarily focus on the systematic classification of insider threats and the development of theoretical frameworks for insider fraud prevention. However, concrete countermeasures and practical approaches have been insufficiently discussed.

3.2.2 Research on Early Detection of Internal Fraud and UX Design

Next, several previous studies have explored early detection of internal fraud through UX and environmental monitoring of users, as specific measures for preventing internal fraud. First, Shima et al. statistically analyzed and evaluated survey results during the development of workplace measures for preventing internal fraud [16]. Their study examined how the workplace environment influences employees' behavior and awareness and explored effective countermeasures to deter internal fraud. Meanwhile, Niihara experimentally analyzed factors that induce internal fraud using crowdsourcing and quantitatively clarified how organizational environmental factors, such as monitoring conditions and account sharing, impact fraudulent behavior. On the basis of these findings, he proposed effective countermeasures for preventing internal fraud [17].

Additionally, M. Graham et al. introduced a case study on the development process of data visualization to enhance commercial software platforms for insider threat countermeasures [18]. Their goal was to overcome the limitations of existing user interfaces (UI), making it easier for analysts to detect patterns and anomalies. Specifically, they proposed a method to support insider threat detection and understanding through improved user experience. Furthermore, S. Bertrand et al. proposed an unsupervised learning method based on the Bayesian Gaussian Mixture Model to detect insider threats through user behavior monitoring [19]. Their study aimed to identify abnormal activities by analyzing user behavioral patterns, contributing to the early detection of internal fraud. Additionally, from a user experience perspective, they proposed a method for modeling users' normal behavior and performing anomaly detection.

These studies explore methods for detecting and preventing insider threats through improvements in user behavior monitoring and interface design. However, none have directly applied UX design as a countermeasure for internal fraud prevention.

As discussed above, research on internal fraud prevention measures, particularly those related to UX design, has not yet advanced sufficiently. Considering the future development of UX design and its potential applications, applying UX design to internal fraud prevention remains an important research issue.

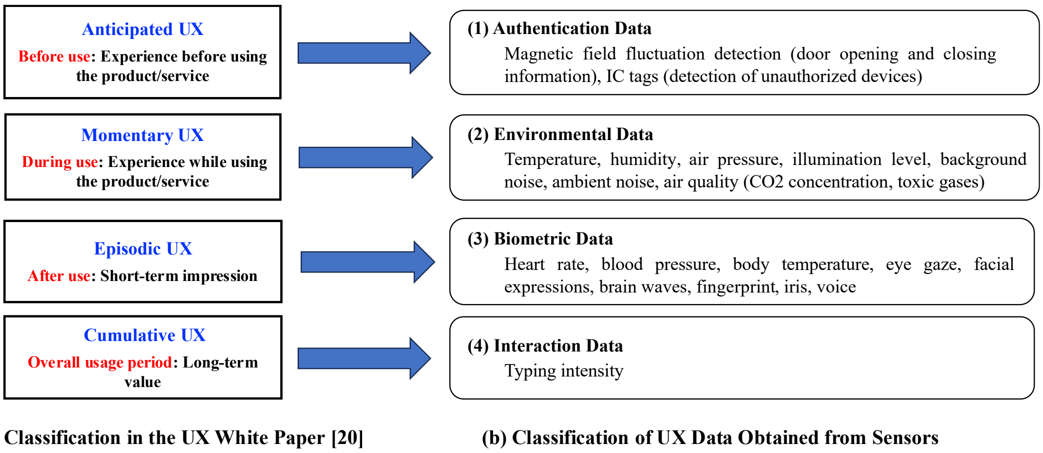
4 Proactive Internal Fraud Detection Strategies

4.1 Classification of UX Data Identified from Sensor Data

Here, referring to the UX White Paper [19] and other sources, we extracted sensor data that can currently be obtained as UX data. Specifically, as shown in Fig. 3(a), we classified sensor data that can be acquired as UX data from a measurement perspective into the four categories presented in the UX White Paper: "Anticipated UX" (pre-use experience), "Momentary UX" (experience during use), "Episodic UX" (short-term impression), and "Cumulative UX" (long-term value). For this classification, we also referred to sources such as [20]. As a result, as shown in Fig. 3(b), the data was categorized into four groups.

1. **Authentication Data**: This category includes door open/close detection using magnetic sensors and device authentication via IC tags in the user environment. Since these data are obtained before UI interaction, they correspond to Anticipated UX (experience before use) according to the UX White Paper classification.
2. **Environmental Data**: This refers to Momentary UX data (experience during use) that can be acquired while the user is working. Unlike personal biometric data, this category includes environmental factors such as temperature, noise levels, and the presence of external individuals. Since these data are collected during UI interaction, they are classified as Momentary UX.
3. **Biometric Data**: This category includes physiological indicators during user activity, such as heart rate, movement, and brain waves. These data reflect the user's physiological state during work and correspond to Episodic UX (short-term impression) in the UX White Paper classification.
4. **Interaction Data**: This category includes Cumulative UX data (long-term value), which is accumulated through repeated use. It consists of data such as typing accuracy and intensity, which can be used to detect anomalies compared to normal user behavior. Since

these data are gradually accumulated during UI interactions, they are classified as Cumulative UX.


Anticipated UX
Before use: Experience before using the product/service
Momentary UX
During use: Experience while using the product/service
Episodic UX
After use: Short-term impression
Cumulative UX
Overall usage period: Long-term value
(1) Authentication Data
Magnetic field fluctuation detection (door opening and closing information), IC tags (detection of unauthorized devices)
(2) Environmental Data
Temperature, humidity, air pressure, illumination level, background noise, ambient noise, air quality (CO2 concentration, toxic gases)
(3) Biometric Data
Heart rate, blood pressure, body temperature, eye gaze, facial expressions, brain waves, fingerprint, iris, voice
(4) Interaction Data
Typing intensity

(a) Classification in the UX White Paper [20] **(b) Classification of UX Data Obtained from Sensors**

Figure 3: UX data classification based on the UX White Paper [19]

4.2 Verification of Proactive Internal Fraud Detection Feasibility Using UX Data

Using the UX data shown in Fig. 3(b), we analyzed the feasibility of proactively detecting elements related to internal fraud. Specifically, on the basis of the four categories in Fig. 3(b), we classified the major sensors currently available and evaluated UX data that can be used to detect precursors of internal fraud. When evaluating UX data for proactive detection, we defined names in accordance with the number of categories used. A single category was referred to as a "Single Sensor", two categories as a "Dual-Sensor Combination", three categories as a "Triple-Sensor Combination", and four categories as a "Quad-Sensor Combination", which formed the basis for our analysis. We conducted a theoretical evaluation to verify whether each element of the Fraud Pentagon Theory, as shown in Fig. 2(c), can be detected using these UX data. Specifically, for the five axes of the Fraud Pentagon Theory (Motivation, Opportunity, Rationalization, Capability, and Arrogance), we assessed whether each sensor effectively detects these axes, specifically, whether it is useful for proactively detecting internal fraud. As an initial examination, a simple evaluation was conducted on the basis of the subjective judgment of the authors (security researchers from academia and industry) to determine feasibility. The assessment was performed using the following three levels:

✔(1.0): Proactive internal fraud detection is directly enabled using data obtained from the sensor.

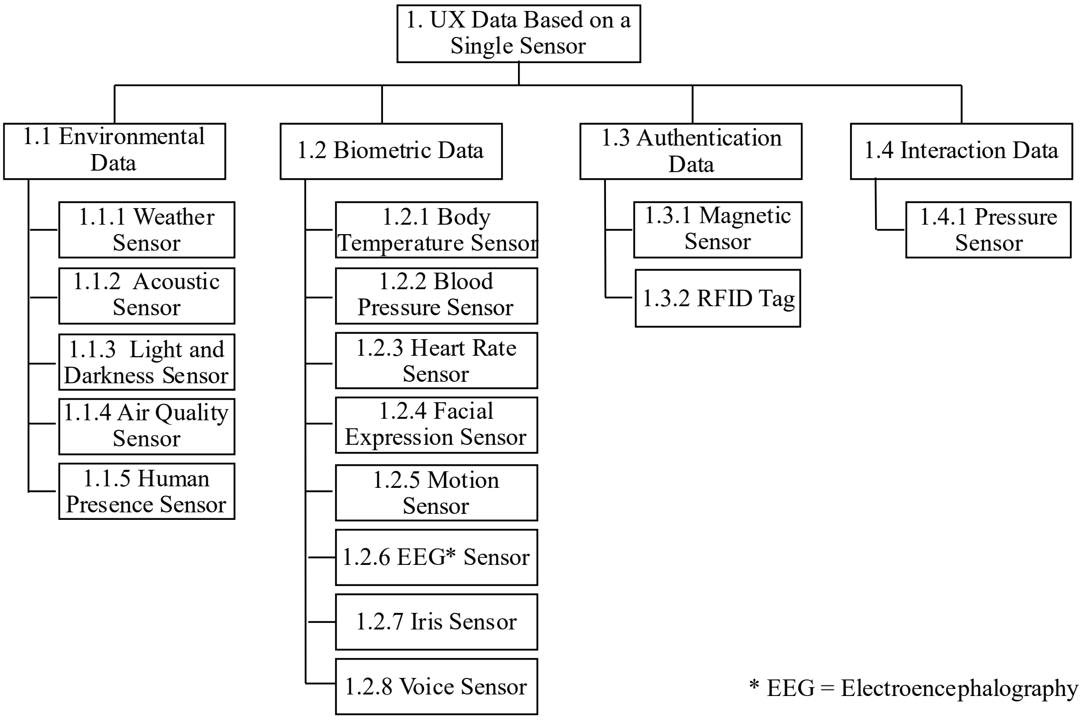
▲(0.5): Proactive internal fraud detection is indirectly enabled by using data obtained from the sensor.

✘ (0.0): Proactive internal fraud detection is difficult using data obtained from the sensor.

These values (1.0, 0.5, 0.0) represent a numerical conversion of qualitative evaluations into a three-value data format and are dimensionless quantities with no physical units.

4.2.1 Case of a Single Sensor

On the basis of literature sources ([20], etc.) and discussions among ourselves, we extracted sensors that are currently considered relevant to UX for each of the four categories in Fig. 3(b). As a result, as shown in Fig. 4, we identified and organized 16 types of UX data that can currently be obtained using a single sensor (e.g., light sensor, motion sensor). Using the UX data shown in Fig. 4, we evaluated the applicability of each data type to the five elements of the Fraud Pentagon Theory. Specifically, as shown in Table 1, we assessed whether proactive internal fraud detection is feasible for each element of the Fraud Pentagon Theory using a single sensor.



* EEG = Electroencephalography

Figure 4: List of UX data selected for single sensors

Table 1: Verification of proactive fraud detection with a single sensor

1.1.1 Weather Sensor		
Fraud Pentagon Theory	Sensor Detectability for Fraud Triangle Elements	Detectability
① Pressure	If the working environment is excessively hot or cold, it can be detected as a motivation for fraudulent behavior (it can be detected by acquiring data such as room temperature in the working environment).	▲
② Opportunity	If the room temperature in the working environment deviates from the appropriate range, it can be detected as an opportunity for fraudulent behavior. Here, the "appropriate temperature" is defined based on the Office Sanitation Standards Regulation of Japan's Ministry of Health, Labour and Welfare, referring to a state where the room temperature in the working environment falls outside the range of 18 to 28°C [21] (it can be detected by acquiring data such as room temperature in the working environment).	✔
③ Rationalization	Thoughts such as "It's the company's fault for not improving the environment" or "It can't be helped" can be detected as Rationalization for fraudulent behavior (it can be detected by acquiring data such as room temperature in the working environment; for example, when a high-temperature working environment persists).	▲
④ Arrogance	Simply acquiring meteorological information such as room temperature in the working environment does not allow the detection of the status, position, or capability of the user operating the user interface (UI).	✕
⑤ Capability	Simply acquiring meteorological information such as room temperature in the working environment does not allow the detection of personal traits such as confidence or arrogance of the user operating the UI.	✕

(Note) ✔ (1.0): Directly detectable ▲ (0.5): Indirectly detectable ✕ (0.0): Difficult to detect

As a result of conducting the same verification for the remaining 15 sensors, the results shown in Table 2 were obtained. On the basis of this analysis, we calculated the average proactive internal fraud detection rate for each of the five elements of the Fraud Pentagon Theory using a single sensor. In this evaluation, since three-value data (✔, ▲, ✖) was used, the arithmetic mean was not applied; instead, the weighted mean was calculated (see Equation (1)). Specifically, when proactive detection was directly possible (✔: data value x_i=1.0), the weight (w_i) was set to 1.0. This is because direct detection has the most significant impact and should be fully reflected. Conversely, when proactive detection was difficult (✖: data value x_i=0.0), the weight (w_i) was set to 0.0. Finally, when proactive detection was indirectly possible (▲: data value x_i=0.5), the weight (w_i) was set to 0.5. This represents a midpoint between direct detection (✔) and difficult detection (✖), as indirect detection has a partial influence. The average values calculated in Section 4.2.2 and beyond were also determined using the weighted mean method.

$$X_w = \frac{\sum w_i x_i}{\sum w_i} \tag{1}$$

X_w: Weighted mean, x_i: Each data value (1.0, 0.5, 0.0), w_i : Corresponding weight (1.0, 0.5, 0.0)

As a result, the weighted average values are shown in the bottom row of Table 2. Furthermore, Fig. 5 presents the weighted average results for each element of the Fraud Pentagon Theory using a radar chart. A radar chart makes it easier to visually grasp the balance among the five elements and identify characteristic biases. For single sensors, the detection rates for Motivation (0.62) and Capability (0.70) are relatively high, suggesting that signs of fraud can be partially detected. On the other hand, Opportunity (0.38) and Rationalization (0.50) remain at moderate detection levels, while Arrogance (0.19) is particularly difficult to detect. These results indicate that combining multiple sensors may enable more accurate proactive fraud detection.

Table 2: Verification of proactive fraud detection feasibility with a single sensor

No	Single Sensor	Fraud Pentagon Theory									
		Pressure	Weight	Opportunity	Weight	Rationalization	Weight	Arrogance	Weight	Capability	Weight
1.1.1	Weather Sensor	0.5	0.5	1	1	0.5	0.5	0	0	0	0
1.1.2	Acoustic Sensor	0.5	0.5	1	1	0.5	0.5	0	0	0	0
1.1.3	Light and Darkness Sensor	1	1	1	1	0.5	0.5	0	0	0	0
1.1.4	Air Quality Sensorr	1	1	1	1	0.5	0.5	0	0	0	0
1.1.5	Human Presence Sensor	0.5	0.5	1	1	0.5	0.5	0	0	0	0
1.2.1	Body Temperature Sensor	0.5	0.5	0	0	0	0	0	0	0.5	0.5
1.2.2	Blood Pressure Sensor	0.5	0.5	0	0	0	0	0	0	0.5	0.5
1.2.3	Heart Rate Sensor	0.5	0.5	0	0	0	0	0	0	0.5	0.5
1.2.4	Facial Expression Sensor	0.5	0.5	0	0	0	0	0	0	1	1
1.2.5	Motion Sensor	0.5	0.5	1	1	0.5	0.5	0	0	0.5	0.5
1.2.6	EEG Sensor	0.5	0.5	0	0	0	0	0	0	0.5	0.5
1.2.7	Iris Sensor	0	0	0	0	0	0	1	1	0	0
1.2.8	Voice Sensor	0.5	0.5	0	0	0	0	0	0	1	1
1.3.1	Magnetic Sensor	0.5	0.5	0	0	0.5	0.5	1	1	0	0
1.3.2	RFID Tag	0.5	0.5	0	0	0.5	0.5	1	1	0	0
1.4.1	Pressure Sensor	0.5	0.5	0	0	0	0	0	0	0.5	0.5
Weighted mean		0.62		0.38		0.50		0.19		0.70	

Note: 1.0 (Directly detectable), 0.5（Indirectly detectable), 0 (Difficult to detect)

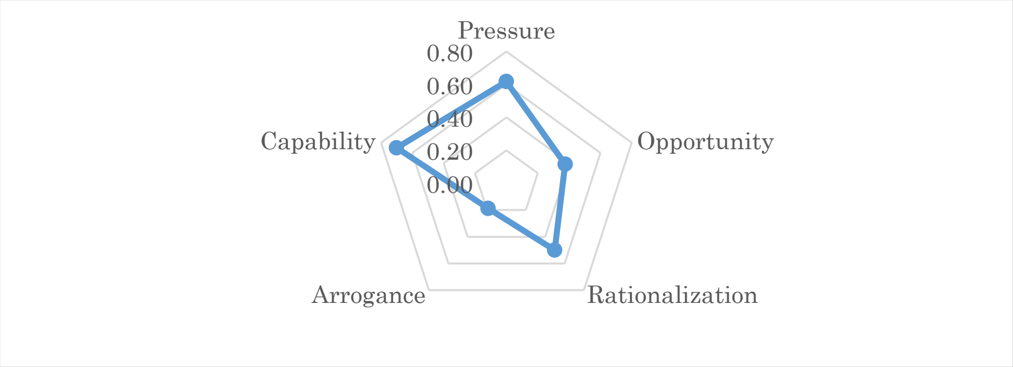


Figure 5: Average proactive detection rate with a single sensor

4.2.2 Case of a Dual-Sensor Combination

In general, when multiple sensors within the same category—such as authentication data, environmental data, biometric data, and operational data, as shown in Fig. 3(b)—are combined, the detectable range for each element of the Fraud Pentagon Theory tends to be similar for each type of data. Therefore, as shown in Fig. 6, the dual-sensor combinations were designed to integrate sensors from different categories. For selecting the sensor combinations, an initial examination was conducted on the basis of subjective discussions among ourselves, considering which combinations would be suitable for acquiring UX data. As a result, nine different sensor combinations were identified, as shown in Fig. 6.

Using these UX data, we evaluated the feasibility of proactive internal fraud detection for the five elements of the Fraud Pentagon Theory. Specifically, as shown in Table 3, we assessed whether each of the five elements could be detected using a dual-sensor combination, on the basis of discussions among ourselves.

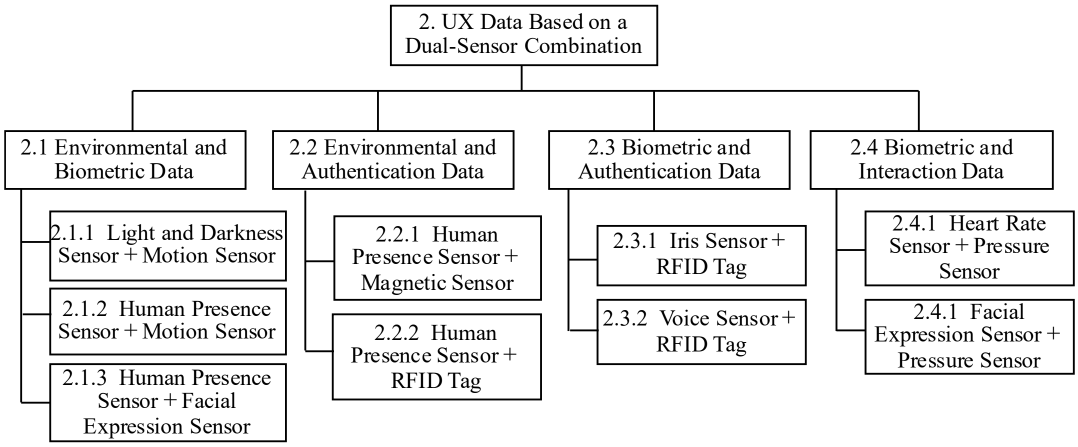

2. UX Data Based on a Dual-Sensor Combination
2.1 Environmental and Biometric Data
2.1.1 Light and Darkness Sensor＋Motion Sensor
2.1.2 Human Presence Sensor＋Motion Sensor
2.1.3 Human Presence Sensor＋Facial Expression Sensor
2.2 Environmental and Authentication Data
2.2.1 Human Presence Sensor＋Magnetic Sensor
2.2.2 Human Presence Sensor＋RFID Tag
2.3 Biometric and Authentication Data
2.3.1 Iris Sensor＋RFID Tag
2.3.2 Voice Sensor＋RFID Tag
2.4 Biometric and Interaction Data
2.4.1 Heart Rate Sensor＋Pressure Sensor
2.4.1 Facial Expression Sensor＋Pressure Sensor

Figure 6: List of UX data selected for dual-sensor combinations

Table 3: Verification of proactive fraud detection with a dual-sensor combination

2.1.1 Light and Darkness Sensor＋Motion Sensor		
Fraud Pentagon Theory	Sensors Detectability for Fraud Triangle Elements	Detectability
① Pressure	If the working environment is excessively bright or dark and there are no other people nearby, it can be detected as a motivation for fraudulent behavior. (This can be detected by acquiring illuminance data from the working environment.)	▲
② Opportunity	If the illuminance in the working environment is inappropriate, it can be detected as an opportunity for fraudulent behavior [20]. (This can be detected by acquiring illuminance data from the working environment. Additionally, it has been pointed out that a dark working environment can be a factor that facilitates fraudulent behavior [22].)	✔
③ Rationalization	Thoughts such as "It's the company's fault for not improving the environment" or "It can't be helped" can be detected as Rationalization for fraudulent behavior. (This can be detected by acquiring illuminance data from the working environment; for example, when a dark working environment persists.)	▲
④ Arrogance	Even if illuminance, the location of people, and the number of people in the working environment are acquired, it is not possible to detect the status, position, or capability of the user operating the UI.	✖
⑤ Capability	If a user exhibits suspicious movements in a dark working environment, their arrogance can be detected. (This can be detected by acquiring illuminance data from the working environment and tracking changes in the user's movements while operating the UI.)	✔

(Note) ✔ (1.0): Directly detectable ▲ (0.5): Indirectly detectable ✖ (0.0): Difficult to detect

As a result of conducting the same analysis on the remaining eight types of dual-sensor combinations, we obtained the results shown in Table 4 (No. 1–9). On the basis of this analysis, Fig. 7 presents the weighted average proactive internal fraud detection rates for each of the five elements of the Fraud Pentagon using dual-sensor combinations. By utilizing dual-sensor combinations, the detection rates for Opportunity (0.92) and Capability (0.95) significantly improved, suggesting that this approach effectively identifies environments that facilitate fraudulent behavior and assesses execution capability. On the other hand, the detection rates for Motivation (0.50) and Rationalization (0.50) showed no significant changes, indicating that additional sensors or different types of data are required to identify these elements. Overall, using dual-sensor combinations is considered particularly effective in identifying fraudulent opportunities and capabilities.

Table 4: Verification of proactive fraud detection feasibility with a dual-sensor combination

No	Dual-Sensor Combination	Fraud Pentagon Theory									
		Pressure	Weight	Opportunity	Weight	Rationalization	Weight	Arrogance	Weight	Capability	Weight
2.1.1	Light and Darkness Sensor + Motion Sensor	0.5	0.5	1	1	0.5	0.5	0	0	1	1
2.1.2	Human Presence Sensor + Motion Sensor	0.5	0.5	1	1	0.5	0.5	0	0	1	1
2.1.3	Human Presence Sensor + Facial Expression Sensor	0.5	0.5	1	1	0.5	0.5	0	0	1	1
2.2.1	Human Presence Sensor + Magnetic Sensor	0.5	0.5	1	1	0.5	0.5	1	1	0	0
2.2.2	Human Presence Sensor + RFID Tag	0.5	0.5	1	1	0.5	0.5	1	1	0	0
2.3.1	Iris Sensor + RFID Tag	0.5	0.5	0.5	0.5	0.5	0.5	1	1	0	0
2.3.2	Voice Sensor + RFID Tag	0.5	0.5	0.5	0.5	0.5	0.5	1	1	1	1
2.4.1	Heart Rate Sensor + Pressure Sensor	0.5	0.5	0	0	0.5	0.5	0	0	0.5	0.5
2.4.2	Facial Expression Sensor + Pressure Sensor	0.5	0.5	0	0	0	0	0	0	1	1
Weighted mean		0.50		0.92		0.50		0.44		0.95	

Note: 1.0 (Directly detectable), 0.5 (Indirectly detectable), 0 (Difficult to detect)

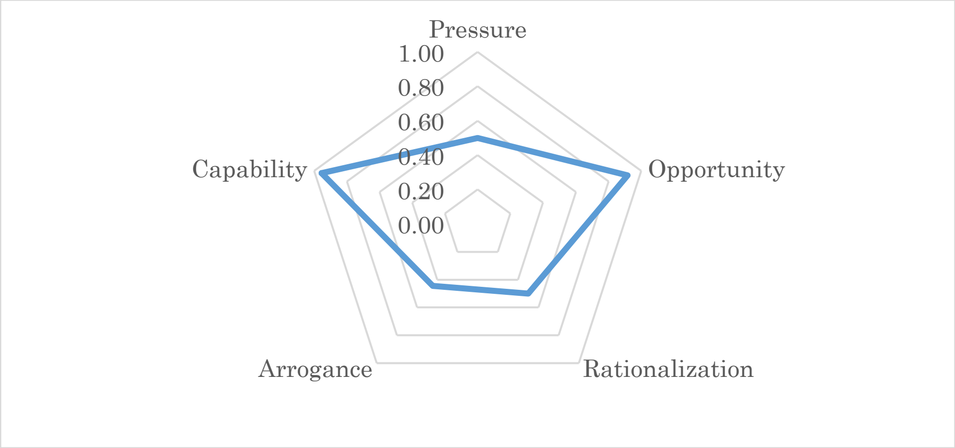


Figure 7: Average proactive detection rate with a dual-sensor combination

4.2.3 Case of a Triple-Sensor Combination

As in Section 4.2.2, the triple-sensor combinations were designed to integrate sensors from three different categories. Additionally, on the basis of subjective discussions among ourselves, we conducted an initial examination to select combinations that were considered suitable for acquiring UX data. As a result, eight different sensor combinations were identified, as shown in Fig. 8. Using these UX data, we evaluated the feasibility of proactive internal fraud detection for the five elements of the Fraud Pentagon Theory. Specifically, as shown in Table 5, we assessed whether each of the five elements could be detected using a triple-sensor combination, on the basis of discussions among ourselves.

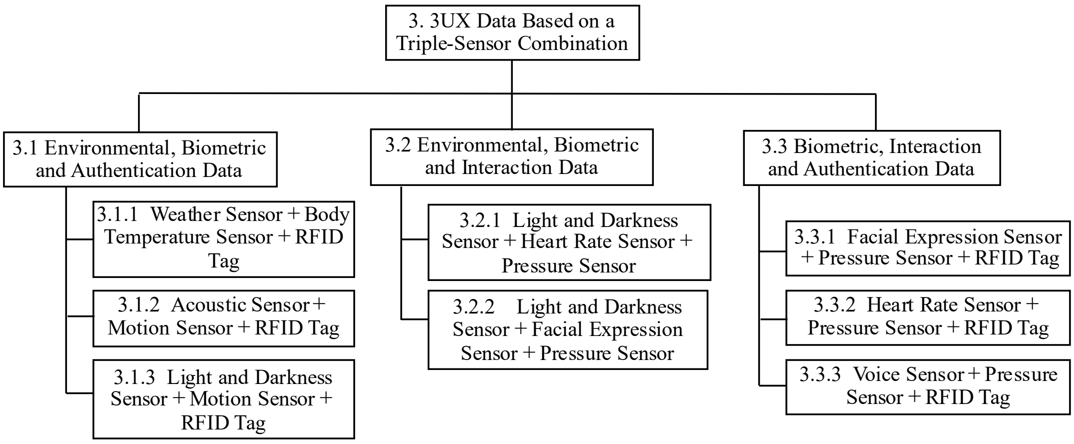

3. 3UX Data Based on a Triple-Sensor Combination
3.1 Environmental, Biometric and Authentication Data
3.1.1 Weather Sensor + Body Temperature Sensor + RFID Tag
3.1.2 Acoustic Sensor + Motion Sensor + RFID Tag
3.1.3 Light and Darkness Sensor + Motion Sensor + RFID Tag
3.2 Environmental, Biometric and Interaction Data
3.2.1 Light and Darkness Sensor + Heart Rate Sensor + Pressure Sensor
3.2.2 Light and Darkness Sensor + Facial Expression Sensor + Pressure Sensor
3.3 Biometric, Interaction and Authentication Data
3.3.1 Facial Expression Sensor + Pressure Sensor + RFID Tag
3.3.2 Heart Rate Sensor + Pressure Sensor + RFID Tag
3.3.3 Voice Sensor + Pressure Sensor + RFID Tag

Figure 8: List of UX data selected for triple-sensor combinations

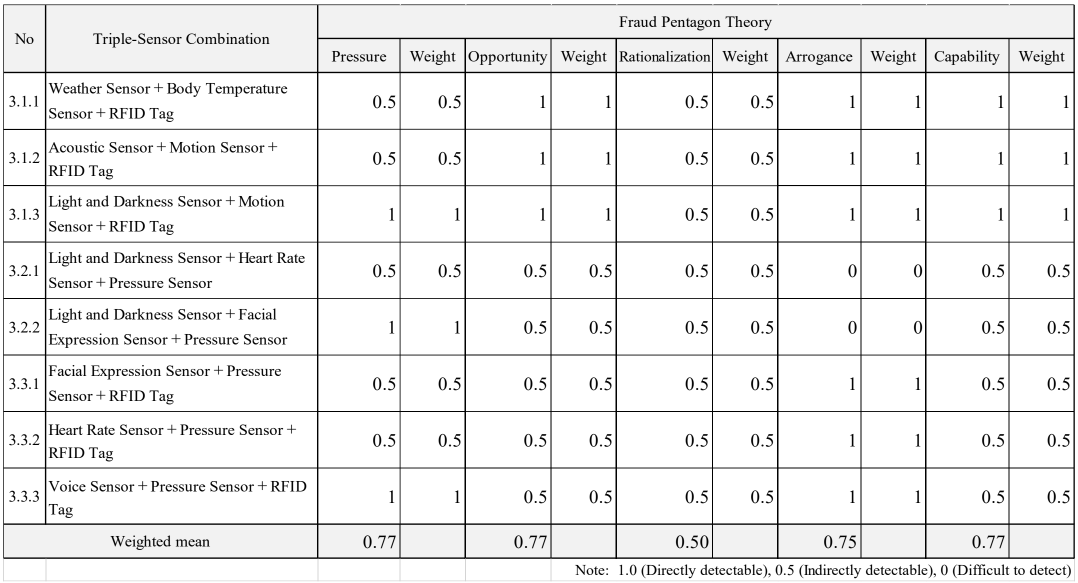
Table 5: Verification of proactive fraud detection with a triple-sensor combination

3.1.1 Weather Sensor＋Body Temperature Sensor＋RFID Tag		
Fraud Pentagon Theory	Sensors Detectability for Fraud Triangle Elements	Detecta-bility
① Pressure	If the working environment is excessively hot or cold, it can be detected as a motivation for fraudulent behavior. (This can be detected by acquiring data such as room temperature in the working environment.)	▲
② Opportunity	If the room temperature in the working environment deviates from the appropriate range, it can be detected as an opportunity for fraudulent behavior. Here, the "appropriate temperature" is defined based on the Office Sanitation Standards Regulation of Japan's Ministry of Health, Labour and Welfare, referring to a state where the room temperature in the working environment falls outside the range of 18 to 28°C [21]. (This can be detected by acquiring data such as room temperature in the working environment.)	✔
③ Rationalization	Thoughts such as "It is the company's fault for not improving the environment or working conditions" or "It can't be helped" can be detected as Rationalization for fraudulent behavior. (This can be detected by acquiring room temperature data or monitoring unauthorized access to restricted areas.)	▲
④ Arrogance	By monitoring access to locations where only authorized personnel are allowed, it is possible to detect the user's status, position, and capability to commit fraudulent acts.	✔
⑤ Capability	A user's arrogance, such as a tendency to be easily angered, can be detected as a capability to commit fraudulent acts. (This can be detected by acquiring the user's body temperature while operating the UI and combining it with employee authentication using IC tags. For example, a significantly higher-than-normal body temperature may indicate such behavior.)	✔

(Note) ✔ (1.0): Directly detectable ▲ (0.5): Indirectly detectable ✕ (0.0): Difficult to detect

As a result of conducting the same analysis on the remaining seven types of triple-sensor combinations, we obtained the results shown in Table 6 (No. 1–8). On the basis of this analysis, we calculated the weighted average proactive internal fraud detection rates for each of the five elements of the Fraud Pentagon when using triple-sensor combinations. The results are presented in the bottom row of Table 6 and in Fig. 9. By utilizing triple-sensor combinations, the detection rates for Motivation (0.77), Opportunity (0.77), Arrogance (0.75), and Capability (0.77) improved overall, suggesting that a broader range of fraudulent behavior indicators can be captured. On the other hand, the detection rate for Rationalization (0.50) remained unchanged from the dual-sensor combination, indicating that additional information may be required to accurately capture this element. Overall, using triple-sensor combinations is effective in detecting multiple aspects of fraudulent behavior, enabling a more comprehensive analysis.

Table 6: Verification of proactive fraud detection feasibility with a triple-sensor combination



No	Triple-Sensor Combination	Fraud Pentagon Theory									
		Pressure	Weight	Opportunity	Weight	Rationalization	Weight	Arrogance	Weight	Capability	Weight
3.1.1	Weather Sensor + Body Temperature Sensor + RFID Tag	0.5	0.5	1	1	0.5	0.5	1	1	1	1
3.1.2	Acoustic Sensor + Motion Sensor + RFID Tag	0.5	0.5	1	1	0.5	0.5	1	1	1	1
3.1.3	Light and Darkness Sensor + Motion Sensor + RFID Tag	1	1	1	1	0.5	0.5	1	1	1	1
3.2.1	Light and Darkness Sensor + Heart Rate Sensor + Pressure Sensor	0.5	0.5	0.5	0.5	0.5	0.5	0	0	0.5	0.5
3.2.2	Light and Darkness Sensor + Facial Expression Sensor + Pressure Sensor	1	1	0.5	0.5	0.5	0.5	0	0	0.5	0.5
3.3.1	Facial Expression Sensor + Pressure Sensor + RFID Tag	0.5	0.5	0.5	0.5	0.5	0.5	1	1	0.5	0.5
3.3.2	Heart Rate Sensor + Pressure Sensor + RFID Tag	0.5	0.5	0.5	0.5	0.5	0.5	1	1	0.5	0.5
3.3.3	Voice Sensor + Pressure Sensor + RFID Tag	1	1	0.5	0.5	0.5	0.5	1	1	0.5	0.5
Weighted mean		0.77		0.77		0.50		0.75		0.77	

Note: 1.0 (Directly detectable), 0.5 (Indirectly detectable), 0 (Difficult to detect)

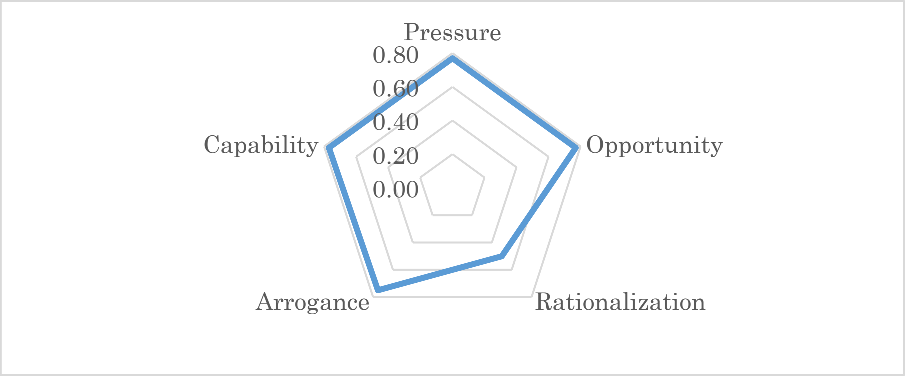


Figure 9: Average proactive detection rate with a triple-sensor combination

4.2.4 Case of a Quad-Sensor Combination

As in Section 4.2.2, the quad-sensor combinations were designed to integrate sensors from four different categories, as shown in Fig. 10. Additionally, on the basis of subjective discussions among ourselves, we conducted an initial examination to select combinations that were considered suitable for acquiring UX data. As a result, six different sensor combinations were identified, as shown in Fig. 10. Using these UX data, we evaluated the feasibility of proactive internal fraud detection for the five elements of the Fraud Pentagon Theory. Specifically, as shown in Table 7, we examined whether each of the five elements could be detected using a quad-sensor combination, on the basis of discussions among ourselves.

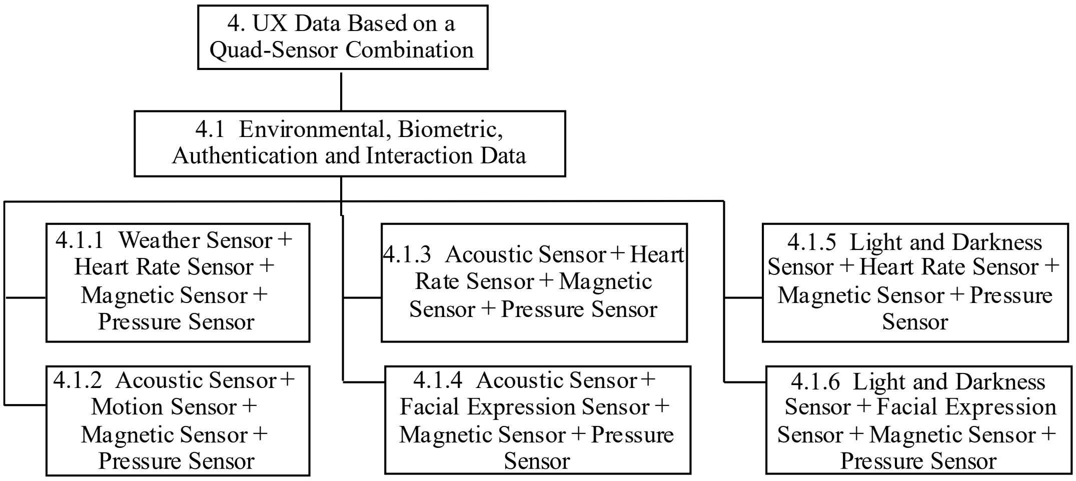

4. UX Data Based on a Quad-Sensor Combination
4.1 Environmental, Biometric, Authentication and Interaction Data
4.1.1 Weather Sensor + Heart Rate Sensor + Magnetic Sensor + Pressure Sensor
4.1.2 Acoustic Sensor + Motion Sensor + Magnetic Sensor + Pressure Sensor
4.1.3 Acoustic Sensor + Heart Rate Sensor + Magnetic Sensor + Pressure Sensor
4.1.4 Acoustic Sensor + Facial Expression Sensor + Magnetic Sensor + Pressure Sensor
4.1.5 Light and Darkness Sensor + Heart Rate Sensor + Magnetic Sensor + Pressure Sensor
4.1.6 Light and Darkness Sensor + Facial Expression Sensor + Magnetic Sensor + Pressure Sensor

Figure 10: List of UX data selected for quad-sensor combinations

Table 7: Verification of proactive fraud detection with a quad-sensor combination

4.1.1 Weather Sensor＋Heart Rate Sensor＋Magnetic Sensor＋Pressure Sensor		
Fraud Pentagon Theory	Sensors Detectability for Fraud Triangle Elements	Detecta-bility
① Pressure	If a user is working in a restricted-access area, the working environment temperature is inappropriate, their heart rate is elevated, and their typing intensity is strong, it can be detected as a motivation for fraudulent behavior. (This can be detected by acquiring meteorological data from the working environment, heart rate, and changes in typing intensity.)	✓
② Opportunity	If the working environment temperature is inappropriate and the user has access to a restricted area, it can be detected as an opportunity for fraudulent behavior.	✓
③ Rationalization	Thoughts such as "It is the company's fault for not improving the environment or working conditions" or "It can't be helped" can be detected as Rationalization for fraudulent behavior. (This can be detected by acquiring temperature data from the working environment and measuring changes in heart rate and typing intensity.)	▲
④ Arrogance	By monitoring entry and exit in areas restricted to authorized personnel, it is possible to detect the user's status, position, and capability to commit fraudulent acts.	✓
⑤ Capability	A user's arrogance, such as dissatisfaction with the current situation or a tendency to be displeased with certain conditions, can be detected. (This can be detected by measuring changes in heart rate and typing intensity while operating the UI, as well as acquiring temperature data from the working environment.)	▲

(Note) ✓ (1.0): Directly detectable ▲ (0.5): Indirectly detectable ✕ (0.0): Difficult to detect

As a result of conducting the same analysis on the remaining five types of quad-sensor combinations, we obtained the results shown in Table 8 (No. 1–6). On the basis of this analysis, we calculated the detection rates for each of the five elements of the Fraud Pentagon when using quad-sensor combinations. The results are presented in the bottom row of Table 8 and in Fig. 11. By utilizing quad-sensor combinations, the detection rate for Arrogance (1.00) reached its maximum, suggesting that signs of attitudes and behaviors that justify fraudulent acts can be captured more accurately. Additionally, Motivation (0.90) and Opportunity (0.90) also exhibited high detection rates, indicating the potential for a comprehensive analysis of factors leading to fraud. On the other hand, the detection rate for Rationalization (0.50) remained unchanged from the triple-sensor combination, highlighting the continued need for supplementary data. Overall, while quad-sensor combinations contribute to highly accurate fraud detection, the balance with additional costs needs to be considered.

Table 8: Verification of proactive fraud detection feasibility with a quad-sensor combination

No	Quad-Sensor Combination	Fraud Pentagon Theory									
		Pressure	Weight	Opportunity	Weight	Rationalization	Weight	Arrogance	Weight	Capability	Weight
4.1.1	Weather Sensor + Heart Rate Sensor + Magnetic Sensor + Pressure Sensor	1	1	1	1	0.5	0.5	1	1	0.5	0.5
4.1.2	Acoustic Sensor + Motion Sensor + Magnetic Sensor + Pressure Sensor	0.5	0.5	1	1	0.5	0.5	1	1	1	1
4.1.3	Acoustic Sensor + Heart Rate Sensor + Magnetic Sensor + Pressure Sensor	1	1	1	1	0.5	0.5	1	1	0.5	0.5
4.1.4	Acoustic Sensor + Facial Expression Sensor + Magnetic Sensor + Pressure Sensor	1	1	1	1	0.5	0.5	1	1	1	1
4.1.5	Light and Darkness Sensor + Heart Rate Sensor + Magnetic Sensor + Pressure Sensor	0.5	0.5	0.5	0.5	0.5	0.5	1	1	0.5	0.5
4.1.6	Light and Darkness Sensor + Facial Expression Sensor + Magnetic Sensor + Pressure Sensor	1	1	0.5	0.5	0.5	0.5	1	1	0.5	0.5
Weighted mean		0.90		0.90		0.50		1.00		0.75	

Note: 1.0 (Directly detectable), 0.5 (Indirectly detectable), 0 (Difficult to detect)

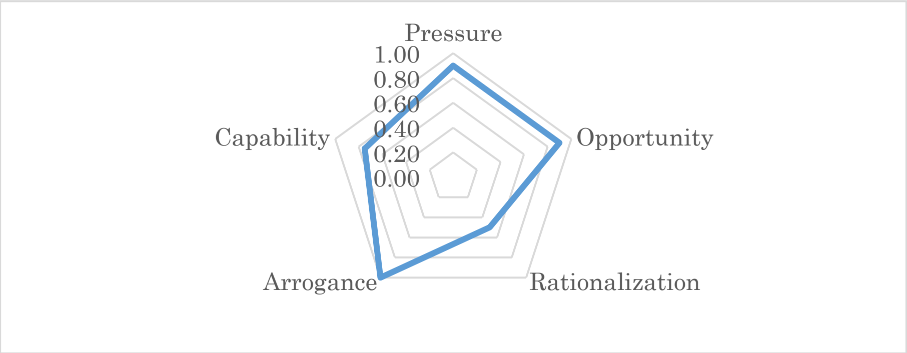


Figure 11: Average proactive detection rate with a quad-sensor combination

4.3 Proactive Internal Fraud Detection Strategies Using UX Data

4.3.1 Summary of Verification Results

The verification results of Section 4.2 are summarized in Table 9 and Fig. 12. Notably, as shown in Table 9, the average prediction detection rate for "Rationalization" consistently remained at 0.50, showing no improvement compared to other elements. This is likely because rationalization strongly depends on individual ethics and values and has a low correlation with the environmental and biometric data that sensors can obtain. More accurate detection will require text and voice analysis, as well as long-term behavioral data being accumulated and compared.

Within the scope of UX data selected in this study, only cumulative UX is related to long-term factors, and the corresponding sensor is limited to typing intensity. Therefore, a future challenge is to develop technologies capable of estimating behavioral pattern changes and stress level fluctuations on the basis of biometric data.

On the other hand, as shown in Table 9, the detection growth rate (e.g., the average detection rate of the dual-sensor combination/the average detection rate of a single sensor = 1.39) for "Opportunity" and "Capability" improved as the number of sensor types increased, with the greatest effect observed when using the dual-sensor combination. The following section provides a detailed analysis of the changes in detection growth rates across different sensor configurations and discusses an optimal sensor utilization strategy.

Table 9: Avg. proactive internal fraud detection and growth rate by number of sensors

No	Number of Sensors	Fraud Pentagon Theory					Evaluation		
		Pressure	Opportunity	Rational-ization	Arrogance	Capability	Avg. Proactive Internal Fraud Detection Rate	Standard Deviation	Detection Growth Rate (Previous Ratio)
1	Single Sensor	0.62	0.38	0.50	0.19	0.70	0.48	0.20	–
2	Dual-Sensor Combination	0.50	0.92	0.50	0.44	0.95	0.66	0.25	1.39
3	Triple-Sensor Combination	0.77	0.77	0.50	0.75	0.77	0.71	0.12	1.07
4	Quad-Sensor Combination	0.90	0.90	0.50	1.00	0.75	0.81	0.19	1.14

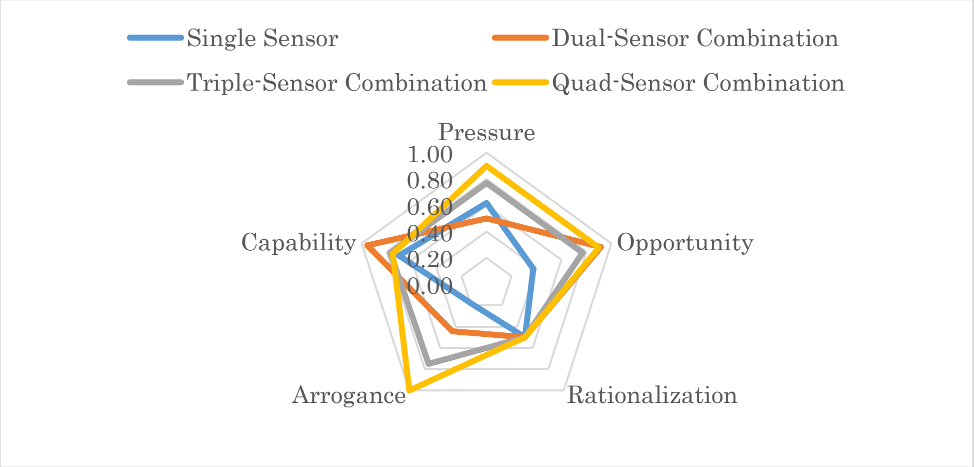


Figure 12: Avg. proactive internal fraud detection rate by number of sensors

4.3.2 Proactive Internal Fraud Detection Strategy Proposals

On the basis of the summary in Section 4.3.1, the following strategies for proactive internal fraud detection are proposed:

(1) **Basic Strategy (Achieving High Effectiveness at Minimal Cost)**: The introduction of a dual-sensor combination is the most cost-effective approach. Transitioning from a single sensor to a dual-sensor combination improves the average prediction detection rate by 1.39 times (detection growth rate in Table 9), demonstrating a significant improvement. In particular, the detection accuracy for "Opportunity" (0.92) and "Capability" (0.95) has markedly improved, making it effective in identifying situations where fraudulent activities are possible.

(2) **High-Precision Strategy (Aiming to Further Improve Accuracy)**: Introducing a triple-sensor combination increases the average prediction detection rate by 1.07 times (detection growth rate in Table 9), with enhanced detection particularly for "Arrogance" (0.75) and "Motivation" (0.77). However, the detection growth rate has slowed (1.07), suggesting that the effectiveness may be limited relative to the additional cost. Therefore,

its implementation should be considered only when high-precision detection is required.

(3) **Maximum-Precision Strategy (Maximizing Detection at a High Cost)**: With a quad-sensor combination, the average detection rate reaches 0.81, as shown in Table 9, with the highest detection accuracy observed for "Arrogance" (1.00), "Motivation" (0.90), and "Opportunity" (0.90). While this enables comprehensive monitoring of fraudulent indicators, the detection growth rate in Table 9 (1.14) has only slightly recovered, and cost efficiency continues to decline. Therefore, careful consideration is required to determine whether the additional investment is justified.

These strategy proposals are characterized by their ability to be implemented incrementally, considering the balance between cost and proactive detection accuracy. In particular, the Basic Strategy offers high cost-effectiveness and serves as a practical option, whereas the Maximum-Precision Strategy enables more comprehensive detection but presents cost-related challenges.

On the basis of these findings, the recommended approach is to first implement the Basic Strategy by introducing dual-sensor combinations, evaluate its effectiveness, and then gradually increase the number of sensors as needed. This step-by-step approach allows for effective internal fraud prevention without imposing an excessive burden.

4.3.3 Discussion

The costs of individual sensors and detection processes remain uncertain, particularly for detection costs, as new software will need to be developed, making precise estimation difficult at this stage. However, assuming that all costs are equal and considering cost-effectiveness, the dual-sensor combination emerges as the optimal choice under current conditions. The detection growth rate of the average prediction detection rate is the highest among the evaluated configurations (detection growth rate in Table 9: 1.39 times), and the detection accuracies of "Opportunity" (0.92) and "Capability" (0.95) are also improved.

On the other hand, the accuracy gains from introducing three or more sensors are limited, and such configurations should only be considered when higher detection precision is required. While quad-sensor combinations offer maximum detection performance, the trade-off with additional costs needs to be carefully evaluated.

5 Conclusion and Future Work

In this paper, we proposed a sensor-based strategy for preventing internal fraud in user experience (UX) environments. Specifically, we explored a method to transition from single sensors to multiple-sensor combinations, utilizing the resulting data as UX data. This approach enables real-world information to be analyzed as virtual UX data through sensors. Furthermore, we applied these UX data to the five elements of the Fraud Pentagon Theory and theoretically analyzed their detectability.

As a key finding, this study revealed that additional sensors need to be integrated in UX environments for proactively detecting signs of intentional internal fraud. In particular, combining multiple sensors was demonstrated to improve detection accuracy. Considering cost-effectiveness, dual-sensor combinations were identified as the optimal configuration.

However, the detection rate for Rationalization consistently remained low, highlighting the challenge of capturing this element using sensor data alone. To achieve higher detection accuracy, complementary approaches need to be introduced, such as text and speech analysis and the long-term accumulation and comparison of behavioral patterns. Addressing this limitation remains an important direction for future work.

References

[1] Ministry of Internal Affairs and Communications, Information and Communications White Paper, 2021 Edition, (in Japanese), https://onl.sc/p6rAUnF

[2] IPA, Top 10 Information Security Threats, 2023, (In Japanese), https://onl.sc/9H12WSd

[3] IPA, Guidelines for Preventing Insider Fraud in Organizations, (in Japanese), https://www.ipa.go.jp/files/000097099.pdf

[4] IPA, Report on the Actual State of Information Security Incidents Caused by Insider Fraud, (in Japanese), https://www.ipa.go.jp/files/000051135.pdf

[5] Ponemon Institute, Cost of Insider Threats: Global Report, 2022, (in Japanese), https://onl.sc/ckixdKW

[6] T. Sekiguchi et al., Risk Assessment of Secure UX Environments Contributing to Error Prevention, Spring Research Presentation of the Society of Project Management, pp.467-474, 2023, (in Japanese)

[7] Cabinet Office, Third Survey on Changes in Awareness and Behavior under the Impact of COVID-19, (in Japanese), htps://www5.cao.go.jp/keizai2/wellbeing/covid/pdf/result3_covid.pdf,

[8] IPA, Report on the Actual State of Internal Fraud Prevention Systems in Companies, (in Japanese), https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html

[9] Cressey, D. R. (1953) Other people's money: A study in the social psychology of embesslement, NY: The Free Press.

[10] H. Kitano, A Study on the Prevention of Insider Fraud in Japanese Management, (in Japanese), http://lab.iisec.ac.jp/degrees/d/theses/iisec_d29_thesis.pdf

[11] A. P. Singh, et al., A systematic literature review on insider threats, Cornell University arXiv, Cryptography and Security, 2022, DOI: https://doi.org/10.48550/arXiv.2212.05347

[12] D. Maimon, et al., Insider Threat Detection: A Solution in Search of a Problem, 2020 International Conference on Cyber Security and Protection of Digital Services, 2020, DOI: https://doi.org/10.1109/CyberSecurity49315.2020.9138862

[13] N. Mehrnezhad, et al., A Multi-Tiered Framework for Insider Threat Prevention, Electronics 2021, 10(9), 1005, DOI: https://doi.org/10.3390/electronics10091005, 2021

[14] J. R. C. Nurse, et al., Understanding Insider Threat: A Framework for Characterising and Identifying Insider Threats in Organisations, 2014 IEEE Security and Privacy Workshops , 2014, DOI: https://doi.org/10.1109/SPW.2014.38

[15] S. Shima, et al., Analysis and Consideration of Work Environments for Incident Prevention

Countermeasure Related to Insider Threat, DICOMO2013, pp.1217-1222, (Japanese Edition), 2013

[16] K. Niihara, A study on incentives to a leakage of information asset caused by malicious insider, Meiji University Ph.D. Thesis 2017, (Japanese Edition), 2018, https://meiji.repo.nii.ac.jp/record/14807/files/niihara_2018_suri.pdf

[17] M. Graham, et al., Developing Visualisations to Enhance an Insider Threat Product: A Case Study, Cornell University arXiv, Human-Computer Interaction, 2021, DOI: https://doi.org/10.48550/arXiv.2109.08445

[18] S. Bertrand, et al., Unsupervised User-Based Insider Threat Detection Using Bayesian Gaussian Mixture Models, Cornell University arXiv, Cryptography and Security, 2022, DOI: https://doi.org/10.48550/arXiv.2211.14437

[19] V. Roto, et al., USER EXPERIENCE WHITE PAPER, 2011, https://experienceresearchsociety.org/wp-content/uploads/2023/01/UX-WhitePaper.pdf

[20] Japan Science and Technology Agency (JST), Sensor Fusion Platform Technology Enabling Acquisition and Integrated Processing of Diverse Data, Science and Technology Future Strategy Workshop Report, 2019, (in Japanese), https://www.jst.go.jp/crds/pdf/2019/WR/CRDS-FY2019-WR-09.pdf

[21] Ministry of Health, Labour and Welfare, Office Sanitation Standards Regulation, (in Japanese), https://www.mhlw.go.jp/web/t_doc?dataId=74089000&dataType=0&pageNo=1

[22] Zhong, C. B., Bohns, V. K., & Gino, F. (2010). Good lamps are the best police: Darkness increases dishonesty and self-interested behavior. Psychological Science, 21(3), 311-314