Access to resources by users may need to be granted only upon certain conditions and contexts, perhaps particularly in cyber-physical settings. Unfortunately, creating and modifying context-sensitive access control solutions in dynamic environments creates ongoing challenges to manage the authorization contexts. This article proposes RASA, a context-sensitive access authorization approach and mechanism leveraging unsupervised machine learning to automatically infer risk-based authorization decision boundaries. We explore RASA in a healthcare usage environment, wherein cyber and physical conditions create context-specific risks for protecting private health information. The risk levels are associated with access control decisions recommended by a security policy. A coupling method is introduced to track coexistence of the objects within context using frequency and duration of coexistence, and these are clustered to reveal sets of actions with common risk levels; these are used to create authorization decision boundaries. In addition, we propose a method for assessing the risk level and labelling the clusters with respect to their corresponding risk levels. We evaluate the promise of RASA-generated policies against a heuristic rule-based policy. By employing three different coupling features (frequency-based, duration-based, and combined features), the decisions of the unsupervised method and that of the policy are more than 99% consistent.

CCS Concepts: • Security and privacy → Systems security; Software and application security; Access control; Authorization; Authentication; • Computing methodologies → Machine learning;

Additional Key Words and Phrases: Cyber-security, IoT, access control, authentication, machine learning

ACM Reference format:
Jinxin Liu, Murat Simsek, Burak Kantarci, Melike Erol-Kantarci, Andrew Malton, and Andrew Walenstein. 2022. Risk-aware Fine-grained Access Control in Cyber-physical Contexts. Digit. Threat.: Res. Pract. 3, 4, Article 43 (December 2022), 29 pages. https://doi.org/10.1145/3480468

1 INTRODUCTION

Whether access should be granted to a resource may depend upon the context in which the access is attempted, including the cyberphysical context. For example, a physician may have a legitimate need to access a patient’s private health information (PHI) on a mobile display screen while in a private consultation room, but it might be important to lock out the access if the physician wheels the display into the hallway, or if a different patient is moved into the shared room. Failure to lock out could lead to leaking PHI to other people whom the patient
has not consented to allow access to. In such cases the identity of the accessing physician has not changed, nor has the physician’s role changed with respect to the patient. The concern is thus unrelated to authentication and static user roles. Instead, it is an issue of context-dependent or context-sensitive authorization.

Recently, context-aware security approaches have gained significant attention, and there have been several studies around inferring and understanding contexts. But even state-of-the-art access control mechanisms for cyber-physical systems may lack the generality or flexibility desired to confine access authorization to dynamic cyberphysical context, or they otherwise burden the access policy administrators with having to tediously and continuously define every context, set the appropriate access restrictions, and understand the resulting policy well enough to assess the residual risks left by the policy. For example, methods for defining geofences may be used to define physical contexts for defining context-dependent access policy, but many geofencing access policies utilize geofences only for authorization decisions, and physical location is one contextual factor affecting authorization risks. For example, a phone may lock when moved out of its “home” geofence, but unlocking restores all prior access; it is only used for context-dependent authentication.

A general framework and approach is required for effective context-dependent authorization policy management. Core concerns in any such context-dependent authorization regime is defining the contexts in which authorization decisions differ, identifying and quantifying risks for those contexts, and then using the derived risk model to create appropriate access control decisions. Given that contexts may change over time, an additional burden is tracking these changing contexts over time. A problem that is not yet well addressed are effective methods for automatically helping define and maintain context-dependent authorization policies, i.e., inferring the contexts, risk models, and access decision boundaries.

This article introduces a framework named Risk-Aware Smart Access (RASA) to learn authentication policies from examples of routine access. RASA begins with the observation that if, in normal practice, responsible actors access information they have ordinary access to only in those contexts in which they need access, and that they take care to guard against known risks. In such cases, even if an existing access control policy is not context-sensitive, responsible actors effectively fill in the missing contextual access conditions through their choices and actions, and these can be used to infer a baseline context-dependent access control policy. In a sense, they can program the context-dependent access conditions by demonstration. RASA uses coupling of access actions to identify patterns of access, clusters the actions, associates these coupling-defined features to risk scores, and then defines access boundaries based simply on these risk scores. To the best of our knowledge, no prior work exists for similar automated policy inference based on mapping-inferred contexts onto risk levels.

The article evaluates the general promise of the approach in a simulated in-person healthcare environment. This use context is cyberphysical, and one where ensuring strong access boundaries—even for fully authenticated users—are critical for protecting sensitive PHI. Nearly 90% of participants, in a health care survey reported by the Ponemon Institute, have been affected by data leakage in the past three years [22]. Furthermore, inappropriate use of devices that handle sensitive documents by internal employees has led to the breach of 4.5M patient records in 2015 [14]. Intelligent approaches to such security may be increasingly important [30], and not all risks are due to remote attackers—shoulder surfing in a shared patient room, for example. The context-dependent appropriateness of PHI access serves as a suitable test of cyberphysical context dependencies.

The article is organized as follows: In Section 2, the related work and motivation are presented. In Section 3, we present our proposed framework in detail. Section 4 presents the numerical results of three different coupling mechanisms and clustering algorithms along with comprehensive discussions. Section 5 concludes the article and provides future directions.

2 BACKGROUND, RELATED WORK, AND MOTIVATION

Some traditional authentication schemes, such as passwords or pin codes, can be inconvenient for some users. They also have well-known limitations to their effective security; for example, passwords set by mobile users can be determined by simple guessing [1], inferred from smudges left on users’ screens [5], or stolen by malware [6].
These concerns have led to plentiful prior work in cyber-physical context-dependencies for access control that has applied context dependency to multi-factor authentication, location-aware access control, and implicit or continuous authentication.

Multi-factor authentication establishes likely identity of users based on at least two pieces of evidences of identity, making identity assessment dependent upon multiple possibly-contextual factors. Commonly, the factors relate to a users’ unique knowledge (such as a private password), and physical possessions (something that is only in possession of the user such as a SecureID token). Common also is adding physical location to the authentication through definitions of geofences, such as a defined “home” location. Ramatsakane et al. [33] utilized location for improving location determination for authentication purposes.

So-called “implicit” authentication that extends multi-factor one-time authentication could be more usable and secure [12, 24]. State-of-the-art in context-aware access control calls for a system for continuous authentication that factors contextual risk into the continuous authentication in addition to other risks, such as the risk that the user is not who they appear to be, or that the resource being accessed is more sensitive than another [31]. Thanks to the rapid advancement of the Internet of Things (IoT), sensors can be utilized for easy-to-use additional access safeguards, such as through contextual, behavioral, and biometric signatures [32]. In particular, IoT devices and networks may be effective in recognizing certain context, as in the case of using sensors, communication, and data (i.e., storage and analytics) as keys to IoT-based smart systems [16]. As Habibzadeh et al. [17] note, security is increasingly critical in smart access systems. Significant work on behavioral authentication has been published recently using a growing list of features collected through sensors including, but not limited to: smartphone touchscreens, wearables, and keystrokes [9, 38, 39].

Ashibani et al. [3] propose a framework that aims to reduce user intervention in access control by identifying the behavioral patterns about user-device interaction, such as service request and login duration. Rule-based behavior analysis aims for resiliency against password misuse, brute-force attacks, and unauthorized modification. Rauen et al. [35] proposed a primary-backup fashion to manage access control on smart mobile devices by using several machine learning algorithms that run on gestural information and spatiotemporal knowledge extracted from sessions on various applications. Thus, once the primary authentication module fails to authenticate a user (or fails to recognize a behavioral pattern), the backup module is activated. In case both primary and backup modules fail to authenticate a user implicitly, multi-factor authentication is triggered. Wu et al. [42] apply Support Vector Machines (SVMs) to classify genuine users as well as adversaries from keystroke signals. Lima et al. [28] introduced an architecture for behavioral data acquisition and presented a behavior model with the building blocks of events, context, action, and behavior. The architecture utilizes a belief analyzer and a recommendation filter to discover anomalous behavior and uncover hidden behavioral patterns. In addition to these, a probability analyzer is proposed to serve as a classifier that outputs three categories: normal, suspicious, and abnormal. Hayashi et al. [18] proposed a framework named Context-Aware Scalable Authentication (CASA) to make a tradeoff between security and usability. In addition to multiple factors that contribute to a context, the authors report that location is the most influential factor on the context. Lee [27] introduced a new continuous authentication system called “SmarterYou” to integrate the data from smart phone with wearable sensors. The proposed system builds on data analytics on these features in both time and frequency domains to ensure fine-grained authentication. Flexibility is another important aspect to address in smart access control research, as it can potentially compromise security. To address this challenge, Hulsebosch et al. [21] provide a secure and flexible access control scheme that builds on context sensitiveness and historical data analysis in the authorization of anonymous users.

While techniques to recognize behavioral patterns have improved, behavioral authentication still cannot guarantee the complete elimination of false positives [2]. In addition, even if false positives can be solved for authentication, implicit authentication alone cannot solve context-dependent risks that may result in undesired access.

Access control models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) have been investigated.
Table 1. Access Control Schemes Comparison

| Access control scheme | Benefits                                                                 | Limitation                                                                 |
|-----------------------|---------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| MAC                   | High security level; Fine-grained; Attackers cannot share or inherit access to other files | Difficult to maintain and configure; Difficult to scale to a large number of files and users; Users have to request permissions for new files |
| DAC                   | Easy to maintain and configure; User-friendly; Low implementation cost; Flexible | Less secure than MAC; Lack of centralized access management                  |
| RBAC                  | Rules are transparent to users; Ease of use for the administrator; Flexible; Secure but no need to configure access for each user | Complex and laborious configuration of roles; Difficult to extend permission for individual users; Complexity is determined by the number of roles; Discards the principle of least privilege |
| ABAC                  | Dynamically updates access permissions; Less effort after configuration; More control variables than RBAC | Low interpretability for the user; Scalability issues                        |
| Proposed Scheme (RASA)| No configuration; Infer document ownerships automatically; Dynamically adjust access permission according to user’s environment; Identify anomalous actions automatically | Sensitive to surroundings. Not suitable for small number of users, since it is difficult to infer the coupling distributions |

by the researchers in this domain [11]. MAC offers operating system-constrained access control to manage process/thread operating files, network ports, memories, and devices. MAC is widely deployed on Linux, Windows, and databases. Rossi et al. [37] propose a framework that allows developers to establish fine-grained ad hoc MAC strategies for applications, protecting the system from misbehavior (caused by bugs or compromised by attackers) of root-privileged apps. Even though MAC provides high-level protection, it requires users to request permission for every resource. When compared to MAC, DAC is more flexible by allowing users to grant access to other users. Khan et al. [25] apply DAC combined with RBAC to access patient files dynamically. RBAC, unlike MAC and DAC, does not assign access to specific users but to predefined roles. By deploying RBAC, IT administration can operate more efficiently, since RBAC can add or switch roles to cope with personnel changes. Cruz et al. [8] propose RBAC-SC, which utilizes RBAC and smart contracts to implement trans-organizational roles. Unlike static access control strategies, ABAC dynamically determines permissions according to a set of attributes such as user, resource, object, environment attributes. ABAC can achieve various levels of access control according to different requirements and environments in spite of its overhead. Ding et al. [10] propose combining ABAC and blockchain to cope with the massive connectivity of IoT to avoid heavy role-engineering for various devices. As listed in Table 1, compared to the conventional access control schemes, this article focuses on implicit access control, which can identify the user-object association by mining historical data and recognize risky actions according to the current context.

Besides the studies that aim to bridge access control with implicit authentication, identifying and assessing the risks of certain contexts is of paramount importance as well. With this in mind, the authors in Reference [19] define a risk-assessment scheme that associates the risk to the location. Cha et al. [7] introduce a data-driven risk-assessment scheme that uses Data Flow Diagrams (DFDs) to model the flows of individual data and to recognize the components employed to process, store, and transmit data. Organizations can identify the potential/implicit incidences according to the associated components. Compared with asset-oriented and process-oriented
approaches, the proposed approach can enhance the risk-assessment accuracy by avoiding underestimating or neglecting the risks to sensitive individual data. In Reference [23], Khambhammettu et al. propose a framework containing four threat-assessment methods for subject-object accesses. Via assigning different weights to the sensitivity score of data/objects and the trustworthiness score of subjects, the proposed framework is flexible enough to satisfy the various preference of organizations. Wang et al. [40] present a new access control model that quantifies the risk of privacy violation in a statistical approach and further detects the physicians/users who over-access or misuse patients’ private data. Atlam et al. [4] propose a risk estimation model that combines a new fuzzy logic algorithm and a set of rule-based policies to perform access control in IoT systems. To generate accurate and realistic risk values for each access request, the proposed fuzzy logic system, which involves 20 experts’ effort, converts experts’ qualitative expression into numeric values and offers a dynamic and context-aware access control by leveraging the contextual features such as resource sensitivity, action severity, and risk history.

The literature review indicates a gap remains between continuous/implicit authentication/access control and risk-awareness, particularly in cyberphysical environments where actions do not only appear in cyberspace but also stem from physical behaviors, interactions, and roles.

3 RASA: RISK-AWARE SMART ACCESS CONTROL

This section presents the system overview along with the cyber-physical action logs in a medical emergency room. We introduce the data pre-processing steps, feature extraction, and risk inference methods in detail.

In our framework, actions are transformed into events that include contextual information that can be recognized through coupling mechanisms. Coupling defines interaction patterns between the objects, which can be recognized through clustering algorithms, that use couplings as the input features. Each coupling feature is associated to a risk level. Upon obtaining the clusters, an aggregate value of the associated risk levels of the features of all data points (i.e., actions) in a cluster is calculated as the risk value of that cluster, (i.e., label of cluster). Note that couplings can be formulated based on time, frequency, or a combination of time and frequency.

The bold letters in the notation represent collections/sets of factors (Ppl, Dev, Doc, and Loc), and lower-case letters stand for the elements of the specific collection, e.g., $A = \{a_1, \ldots, a_i, \ldots\}$. $A$ and $B$ denote any pair of the four collections/sets. $C$ and $R$ indicate coupling and risk, respectively, and can be denoted in terms of Frequency
Table 2. Action Log Examples

| time       | act | agent   | device | document | location | monitor |
|------------|-----|---------|--------|----------|----------|---------|
| 06-26 19:00 | enter | actor: 35...9d | loc: fe...fb | dev: bd...77 |
| 06-26 20:02 | exit | actor: 50...df | loc: fe...fb | dev: bd...77 |
| 06-26 19:31 | read | dev: ae...2e | doc: 9a...de |

(Freq) and/or Duration (Dur). \( F_n^{A,B} \) denotes the \( n \)th coupling feature extracted (from the \( n \)th event \( E_n \)). More detailed explanations are listed in Table 3.

3.1 System Overview

The overview of the proposed RASA scheme is presented in Figure 1. The use case in this study involves an emergency room of a healthcare organization where sensors record activities of people (i.e., patients and physicians) and devices, such as entering or exiting some locations and reading documents/records (as examples in Table 2). To protect patient privacy and physical security, protection systems should raise alarms or introduce access control levels against hazardous actions, such as a read access to a document by an unfamiliar patient or entering into unfamiliar rooms. The proposed scheme aims to quantify the risk of given actions and find potential threats without prior knowledge (e.g., document ownership, patient wards). Nevertheless, if only the action were considered, then not only the context information would be overlooked but similar actions would be repeated, which might have led to many false alarms. Therefore, in the proposed framework, the first step is to reproduce the events where actions are performed. Then, these events are used for calculating the couplings, which are then clustered and at the same time assigned some risk levels. The risk levels of couplings determine the risk level of a cluster of couplings. Finally, the risk levels of clusters are verified against a pre-defined policy.

An argument for using couplings as features described is as follows: Since the risk level is not only determined by actions but also their context, the actions are initially transformed into events to obtain the surrounding information, e.g., location, and co-presence. The coupling concept (see Section 3.3 for more details) is introduced to infer the relationship of objects in action logs. Coupling values are extracted from events and normalized. These values are stored in coupling matrices to explore their distributions and are marked with high, medium, and low-risk levels according to their mean value and standard deviation. Coupling features are fed into clustering algorithms. In this article, three different coupling features are used: frequency-based features, duration-based features, and a combination of them. A simple scenario that would trigger the RASA framework to compute coupling values is illustrated in Figure 4. One physical action of entering a room and one cyber action of accessing a document on a device is given as an example.

After the computation of couplings, their risk levels, and forming clusters of couplings, the risk of each cluster is calculated based on the number of high, medium, and low labels of couplings in that cluster. Then, the cluster is labeled according to cluster risk value. Furthermore, the risk of the entire action log can be determined by the same calculation to provide the general risk information to the security experts to raise alarm.

In a privacy-sensitive environment such as a clinical setting, the inferred risk context can be utilized to define a rule-based access control policy managing access and defining risk-based system actions based on calculated risk. Given a risk level of a cluster of actions or events, a policy can be defined wherein access decisions are made per read attempt by calculating the overall risk within the current context. RASA estimates overall risk from the weighted sum of all per-feature risk values. Rather than assigning equal weights to the features, the policy author may adjust the weights of these coupling features based on direct inputs from subject matter experts. For instance, when patient documents are the assets considered, the couplings related to documents may be assigned greater weight factors compared to other couplings that do not consider documents. Furthermore, the policy may permit or deny read actions by tuning a threshold value for the risk factor. Although such policy
Table 3. Notations

| Notation   | Description                                                   |
|------------|---------------------------------------------------------------|
| $C_{freq}^{a_i,b_j}$ | Frequency-based Normalized Coupling Values                  |
| $C_{dur}^{a_i,b_j}$  | Duration-based Normalized Coupling Values                    |
| $R_{freq}^{a_i,b_j}$ | Risk of Frequency-based Normalized Coupling Values           |
| $R_{dur}^{a_i,b_j}$  | Risk of Duration-based Normalized Coupling Values            |
| $Freq_{a_i,b_j}$    | Number of times $a_i$ and $b_j$ occur together                |
| $Dur_{a_i,b_j}$      | Duration of the occurrence of $a_i$ and $b_j$                |
| $\delta_{a_i,b_j}(k)$ | Coupling distribution                                         |
| $Ppl$              | Collection of people                                          |
| $Dev$              | Collection of devices                                         |
| $Doc$              | Collection of documents                                       |
| $Loc$              | Collection of locations                                       |
| $A,B$              | Any two of four collections, $Ppl$, $Dev$, $Doc$, or $Loc$  |
| $a_i, b_j$         | Elements from four collections                                |
| $E_k$              | The $k$th event, which is defined as a collection of the elements from various sets |
| $F_{A,B}^n$        | The coupling Feature                                          |

Definitions require a threshold to be tuned, the decisions are over clusters rather than individual actions, which is more scalable, stable, and explainable for policy analysts and users alike. In the conclusion part, we elaborate on AI outcomes versus policy decisions to analyze the efficiency of the AI results.

In the following sections, we explain the components of RASA in detail.

### 3.2 Action Logs

In RASA’s model, action logs consist of data of physical activity such as entering or exiting a room as well as cyber activity such as logging in a device or accessing a document. In a multi-user distributed system, the access control of documents is effective to all kinds of actions. Regardless of the devices used in an environment, wired or mobile, the access of a document can always be abstracted in association with user movements such as entering or exiting a room, device usage, and operating documents. Our simulated action logs are inspired by typical actors in clinical, in-person settings.

An example of a sequence of actions is given in Figure 2. When users or devices enter or exit a specific location, the ID of the room and the ID of the user are logged with a timestamp. If a user attempts to access a document, then the device first requests grant for access, and this attempt is also logged. The distribution of the simulated actions is visualized in Figure 3 by using **T-distributed Stochastic Neighbor Embedding (t-SNE)**.

As a widely used and effective statistical visualization technique, mapping high-dimensional data onto 2D or 3D, t-SNE calculates the probability distributions of each pair of data samples in high- and low-dimensional spaces, assigning high probabilities to similar data samples, and by doing so, it minimizes Kullback-Leibler divergence between the high- and low-dimension distributions. t-SNE can exhibit the data distribution lying in various manifolds and clusters, while the distance between two samples in low-dimensional space do not represent the distance in high-dimensional space but the probabilities [29]. Hence, the axes in the plot do not represent physical units. By visualizing the dataset with t-SNE, we aim to understand the dataset distribution, discover potential clusters, and analyze the complexity of the problems.

General characteristic of the actions can be formulated as moving these objects (i.e., people, documents, and devices) across different locations over time. Thus, an event or a state machine is defined as a combination of time, location, and a set of objects in this space.
3.3 Feature Extraction and Risk Inference

The coupling concept aims to reveal the interactions among different factors of action logs. As illustrated in Figure 4, coupling can be defined between people and location, location and device, as well as location and document. In the figure, the interaction between two factors: document and people is presented in terms of duration and frequency. Duration denotes how long two objects spend time with each other; frequency denotes how many times two elements encounter each other. Using the logs, RASA first constructs the frequency and
duration matrices for each object pair (i.e., person-person, person-device, device-location, person-location). The coupling values in the matrices are normalized to enable comparability between different coupling values.

The coupling factors are denoted as: $\text{Ppl} = \{p_1, p_2, p_3, \ldots, p_n\}$, $\text{Doc} = \{\text{doc}_1, \text{doc}_2, \text{doc}_3, \ldots, \text{doc}_n\}$, $\text{Dev} = \{\text{dev}_1, \text{dev}_2, \text{dev}_3, \ldots, \text{dev}_n\}$, $\text{Loc} = \{\text{loc}_1, \text{loc}_2, \text{loc}_3, \ldots, \text{loc}_N\}$. The computation of coupling values is given in Equations (1) and (2) for frequency and duration, respectively.

In the RASA framework, the first step is converting the action logs to events. Algorithm 1 presents the generation of event list dictionary, which stores the status transitions of all factors. As discussed in Section 3.2, an action log contains a factor (e.g., a person, document, or device), an action (e.g., enter, read, or exit), and a location. For each action log, the algorithm determines the previous event, creates a new event according to whether the action is to move the factor in or out, and finally updates the statuses of all elements of the new event. It is worth to note that factors do not include locations as opposed to the element of an event. The event list dictionary is further processed by Algorithm 2 to generate $\text{Freq}_{a_i, b_j}$, which counts the number of times that $a_i$ and $b_j$ coexist in the same event, and $\text{Dur}_{a_i, b_j}$, which records the duration that two elements occur in the same event.

If $\text{Freq}_{a_i, b_j}$ and $\text{Dur}_{a_i, b_j}$ are considered, then they can be abstracted as $G_{a_i, b_j}$. Then, Equation (3) represents a coupling matrix (not yet normalized). The time window of the distribution is determined by the tuple $(k_{\text{start}}, k_{\text{end}})$. $T_{E_k}$ indicates the duration of each event. Note that $A$ and $B$ should satisfy $\text{Var}(A) > \text{Var}(B)$. The rationale behind this condition is as follows: According to Equations (1) and (2), these two formulas asymmetrically normalize the values. That said, to make coupling values comparable, the differences between the elements that have larger variance need to be reduced.
ALGORITHM 1: Event List Dictionary Generation

Input: actionLogs
Output: eventListDict
// Create a list if visit missing keys
eventListDict ← EmptyDict;

foreach actionLog in actionLogs do
    event ← eventListDict[actionLog.loc].lastElement;
    if event not found then
        event ← {actionLog.loc};
    end
    if action is moving a factor in (e.g., enter) then
        event ← event ∪ {actionLog.factor};
    end
    else if action is moving a factor out (e.g., exit) then
        event ← event – {actionLog.factor};
    end
    foreach elem in event do
        eventListDict[elem].add(event);
    end
end
return eventListDict

\[
\begin{bmatrix}
C_{a_1, b_1} & C_{a_1, b_2} & \ldots & C_{a_1, b_N} \\
C_{a_2, b_1} & C_{a_2, b_2} & \ldots & C_{a_2, b_N} \\
\vdots & \vdots & \ddots & \vdots \\
C_{a_N, b_1} & C_{a_N, b_2} & \ldots & C_{a_N, b_N}
\end{bmatrix}
\] (4)

Since the action logs contain four factors—namely, people, document, device, and location—theoretically $4^2 = 16$ different couplings can be obtained. These are: $C_{\text{device}.\text{location}}$, $C_{\text{device}.\text{document}}$, $C_{\text{document}.\text{location}}$, $C_{\text{people}.\text{location}}$, $C_{\text{people}.\text{device}}$, and $C_{\text{people}.\text{document}}$. As mentioned earlier, coupling values are asymmetric. For instance, $C_{A,B}$ is applied instead of $C_{B,A}$ in case the variance of the elements over $B$ is greater than those in $A$.

In case an object, such as a physician, interacts/couples with other objects or locations equally, its couplings will tend towards 1. If two objects less frequently interact, then their coupling tends towards 0, which means the risk associated to their coexistence is high.

Figure 5 illustrates how the coupling distribution in a matrix can be skewed.

When multiple coupling values are of the same type, lower coupling value is used to ensure that the impact of risky elements will not be alleviated by safe ones. This is formulated in Equation (5). For instance, given $C_{a_i, b_k} < C_{a_j, b_k}$, when $a_i$ and $a_j$ appear with $b_k$ at the same time, $F_{AB}^n = C_{a_i, b_k}$. Specifically, if $E_j \subseteq E_j$, then $\text{Risk}(E_i) \leq \text{Risk}(E_j)$. For instance, as shown in Figure 6, $p_1$ and $p_3$ co-exist with $doc_1$ in $E_{13}$. $C_{p_1, doc_1}$ and $C_{p_3, doc_1}$ are determined according to historical records and $C_{p_1, doc_1} > C_{p_3, doc_1}$. Therefore, for this event, $F_{13}^{\text{Ppl}, \text{Doc}} = C_{p_3, doc_1}$

\[
F_{n}^{A,B} = \min_{i,j} C_{a_i, b_j}, \forall a_i, b_j \in E_n
\] (5)

Our final goal is to label each cluster of couplings with a risk level, which will be described in the next section. To be able to associate clusters with the risk, we need to first assign risk levels to each individual coupling. Therefore, for each coupling matrix, we map the coupling values to onto three risk levels as high, medium, or low risk. To achieve this, we set a threshold as Equation (6) and apply mean value binning over the coupling values.

\[
\text{Threshold}_{\text{High}} = \text{mean} - \alpha \times \text{stdev}
\] (6)
To formulate the risk level of each event, several strategies are applied, one of which is to code high as three, medium as two, and low as one. This is followed by calculating the average risk of each event. Then the average risk will be marked as high-, medium-, low-risk. The other one is to directly code the risk level of each feature, which can directly represent features’ pattern. The latter one is used to evaluate the results. Even if the risk level of each coupling value is inferred, still, it cannot be used as ground truth, because we introduce human subjectivity and intuition into this inference.

Conventionally, researchers may adopt a risk matrix \([15]\) to evaluate the risk level, e.g., \(\text{Risk} \propto \text{Probability} \times \text{Impact}\). However, this study infers risk by defining association between various objects and situations in the action logs. Thus, the use of conventional risk formulation is left to future work along with further investigations on the quantification of the impact.

3.4 Clustering of Couplings and Labeling of the Clusters

RASA framework clusters the couplings into groups and uses the cluster members’ risk levels to determine the label of each cluster. Note that non-clustered couplings are less frequently observed, and so possess higher risk.

Most clustering algorithms put similar distance samples into one cluster. In this work, risk levels of couplings are used as the distance metric in cluster formation.

The cluster risk value (CRV) is determined based on the following formula:

\[
CRV = \frac{N_H \times C_H + N_M \times C_M + N_L \times C_L}{N_H + N_M + N_L},
\]

(7)

where \(N_H, N_M, N_L\) denote the number of high-, medium-, and low-risk features, respectively; and \(C_H, C_M, C_L\) are the codes that are assigned to high-, medium-, and low-risk levels. \(C_H, C_M, C_L\) correspond to 3, 2, 1, respectively, 3 denoting a higher risk. This is followed by mapping these values to Low (L), Low-Medium (LM), Medium-Low (ML), Medium (M), Medium-High (MH), High-Medium (HM), and High (H) risk levels according to Table 4. In case a cluster is labeled high-risk, all actions in this cluster would be denied.
Otherwise, the clusters with medium or low-risk labels contain the actions that may be permitted. The decision for medium-risk clusters depends on the coupling feature-based risk levels for each individual point.

4 NUMERICAL RESULTS

In this section, we evaluate the initial promise of the RASA approach by comparing the decisions against an heuristic policy, and also validated with two supervised learning methods, namely, decision tree and Support Vector Machine (SVM).

The action logs used in this work contain one device; hence, the available features are Location-People, Location-Device, Location-Document, and Document-People. Because the action logs cover a single device, only $C_{document,location}$, $C_{people,location}$, $C_{people,people}$, and $C_{people,document}$ are used in the evaluations. We present the results under using duration-based features, frequency-based features, and the combined (i.e., frequency and duration-based) features. In addition, three different clustering algorithms are applied, which are Gaussian mixture models (GMM) [36], Agglomerative Hierarchical [43], and DBSCAN [13]. The target is to cluster these
features (couplings) and label the clusters with risk levels. The aim of the clustering algorithm is to form the least possible number of clusters where within each cluster co-existence of high- and low-risk patterns is avoided.

4.1 Numerical Results of Clustering and Labeling
This subsection presents visualization of features followed by feature-by-feature risk of each cluster in the action logs. Then, results under different clustering algorithms are discussed, and finally cluster risk levels are presented.

4.1.1 Visualization of Features. Figure 7 illustrates the features visualized via using t-SNE [34, 41]; features are presented by color codes to show risk levels of samples (red=high-risk, green=low-risk, and orange=medium-risk). In Figure 7 (a–c), most of the data points are of low-risk level (green) whereas the medium and high average-risk samples are less frequently observed. t-SNE maps every multi-dimensional input in a dataset onto two or three dimensions. When t-sNE-based modeling is complete, similar data are mapped close to each other, whereas dissimilar data are mapped onto distant points [29].

4.1.2 Feature-by-feature Risk of Clusters. We calculate and present the percentage of feature-by-feature risk level (high/medium/low risk) found at each cluster when we use DBSCAN, Hierarchical, and GMM clustering. Note that hierarchical and GMM clustering schemes generate the same results, as shown in Figure 9. It is not viable to apply the frequency or duration as the only metric to evaluate objects’ relationship and their risk levels. In this study, we also consider the circumstances under which people may stay in a room for a long time while they enter and exit other rooms with high frequency. Therefore, the frequency-based features are also expected to affect the risk assessment. Since the duration-based coupling features and frequency-based features show distinctive perspective of the action logs, this study also employs the combined features defined as concatenation of two features. Clustering results and risk value results are generated by using three different features. Figures 8 and 9 present the percentage of feature-by-feature risk levels of clusters by using frequency-based, duration-based, and combined features. When Figures 8 and 9 are compared when given the same number of clusters, DBSCAN, Hierarchical, and HMM provide similar results, although DBSCAN results suggest it may increase noise.

Both Figures 8 and 9 illustrate the diversity of three features; however, the results of these three features have a similar pattern. Low-risk events are dominant, other types of risk are minor, which is what one would hope.
is a realistic distribution of event risks in normal clinical practice. This pattern also results in the similarity of the three figures in Figure 10. It is worth to note that the occurrence of this pattern is only due to the simulated action logs used in this study. When different action logs are employed, the result of three features may lead to a more significant variation.

4.1.3 Clustering Algorithms: (HMM and DBSCAN). The strength of DBSCAN is that we do not need to specify the number of clusters upfront, while in hierarchical and GMM, the number of desired clusters are given. If there were more factors in the action logs, then the number of features would increase, hence labeling of action clusters by using DBSCAN is generalizable. Indeed, outliers are expected, however, the outliers are not treated as high-risk samples directly, because the events may be the sub-events of another cluster. For instance, in Tables 5, 6, and 7, the sample in the cluster –1 does not have documents in this event; hence, there is no possibility of leaking sensitive data in such an event. Nevertheless, in practice, we expect that, as a matter of policy, outliers would be escalated to the security operations and policy experts.

4.1.4 Cluster Risk Levels. As clusters and their feature-by-feature risk levels are obtained, risk values of clusters are calculated according to Equation (7) and binned into seven groups: low, low-medium, medium-low,
medium, medium-high, high-medium, and high. Since the actions in medium and low-risk level clusters will be permitted, we aim to prevent high-risk samples from being clustered into medium- and low-risk clusters. Although the average-risk level is not a kind of ground truth, if it shows high-risk, then most of the features of the sample raise alert or medium-risk. As explained in the feature extraction section, the coupling value of medium-risk is similar to that of high-risk. There is no obvious boundary between these two risk levels, and clustering algorithms provide some potential risk patterns in the action logs.

The risk values and levels of each cluster are shown in Tables 5, 6, and 7. The cluster risk values are sorted and plotted as illustrated in Figure 10. This article further compares the outcomes of three features in Figure 11. Most of them are safe clusters, whereas only one cluster raises a high-risk alert. Based on this, the risk value of the entire dataset (i.e., action log) can be calculated as well, which is 1.28 in this case.

4.2 Validation via Supervised Learning
In the final step, as shown in the Figure 13, this work utilizes supervised learning methods, decision tree, and SVM to validate the results of unsupervised learning and to verify whether the coupling idea can be generalized.
As shown in Figure 14, when the model is trained with dataset 1 and tested with dataset 2, 100% training accuracy and 99.86% test accuracy are achieved. As Figures 3 and 12 present, despite the distinct distributions of datasets 1 and 2, the proposed methodology can still function well. Support Vector Machine (SVM) is also employed, and it achieves 99.95% test accuracy.

4.3 Access Control Policy-based Decisions

The performance of RASA framework is validated against a policy-based access control scheme. Policy-based decisions can be considered as a Attribute-Based Access Control (ABAC) [20] approach, utilizing the four frequency-based coupling features introduced above in addition to the traffic, which indicates the number of people in the current event, and co-existence, which is triple-coupling, people-document-location coupling. Even though the traffic does not entail any coupling, it is possible to use Equation (6) and the average value to determine the risk level of each coupling value.

Other features would further transform into risk as well. The policy maps the features’ risk onto three risk categories: Device Risk, Environment Risk, and Action Risk. Furthermore, it applies a weighted sum of these
Fig. 10. DBSCAN cluster risk values using different features.

risks together to determine the overall risk.

\[
R_{Dev} = 0.5 \times R_{dev,loc}^{Freq}
\]
\[
R_{Env} = 0.5 \times R_{traffic}^{Freq} + 0.5 \times R_{co-existence}^{Freq}
\]
\[
R_{Act} = 0.5 \times R_{doc,loc}^{Freq} + 0.5 \times R_{doc,time}
\]
\[
R_{Overall} = 0.3 \times R_{Dev} + 0.4 \times R_{Env} + 0.3 \times R_{Act}
\]

Due to the lack of labels or other methods to prove the efficiency of these methods, to examine the performance of the proposed scheme, the unsupervised method and policy-based method are also compared with each other [26]. By tuning the parameters of policy, we also investigated the outcomes of RASA and policy and analyzed the action log. As shown in Tables 8, 9, and 10, the frequency-based, duration-based, and combined coupling features show 99.32%, 99.27%, and 99.32% overall consistency, respectively. Since the policy uses the triple factor coupling, it is more likely to detect the rare cases but meanwhile, it is the only triple factor coupling, since only one device exists in the action log. When the number of coupling factors increases, the types of couplings will reduce, and such a situation would occur where the frequency or duration is not enough to make statistical decision, because the frequency or duration disperse on more coupling combinations.
### Table 5. DBSCAN Result Using Duration-based Features

| Index | Risk Value | Risk Level | Number of samples |
|-------|------------|------------|-------------------|
| −1    | 1.5        | LM         | 1                 |
| 0     | 1          | L          | 12,612            |
| 1     | 3          | H          | 2,804             |
| 2     | 1.31       | LM         | 2,234             |
| 3     | 1.97       | ML         | 1,492             |
| 4     | 1.59       | ML         | 608               |
| 5     | 1.16       | LM         | 20,489            |
| 6     | 1.74       | ML         | 480               |
| 7     | 1.5        | LM         | 246               |

### Table 6. DBSCAN Result Using Frequency-based Features

| Index | Risk Value | Risk Level | Number of samples |
|-------|------------|------------|-------------------|
| −1    | 1.5        | LM         | 1                 |
| 0     | 1          | L          | 11,754            |
| 1     | 3          | H          | 2,804             |
| 2     | 1.25       | LM         | 3,082             |
| 3     | 1.94       | ML         | 2,100             |
| 4     | 1.15       | LM         | 20,979            |
| 5     | 1.55       | ML         | 246               |

### Table 7. DBSCAN Result Using Combined-based Features

| Index | Risk Value | Risk Level | Number of samples |
|-------|------------|------------|-------------------|
| −1    | 1.5        | LM         | 1                 |
| 0     | 1          | L          | 11,222            |
| 1     | 3          | H          | 2,804             |
| 2     | 1.25       | LM         | 1,702             |
| 3     | 1.13       | LM         | 1,390             |
| 4     | 1.97       | ML         | 1,492             |
| 5     | 1.72       | ML         | 608               |
| 6     | 1.15       | LM         | 20,489            |
| 7     | 1.25       | LM         | 532               |
| 8     | 1.48       | LM         | 490               |
| 9     | 1.52       | ML         | 246               |

5 CONCLUSION AND FUTURE WORK

In this article, we propose the **Risk-Aware Smart Access Control (RASA)** framework, which defines a simple overall structure to learn use contexts from observed resource access within cyberphysical contexts, and use simple parameters to define a context-dependent and risk-based authorization scheme based on those contexts. The basic framework can be utilized to extend other access control regimes that lack sufficient support for security policy analysts to craft and maintain context-dependent authorization policies. RASA utilizes combined cyber and physical activity logs, converts action sequence to events that contain contextual information, and identifies common relations through a coupling approach based on duration and frequency of interactions.
Every coupling is assigned a risk value that results from the intuition that frequently occurring interactions can be considered as low-risk and rarely occurring actions as high-risk. RASA further feeds these couplings to clustering algorithms, after which the level of risk for a cluster is determined based on the risk levels of cluster members (i.e., couplings). Thereafter, RASA denies actions in high-risk clusters and permits safe actions. One of
Fig. 12. Visualization of raw actions in dataset 2.

Fig. 13. Supervised learning validation.
the insights from our study in a simulated clinical environment is the importance of the selection of couplings on risk inference.

Three different features are explored in this study, namely, frequency-based, duration-based, and the combination of frequency and duration. According to clustering and labelling results, these features can exhibit distinct perspectives of risk. We show that combined features can more comprehensively represent the risk of events and actions.

It may be helpful in future work to define other risk factor compositions and understand better their interactions.

RASA is purposefully designed to require little in the way of security policy analyst input—for example, no extensive labeling of actions into risk is required to develop a training set. Our evaluation established a basic validation of the promise of building on this approach.

In the tuning process, rule-based policy results are compared with the outcomes of RASA, and rule-based policy and RASA are updated in each iteration. After multiple tuning iterations, the decisions of two approaches achieved >99% consistency. Furthermore, to validate the results of RASA, when two supervised methods (Decision tree and SVM) are trained and tested by using different action logs labeled by RASA, 99.95% test accuracy is achieved.
Future work could seek evaluation against data derived from authentic use cases. Similar approaches to automatic inference of authorization contexts and associated risks may be particularly applicable in rich cyberphysical environments where sensors are deployed to generate activity logs by monitoring physical actions, in addition to common network and endpoint cyber action logs. Such sensor-rich environments are becoming increasingly common in extremely diverse cyberphysical contexts, including clinical, industrial, home, automotive, smart-building, and smart-city contexts. As these cyberphysical systems grow in size and complexity, human-written context-dependent authorization access rules will not scale, nor will expert risk analysis be cost effective and reliable without evidence-based risk assessment of such accesses. The RASA framework proposed in this article may be a stepping stone to rich exploration of similar approaches to address such growing problems in cyberphysical security.

APPENDIX

In this section, we present further detailed results about coupling matrices and normalized coupling matrices for each pair of coupled factors.

By following Algorithms 1 and 2, the action logs are transformed into events, and the frequency and duration information are extracted. As shown in Tables 11 and 12, we present $Freq_{a_i,b_j}$ and $Dur_{a_i,b_j}$ in $Freq_{A,B}$ and $Dur_{A,B}$ coupling matrices, respectively. By applying Equations (1) and (2), the coupling matrices are transformed into normalized coupling matrices listed in Tables 13 and 14. Since one device exists in the dataset, four couplings are selected as features (i.e., $C_{Doc,Loc}$, $C_{Ppl,Doc}$, $C_{Ppl,Loc}$, and $C_{Ppl,Ppl}$). By viewing both the frequency-based and duration-based coupling matrices, one can have a clear understanding of how factors interact with each other.
Table 11. Frequency-based Coupling Matrices

(a) $Freq_{Dev, Loc}$

| Location   | Device1 |
|------------|---------|
| Location1  | 5,065   |
| Location2  | 0       |
| Location3  | 0       |
| Location4  | 854     |
| Location5  | 0       |
| Location6  | 0       |
| Location7  | 0       |

(b) $Freq_{Doc, Loc}$

| Location   | Doc1 | Doc2 | Doc3 | Doc4 | Doc5 | Doc6 |
|------------|------|------|------|------|------|------|
| Location1  | 782  | 846  | 957  | 834  | 794  | 852  |
| Location2  | 0    | 0    | 0    | 0    | 0    | 0    |
| Location3  | 0    | 0    | 0    | 0    | 0    | 0    |
| Location4  | 215  | 232  | 233  | 298  | 245  | 241  |
| Location5  | 0    | 0    | 0    | 0    | 0    | 0    |
| Location6  | 0    | 0    | 0    | 0    | 0    | 0    |
| Location7  | 0    | 0    | 0    | 0    | 0    | 0    |

(c) $Freq_{Ppl, Doc}$

| Doc   | Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|-------|------|------|------|------|------|------|------|------|
| Doc1  | 997  | 1,543| 45   | 38   | 116  | 47   | 63   | 46   |
| Doc2  | 1,078| 1,647| 55   | 24   | 51   | 40   | 55   | 116  |
| Doc3  | 1,190| 1,937| 70   | 116  | 55   | 42   | 63   | 37   |
| Doc4  | 1,132| 1,601| 79   | 45   | 49   | 74   | 203  | 46   |
| Doc5  | 1,039| 1,560| 140  | 37   | 46   | 70   | 62   |      |
| Doc6  | 1,093| 1,712| 52   | 35   | 35   | 144  | 75   | 48   |

(d) $Freq_{Ppl, Loc}$

| Loc   | Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|-------|------|------|------|------|------|------|------|------|
| Loc1  | 5,066| 4,936| 159  | 167  | 201  | 166  | 161  | 168  |
| Loc2  | 0    | 0    | 1    | 0    | 0    | 0    | 0    | 0    |
| Loc3  | 0    | 0    | 0    | 1    | 0    | 0    | 0    | 0    |
| Loc4  | 854  | 818  | 25   | 22   | 28   | 26   | 36   | 25   |
| Loc5  | 0    | 0    | 0    | 0    | 1    | 0    | 0    |      |
| Loc6  | 0    | 0    | 0    | 0    | 0    | 0    | 1    | 0    |
| Loc7  | 0    | 0    | 0    | 0    | 0    | 0    | 1    |      |

(e) $Freq_{Ppl, Ppl}$

| Ppl   | Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|-------|------|------|------|------|------|------|------|------|
| Ppl1  | 10,001| 259  | 190  | 222  | 239  | 304  | 218  |      |
| Ppl2  | 10,001| 243  | 171  | 231  | 210  | 284  | 207  |      |
| Ppl3  | 259  | 243  | 11   | 6    | 9    | 15   | 9    |      |
| Ppl4  | 190  | 171  | 11   | 6    | 6    | 11   | 4    |      |
| Ppl5  | 222  | 231  | 6    | 6    | 7    | 18   | 11   |      |
| Ppl6  | 239  | 210  | 9    | 6    | 7    | 17   | 7    |      |
| Ppl7  | 304  | 284  | 15   | 11   | 18   | 17   | 15   |      |
| Ppl8  | 218  | 207  | 9    | 4    | 11   | 7    | 15   |      |

Digital Threats: Research and Practice, Vol. 3, No. 4, Article 43. Publication date: December 2022.
Table 12. Duration-based Coupling Matrices

(a) $Dur_{Dev, Loc}$

|             | Location1 | Location2 | Location3 | Location4 | Location5 | Location6 | Location7 |
|-------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| Device1     | 335,384.62449996645 | 0.0       | 0.0       | 56,341.1491895333 | 0.0       | 0.0       | 0.0       |

(b) $Dur_{Doc, Loc}$

|             | Doc1 | Doc2 | Doc3 | Doc4 | Doc5 | Doc6 |
|-------------|------|------|------|------|------|------|
| Loc1        | 51,227 | 54,270 | 66,317 | 52,308 | 52,734 | 58,526 |
| Loc2        | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   |
| Loc3        | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   |
| Loc4        | 7,827 | 9,155 | 9,150 | 11,185 | 9,754 | 9,237 |
| Loc5        | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   |
| Loc6        | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   |
| Loc7        | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   |

(c) $Dur_{Ppl, Doc}$

|             | Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|-------------|------|------|------|------|------|------|------|------|
| Doc1        | 59,054 | 1,544 | 1,344 | 1,134 | 3,840 | 1,468 | 1,887 | 1,439 |
| Doc2        | 63,425 | 1,647 | 1,711 | 720   | 1,593 | 1,202 | 1,713 | 3,781 |
| Doc3        | 75,468 | 1,935 | 2,285 | 3,958 | 1,649 | 1,262 | 1,954 | 1,171 |
| Doc4        | 63,494 | 1,600 | 2,486 | 1,354 | 1,589 | 2,214 | 7,106 | 1,556 |
| Doc5        | 62,489 | 1,560 | 4,682 | 1,171 | 1,379 | 1,290 | 2,096 | 1,857 |
| Doc6        | 67,763 | 1,712 | 1,616 | 1,047 | 1,111 | 4,560 | 2,311 | 1,502 |

(d) $Dur_{Ppl, Loc}$

|             | Loc1 | Loc2 | Loc3 | Loc4 | Loc5 | Loc6 | Loc7 | Loc8 |
|-------------|------|------|------|------|------|------|------|------|
| Ppl1        | 335,385 | 343,051 | 4,772 | 5,002 | 6,028 | 4,978 | 4,828 | 5,042 |
| Ppl2        | 0.0   | 0.0   | 3,167 | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   |
| Ppl3        | 0.0   | 0.0   | 0.0   | 2,801 | 0.0   | 0.0   | 0.0   | 0.0   |
| Ppl4        | 56,341 | 54,442 | 121,547 | 80,092 | 107,772 | 108,641 | 139,899 | 102,243 |
| Ppl5        | 0.0   | 0.0   | 0.0   | 0.0   | 4627   | 0.0   | 0.0   | 0.0   |
| Ppl6        | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   | 913   | 0.0   | 0.0   |
| Ppl7        | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   | 0.0   | 670   | 0.0   |
| Ppl8        | 10,001 | 14,127 | 9,386 | 11,193 | 11,998 | 17,069 | 11,309 | 0.0   |

(e) $Dur_{Ppl, Ppl}$

|             | Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|-------------|------|------|------|------|------|------|------|------|
| Ppl1        | 10,001 | 14,127 | 9,386 | 11,193 | 11,998 | 17,069 | 11,309 | 0.0   |
| Ppl2        | 10,001 | 12,633 | 8,251 | 11,043 | 10,840 | 15,580 | 10,140 | 0.0   |
| Ppl3        | 14,127 | 12,633 | 16,476 | 9,255 | 19,966 | 37,563 | 24,455 | 0.0   |
| Ppl4        | 9,386 | 8,251 | 16,476 | 16,825 | 5,055 | 19,705 | 4,385 | 0.0   |
| Ppl5        | 11,193 | 11,043 | 9,255 | 16,825 | 13,669 | 23,381 | 14,461 | 0.0   |
| Ppl6        | 11,998 | 10,840 | 19,966 | 5,055 | 13,669 | 34,577 | 17,834 | 0.0   |
| Ppl7        | 17,069 | 15,580 | 37,563 | 19,705 | 23,381 | 34,577 | 26,891 | 0.0   |
| Ppl8        | 11,309 | 10,140 | 24,455 | 4,385 | 14,461 | 17,834 | 26,891 | 0.0   |
Table 13. Normalized Frequency-based Coupling Matrices

(a) $C_{Dev, Loc}^{Freq}$

| Device1 | Location1 | Location2 | Location3 | Location4 | Location5 | Location6 | Location7 |
|---------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
|         | Location1 | Location2 | Location3 | Location4 | Location5 | Location6 | Location7 |
|         | 1.0       | 0.0       | 0.0       | 0.1686080947680158 | 0.0       | 0.0       | 0.0       |

(b) $C_{Doc, Loc}^{Freq}$

| Location1 | Location2 | Location3 | Location4 | Location5 | Location6 | Location7 |
|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| Location1 | Location2 | Location3 | Location4 | Location5 | Location6 | Location7 |
| Location1 | Location2 | Location3 | Location4 | Location5 | Location6 | Location7 |

(c) $C_{Ppl, Doc}^{Freq}$

| Doc1 | Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|------|------|------|------|------|------|------|------|------|
| 0.84 | 0.80 | 0.32 | 0.33 | 1.00 | 0.33 | 0.31 | 0.40 |
| 0.91 | 0.85 | 0.39 | 0.21 | 0.44 | 0.28 | 0.27 | 1.00 |
| 1.00 | 1.00 | 0.50 | 1.00 | 0.47 | 0.29 | 0.31 | 0.32 |
| 0.95 | 0.83 | 0.56 | 0.39 | 0.42 | 0.31 | 1.00 | 0.40 |
| 0.87 | 0.81 | 1.00 | 0.52 | 0.28 | 0.34 | 0.53 |
| 0.92 | 0.88 | 0.37 | 0.30 | 0.30 | 1.00 | 0.37 | 0.41 |

(d) $C_{Ppl, Loc}^{Freq}$

| Loc1 | Loc2 | Loc3 | Loc4 | Loc5 | Loc6 | Loc7 |
|------|------|------|------|------|------|------|
| 1.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| 0.17 | 0.17 | 0.16 | 0.13 | 0.14 | 0.16 | 0.22 |
| 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |

(e) $C_{Ppl, ppl}^{Freq}$

| Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|------|------|------|------|------|------|------|------|
| 1.00 | 0.94 | 0.90 | 1.00 | 0.88 | 0.93 | 0.95 |
| 0.03 | 0.02 | 0.02 | 0.04 | 0.03 | 0.03 | 0.04 |
| 0.02 | 0.02 | 0.02 | 0.04 | 0.03 | 0.03 | 0.04 |
| 0.02 | 0.02 | 0.02 | 0.03 | 0.03 | 0.06 | 0.05 |
| 0.02 | 0.02 | 0.02 | 0.02 | 0.03 | 0.03 | 0.03 |
| 0.02 | 0.02 | 0.02 | 0.02 | 0.02 | 0.02 | 0.02 |
Table 14. Normalized Duration-based Coupling Matrices

(a) $c_{Dev, Loc}^{Dur}$

| Location | Device1 |
|----------|---------|
| Location1 | 1.00    |
| Location2 | 0.00    |
| Location3 | 0.00    |
| Location4 | 0.17    |
| Location5 | 0.00    |
| Location6 | 0.00    |
| Location7 | 0.00    |

(b) $c_{Doc, Loc}^{Dur}$

| Location | Doc1 | Doc2 | Doc3 | Doc4 | Doc5 | Doc6 |
|----------|------|------|------|------|------|------|
| Loc1     | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| Loc2     | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Loc3     | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Loc4     | 0.15 | 0.17 | 0.14 | 0.21 | 0.18 | 0.16 |
| Loc5     | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Loc6     | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Loc7     | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |

(c) $c_{Ppl, Doc}^{Dur}$

| Document | Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|----------|------|------|------|------|------|------|------|------|
| Doc1     | 0.78 | 0.80 | 0.29 | 0.29 | 1.00 | 0.32 | 0.27 | 0.38 |
| Doc2     | 0.84 | 0.85 | 0.37 | 0.18 | 0.42 | 0.26 | 0.24 | 1.00 |
| Doc3     | 1.00 | 1.00 | 0.49 | 1.00 | 0.43 | 0.28 | 0.27 | 0.31 |
| Doc4     | 0.84 | 0.83 | 0.53 | 0.34 | 0.41 | 0.49 | 1.00 | 0.41 |
| Doc5     | 0.83 | 0.81 | 1.00 | 0.30 | 0.36 | 0.28 | 0.29 | 0.49 |
| Doc6     | 0.90 | 0.88 | 0.35 | 0.26 | 0.29 | 1.00 | 0.33 | 0.40 |

(d) $c_{Ppl, Loc}^{Dur}$

| Location | Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|----------|------|------|------|------|------|------|------|------|
| Loc1     | 1.00 | 1.00 | 0.04 | 0.06 | 0.06 | 0.05 | 0.03 | 0.05 |
| Loc2     | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| Loc3     | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 |
| Loc4     | 0.17 | 0.16 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| Loc5     | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.04 | 0.00 | 0.00 |
| Loc6     | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.01 | 0.00 |
| Loc7     | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.01 |

(e) $c_{Ppl, Ppl}^{Dur}$

| Ppl1 | Ppl2 | Ppl3 | Ppl4 | Ppl5 | Ppl6 | Ppl7 | Ppl8 |
|------|------|------|------|------|------|------|------|
| Ppl1 | 0.64 | 0.38 | 0.48 | 0.48 | 0.35 | 0.45 | 0.42 |
| Ppl2 | 0.59 | 0.34 | 0.42 | 0.47 | 0.31 | 0.41 | 0.38 |
| Ppl3 | 0.83 | 0.81 | 0.84 | 0.40 | 0.58 | 1.00 | 0.91 |
| Ppl4 | 0.55 | 0.53 | 0.44 | 0.72 | 0.15 | 0.52 | 0.16 |
| Ppl5 | 0.66 | 0.71 | 0.25 | 0.85 | 0.40 | 0.62 | 0.54 |
| Ppl6 | 0.70 | 0.70 | 0.53 | 0.26 | 0.58 | 0.92 | 0.66 |
| Ppl7 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| Ppl8 | 0.66 | 0.65 | 0.65 | 0.22 | 0.62 | 0.52 | 0.72 |
ACKNOWLEDGMENT

The authors would like to thank Yueqian Zhang for collaborating with the team to provide the security policy updates.

REFERENCES

[1] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, and Can Yildiz. 2013. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec’13). Association for Computing Machinery, New York, NY, 1–6. DOI: https://doi.org/10.1145/2462096.2462098

[2] Fazel Anjomshoa, Moayad Aloqaily, Burak Kantarci, Melike Erol-Kantarci, and Stephanie Schuckers. 2017. Social behaviometrics for personalized devices in the Internet of Things Era. IEEE Access 5 (2017), 12199–12213. DOI: https://doi.org/10.1109/ACCESS.2017.2719706

[3] Yosef Abishabi, Dylan Kauling, and Qusay H. Mahmoud. 2017. A context-aware authentication framework for smart homes. In Proceedings of the IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE’17). 1–5. DOI: https://doi.org/10.1109/CCECE.2017.7946657

[4] Hany F. Atlam and Gary B. Wills. 2019. An efficient security risk estimation technique for risk-based access control model for IoT. Internet Things 6 (2019), 10052.

[5] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT’10). USENIX Association, 1–7.

[6] Adam J. Aviv, Benjamin Sapp, Matt Blaze, and Jonathan M. Smith. 2012. Practicality of accelerometer side channels on smartphones. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC’12). Association for Computing Machinery, New York, NY, 41–50. DOI: https://doi.org/10.1145/2420950.2420957

[7] S. Cha and K. Yeh. 2018. A data-driven security risk assessment scheme for personal data protection. IEEE Access 6 (2018), 50510–50517. DOI: https://doi.org/10.1109/ACCESS.2018.2865726

[8] Jason Paul Cruz, Yuichi Kaji, and Naoto Yanai. 2018. RBAC-SC: Role-based access control using smart contract. IEEE Access 6 (2018), 12240–12251. DOI: https://doi.org/10.1109/ACCESS.2018.2812844

[9] I. Deutschmann, P. Nordström, and L. Nilsson. 2013. Continuous authentication using behavioral biometrics. IT Profess. 15, 4 (July 2013), 12–15. DOI: https://doi.org/10.1109/MITP.2013.50

[10] Sheng Ding, Jin Cao, Chen Li, Kai Fan, and Hui Li. 2019. A novel attribute-based access control scheme using blockchain for IoT. IEEE Access 7 (2019), 38431–38441. DOI: https://doi.org/10.1109/ACCESS.2019.2905846

[11] Besik Dundua and Mikhail Rukhaia. 2019. Towards integrating attribute-based access control into ontologies. In Proceedings of the IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON’19). 1052–1056. DOI: https://doi.org/10.1109/UKRCON.2019.8879922

[12] Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are you ready to lock? In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS’14). Association for Computing Machinery, 750–761. DOI: https://doi.org/10.1145/2660267.2660273

[13] Martin Ester, Hans-Peter Kriegel, Jörg Sander, and Xiaowei Xu. 1996. A density-based algorithm for discovering clusters in large spatial databases with noise. In Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD’96). AAAI Press, Portland, Oregon, 226–231.

[14] Travis Floyd, Matthew Greico, and Edna F. Reid. 2016. Mining hospital data breach records: Cyber threats to U.S. hospitals. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS’16). 43–48. DOI: https://doi.org/10.1109/CCS.2016.7745441

[15] Kevin Fu, Tadayoshi Kohno, Daniel Lopresti, Elizabeth Mynatt, Klara Nahrstedt, Shwetak Patel, Debra Richardson, and Ben Zorn. 2020. Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things. Retrieved from arXiv:cs.CY/2008.00017.

[16] Hadi Habibzadeh, Cem Kaptan, Tolga Soyata, Burak Kantarci, and Azedine Boukerche. 2019. Smart city system design: A comprehensive study of the application and data planes. ACM Comput. Surv. 52, 2 (May 2019). DOI: https://doi.org/10.1145/3309545

[17] Hadi Habibzadeh, Tolga Soyata, Burak Kantarci, Azedine Boukerche, and Cem Kaptan. 2018. Sensing, communication and security planes: A new challenge for a smart city system design. Comput. Netw. 144 (2018), 163–200. DOI: https://doi.org/10.1016/j.comnet.2018.08.001

[18] Eiji Hayashi, Sunvik Das, Shahriyar Amini, Jason Hong, and Ian Oakley. 2013. CASA: Context-aware scalable authentication. In Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS’13). ACM, New York, NY, 3:1–3:10. DOI: https://doi.org/10.1145/2501604.2501607

[19] Daniel Hintze, Eckhard Koch, Sebastian Scholz, and René Mayrhofer. 2016. Location-based risk assessment for mobile authentication. In Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (UbiComp ’16). ACM, New York, NY, 85–88. DOI: https://doi.org/10.1145/2968219.2971448

Digital Threats: Research and Practice, Vol. 3, No. 4, Article 43. Publication date: December 2022.
[20] Vincent C. Hu, D. Richard Kuhn, David F. Ferraiolo, and Jeffrey Voas. 2015. Attribute-based access control. Computer 48, 2 (Feb. 2015), 85–88. DOI: https://doi.org/10.1109/MC.2015.33

[21] Chung-Hong Lee. 2012. Unsupervised and supervised learning to evaluate event relatedness based on content mining from social-media streams. Expert Syst. Appl. 39, 18 (Dec. 2012), 13338–13356. DOI: https://doi.org/10.1016/j.eswa.2012.05.068

[22] Wei-Han Lee and Ruby B. Lee. 2017. Implicit smartphone user authentication with sensors and contextual machine learning. In Proceedings of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN’17). 297–308. DOI: https://doi.org/10.1109/DSN.2017.24

[23] Hemanth Kambhamettu, Sofiene Boulares, Kamel Adi, and Luigi Logrippo. 2013. A framework for risk assessment in access control systems. Comput. Secur. 39 (2013), 86–103.

[24] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2015. Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In Proceedings of the 11th USENIX Conference on Usable Privacy and Security (SOU15). USENIX Association, 225–239.

[25] M. Fahim Ferdous Khan and Ken Sakamura. 2015. Fine-grained access control to medical records in digital healthcare enterprises. In Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC’15). 1–6. DOI: https://doi.org/10.1109/ISNCC.2015.7238590

[26] Wei-Han Lee and Ruby B. Lee. 2017. Implicit smartphone user authentication with sensors and contextual machine learning. In Proceedings of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN’17). 297–308. DOI: https://doi.org/10.1109/DSN.2017.24

[27] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani. 2016. HMOG: New behavioral biometric features for continuous authentication of smartphone users. IEEE Trans. Inf. Forens. Secur. 11, 5 (May 2016), 877–892. DOI: https://doi.org/10.1109/TIFS.2015.2506542

[28] S. Vadhuri and C. Poellabauer. 2019. Multi-modal biometric-based implicit authentication of wearable device users. IEEE Trans. Inf. Forens. Secur. 14, 12 (Dec. 2019), 3116–3125. DOI: https://doi.org/10.1109/TIFS.2019.2911170

[29] Laurens van der Maaten and Geoffrey Hinton. 2008. Visualizing data using t-SNE. J. Mach. Learn. Res. 9, Nov. (2008), 2579–2605.

[30] Vishal M. Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello. 2016. Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Sig. Process. Mag. 33, 4 (July 2016), 49–61. DOI: https://doi.org/10.1109/MSP.2016.2555335

[31] Hemanth Kambhamettu, Sofiene Boulares, Kamel Adi, and Luigi Logrippo. 2013. A framework for risk assessment in access control systems. Comput. Secur. 39 (2013), 86–103.

[32] Kyle Quintal, Burak Kantarcı, Meline Erol-Kantarcı, Andrew Malton, and Andrew Walenstein. 2019. Contextual, behavioral and biometric signatures for continuous authentication. IEEE Internet Comput. (2019). DOI: https://doi.org/10.1109/MIC.2019.2941391

[33] K. L. Ramatsakane and W. S. Leung. 2017. Pick location security: Seamless integrated multi-factor authentication. In Proceedings of the 21st Africa Week Conference (IST-Africa). 1–10. DOI: https://doi.org/10.1109/ISTAFRICA.2017.8102391

[34] Paulo E. Rauber, Alexandre X. Falcao, and Alexandru C. Telea. 2016. Visualizing time-dependent data using dynamic t-SNE. In Proceedings of the Eurographics/IEEE VGTC Conference on Visualization: Short Papers (EuroVis’16). Eurographics Association, Goslar, DEU, 73–77.

[35] Zachary I. Rauen, Fazel Anjomshoaa, and Burak Kantarcı. 2018. Gesture and sociability-based continuous authentication on smart mobile devices. In Proceedings of the 16th ACM International Symposium on Mobility Management and Wireless Access (MobiWac’18). ACM, New York, NY, 51–58. DOI: https://doi.org/10.1145/3265863.3265873

[36] D. A. Reynolds. 1993. A Gaussian mixture modeling approach to text-independent speaker identification. (1993). Retrieved from https://elibrary.ru/item.asp?id=5779793.

[37] Matthew Rossi, Dario Facchinetti, Enrico Bacis, Marco Rosa, and Stefano Paraboschi. 2021. SEApp: Bringing mandatory access control to Android apps. Retrieved from https://www.usenix.org/conference/usenixsecurity21/presentation/rossi.

[38] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani. 2016. HMOG: New behavioral biometric features for continuous authentication of smartphone users. IEEE Trans. Inf. Forens. Secur. 11, 5 (May 2016), 877–892. DOI: https://doi.org/10.1109/TIFS.2015.2506542

[39] S. Vadhuri and C. Poellabauer. 2019. Multi-modal biometric-based implicit authentication of wearable device users. IEEE Trans. Inf. Forens. Secur. 14, 12 (Dec. 2019), 3116–3125. DOI: https://doi.org/10.1109/TIFS.2019.2911170

[40] Junhua Wang and Hongxia Jin. 2011. Quantified risk-adaptive access control for patient privacy protection in health information systems. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS’11). Association for Computing Machinery, New York, NY, 406–410. DOI: https://doi.org/10.1145/1966913.1966969

[41] Martin Wattenberg, Fernanda Viégas, and Ian Johnson. 2016. How to use t-SNE effectively. Distill 1, 10 (Oct. 2016), e2. DOI: https://doi.org/10.23915/distill.00002

Digital Threats: Research and Practice, Vol. 3, No. 4, Article 43. Publication date: December 2022.
[42] Changsheng Wu, Wenbo Ding, Ruiyuan Liu, Jiyu Wang, Aurelia C. Wang, Jie Wang, Shengming Li, Yunlong Zi, and Zhong Lin Wang. 2018. Keystroke dynamics enabled authentication and identification using triboelectric nanogenerator array. *Mater. Today* 21, 3 (Apr. 2018), 216–222. DOI: https://doi.org/10.1016/j.mattod.2018.01.006

[43] Tian Zhang, Raghu Ramakrishnan, and Miron Livny. 1996. BIRCH: An efficient data clustering method for very large databases. *ACM SIGMOD Rec.* 25, 2 (June 1996), 103–114. DOI: https://doi.org/10.1145/235968.233324

Received 11 February 2021; revised 15 June 2021; accepted 5 August 2021