Physical Access Log Analysis: An Unsupervised Clustering Approach for Anomaly Detection

Ju Peng Poh
Certis Group
Singapore
poh_ju_peng@certisgroup.com

Jun Yu Charles Lee
Certis Group
Singapore
charlesjy_lee@certisgroup.com

Kah Xuan Tan
Certis Group
Singapore
tan_kah_xuan@certisgroup.com

Eric Tan
Sift Analytics
Singapore
eric.tan@sift-ag.com

ABSTRACT

There are ample of research work on the detection of anomalies in the area of cyber security. However, only a few of them focus on physical access security. Physical access control, including employee and guest access and management system, supervised doors or location, surveillance camera, are critical checkpoints of a premise in terms of security monitoring. Breaches of these checkpoints can cause serious damage, where an insider or an outsider (e.g. through social engineering) may gain access to sensitive areas of the premise and may further result in data leakage or disruptions of services. In this paper, we characterise users based on their physical movement behavior and job profile in order to identify users with anomalous physical access behaviour using an unsupervised machine learning algorithm known as the Two Step clustering method. We further evaluate the type of risk posed by these users by comparing the user's behaviour with its peer group and observing a set of rule-based metrics. The framework is then being compared with other recent approaches for anomaly detection of physical access logs. Lastly, this framework is deployed in a real-world environment and successfully assisted in the detection of anomalous physical access behaviour.

CCS CONCEPTS

•Information systems~Information systems applications~Data mining~Clustering •Security and privacy~Intrusion/anomaly detection and malware mitigation~Intrusion detection systems

KEYWORDS

Anomaly Detection, Physical Access, Clustering, Machine Learning, Data Mining, Data Modeling

DSIT 2020, July 24–26, 2020, Xiamen, China

ACM ISBN 978-1-4503-7604-4/20/07…$15.00
https://doi.org/10.1145/3414274.3414285

ACM Reference format:

Ju Peng Poh, Jun Yu Charles Lee, Kah Xuan Tan and Eric Tan. 2020. Physical Access Log Analysis: An Unsupervised Clustering Approach for Anomaly Detection. In *Proceedings of 2020 International Conference on Data Science and Information Technology (DSIT' 20). Xiamen, China, 7 pages.* https://doi.org/10.1145/3414274.3414285

1 Introduction

Physical access control, including employee and guest access and management system, supervised doors or location, surveillance camera, are critical checkpoints of a premise in terms of security monitoring. Breaches of these checkpoints can cause serious damage, where an insider or an outsider (e.g. through social engineering) may gain access to sensitive areas of the premise. The threats posed by the insiders are difficult to detect as the adversary has cyber and physical access to the organization's assets. The latest research and practice focus on insider cyber-attacks by analysing the user's cyber footprint (e.g logins and file accesses). By considering only the cyber aspect of users' behavior, organisations leave themselves vulnerable to future cyber-attacks, data leakage or disruption of services and even less tech-savvy attacks such as theft and vandalism. One example of a physical access breach is a case of a technician in Singapore Changi Airport misusing his pass to illegally enter the transit area close to 50 times to purchase duty-free items in Singapore [1]. This issue could be more severe if, for example, a user trespasses more critical areas like the control station.

Companies usually issue out temporary or staff passes to employees but do not have a system to keep track of their staff pass usage for the identification of potentially malicious behaviour. Although one way to mitigate these threats is to restrict locations accessible to different users, there may be locations that are administratively costly to restrict as it would require the security manager to evaluate many access requests. An organisation will benefit from anomaly detection as they would be able to keep track of their employee staff pass usage and flag out unusual behaviour. This is especially critical in recent years as insider threats have become more prevalent with more than 53% of companies experienced insider attacks against their organisation in the year

2018, with 27 % saying insider attacks have become more frequent. [2]. Our approach to anomaly detection of physical access will enhance the security for these organisations and ensure that their day to day operation runs smoothly.

In our approach, we use the Two Step Clustering Algorithm as it does not require any predefined rules or patterns and is able to consider both categorical and continuous data. This makes it a suitable anomaly detection technique for cases whereby profile of the user, in the form of job role and profile, are important inputs for the model. Its ability to measure the degree of anomalousness allows the flexibility for security manager to evaluate the number of high-risk users to investigate for possible insider threats. Its high scalability allows the company to manage large amount of physical access data and implement real-time threat detection capabilities. After evaluating the features of the recent approaches adopted for anomaly detection of physical access log data, we are able show that our framework is useful in providing an efficient way of identifying potentially malicious physical accesses.

Currently, the activities of the malicious physical accesses are hard to identify as it is often a manual process of going through the physical logs to identify abnormal behaviour. By implementing our framework, the time and effort required to identify potentially malicious physical accesses is estimated to be 30 to 50 per cent smaller. The security manager would only look through a smaller subset of these potentially malicious physical accesses by observing the risk score of the individual users. The risk score reflects the likelihood of a user having exhibited malicious behaviour. This allows for a more targeted investigation over a fewer number of suspects using other possible sources of evidence like video surveillance and cyber log activities.

In this paper, we use the physical card access behavior of the users and their peers to identify anomalous physical accesses. When there is a large deviation in the physical access pattern of a user from the usual behavior of their assigned peer group, the user would be flagged as an anomaly. We show that abnormal movement of users can be detected from physical access logs through a real-life case and demonstrates its ability to strengthen a system's physical security. This is done by using a framework that characterises users based on their physical movement behavior and job profile. The clustering algorithm will then output a risk score for each user based on the deviation of a user's physical access behaviour from their peer group. The risk score reflects a user's likelihood of having exhibited malicious behaviour. Lastly, we deployed this framework in a real-world environment and successfully assisted in the detection of anomalous physical access behaviour.

2 Related Work

There are several works proposing the use of data mining methods in the analysis of log file to identify potentially malicious accesses in the area of cyber security. In order to detect anomalies in log files, Frei and Rennhard [3] created the Histogram Matrix, a log file visualization technique that helps security administrators to spot anomalies. In addition, Fu et al. [4] proposed techniques for anomaly detection in unstructured system logs that does not require any application of specific knowledge. This includes methods to extract log keys from free text messages.

The use of unsupervised algorithm for anomaly detection in the field of cyber security is widely researched as this technique does not require previous knowledge about the data. As log data may be represented in high-dimensional spaces, dimensionality reduction techniques may be used to detect outliers [5]. Other approaches apply probability theory [6] and Bayes Statistics [7] together with clustering techniques [8] in order to analyse network traffic for outliers. Similarly, our framework does not require any predefined rule or pattern in order to detect suspicious behaviour.

Incremental cluster methods can dynamically add any number of incoming data points by either allocating them to one of the existing clusters or declaring them as outliers if the distance to the nearest cluster exceeds a certain threshold. In the paper by Wurzeneber et al. [9], this incremental approach has been applied to anomaly detection of cyber log file on systems with a highly predictable behaviour and many repeating sequences. Our approach also does not require the processing of all clustered data at once which helps in the processing of large amount of data in real-time.

There are different anomaly detection techniques applied using physical access logs in office building. For indoor physical access, there are pre-existing techniques to detect differences in a user's movement. Graph models have been studied by Eberle [10] and Davis [11] for this purpose. Davis et al. [11] uses search labeled graphs for both structural and numeric anomalies and apply their approach to physical access logs in an office building. In addition, Eberle et al. [10] detect structural anomalies by extracting common subgraph movement patterns. Although the physical layouts have been considered in these papers, their techniques fail to consider the differences between users' job role.

Taking reference from a systematic framework proposed by Cheh et al. [12], our model also uses knowledge of the system and its users to analyse physical access log for the detection of malicious behaviour. The paper is unlike ours as it uses Markov model and is implemented in a railway station, which has a highly restricted number of paths a user can take. In a large office building with many levels and delineated rooms, where this study is implemented, there are many more possible paths. This makes the implementation of Markov model challenging since it requires the understanding of the system layout. Our model can detect suspicious behaviour with no predefined patterns or rules. This makes it more easily implemented in large office buildings with many access control points. This approach enables us to identify locations that may have contributed to the high-risk score of a user by comparing with the locations accessed rarely by the user's peer group. This allows us to assess the type of risk that could be posed by the user based on the access location.

3 Physical Access Anomaly Detection Framework

In recent decades, the technology and computer environment in many organisations allow more compromises to occur due to its increased vulnerabilities. Many technological tools organisations use

such as USB, hard drives, laptops, tablets and smartphones are highly portable and allows for mobile access. Therefore, it is easier for information to be lost or stolen [13]. As the environment of organisations are becoming more "complex and dynamic", there is an increasing cost of physical security breaches, including fraud, vandalism, sabotage, accidents and theft [14]. Our anomaly detection framework proposes an approach to deal with these threats.

As our approach uses the log data from physical access control systems, we track the behaviour of personnel with access to our building. This includes all personnel that pose the greatest insider security risk to organisations, including regular employees, privileged IT users, followed by contractors [2]. Based on the physical access pattern of the users, we identify users who exhibited high risk behaviour. We can protect the valuable data of our organisations by monitoring the location and time period of access for each high-risk user. By identifying the functions of the locations accessed by high-risk users, we can assess the possible threats posed by the suspicious user.

3.1 Overview

The framework splits the problem into three parts: (1) characterisation of users based on users' profile and behavioural pattern from physical access log data, (2) the identification of users with anomalous physical access behaviour using a clustering algorithm and (3) the evaluation of the type of risk posed by the high-risk users by conducting behavioural analysis, comparison of user's behaviour with peer group and rule-based pattern analysis as shown in figure 1.

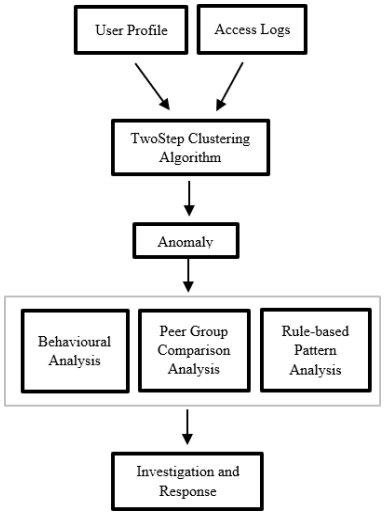

Figure 1: Anomaly Detection for Physical Access Logs

3.2 Two Step Clustering Method

Most anomaly detection methods use a supervised approach, which requires data that has already been labeled, i.e. normal user access versus malicious insider physical access. In the case of physical access log data, it is seldom the case. As such, we use an unsupervised machine learning algorithm which is designed for unlabeled data. In addition, physical access normally involves many users, cover multiple zones and require the running of huge volume of information with real time data streaming [15]. It is also important for the chosen algorithm to be scalable and not require any predefined rules or pattern.

The Two Step clustering algorithm involves two steps: Pre-clustering and Clustering. The pre-cluster step uses a sequential clustering approach. It scans the data records one by one and decides if the current record should be merged with previously into the desired number of clusters. Each cluster will form a peer group based on similarity in their physical access pattern and their job role and department.

The Two Step clustering method uses a log-likelihood distance measure. The distance between two clusters is related to the decrease in log-likelihood as they are combined into one cluster. In calculating log-likelihood, normal distributions for range fields and multinomial distributions for symbolic fields are assumed. It is also assumes that the fields are independent of each other, and so are the records. The distance between clusters i and j is defined as:

$$d(i,j) = \varepsilon_i + \varepsilon_j - \varepsilon_{(i,j)}$$

where

$$\xi_v = \left(\sum_{k=1}^{K^A} \frac{1}{2} \log\left(\hat{\sigma}_k^2 + \hat{\sigma}_{vk}^2\right) + \sum_{k=1}^{K^B} \hat{E}_{vk} \right)$$

and

$$\hat{E}_{vk} = -\sum_{l=1}^{Lk} \frac{N_{vkl}}{N_v} log \frac{N_{vkl}}{N_v}$$

In these expressions,

K^A is the number of range type input fields,
K^B is the number of symbolic type input fields,
L_k is the number of categories for the kth symbolic field,
N_V is the number of records in cluster v,
N_{vkl} is the number of records in cluster v which belongs to the lth category of the kth symbolic field,
$\hat{\sigma}_k^2$ is the estimated variance of the kth continuous variable for all records,
$\hat{\sigma}_{vk}^2$is the estimated variance of the kth continuous variable for records in the vth cluster
<i,j> is an index representing the cluster formed by combining clusters i and j.

The algorithm employed differentiate it from traditional clustering techniques by being able to handle both categorical and continuous variables [16]. This is unlike Euclidean distance which measures a straight-line distance between two clusters and can only measure continuous variable. Since the user's role and department are categorical data, the method is suitable for our framework.

The risk score computed is based on the log-likelihood distance measure between the user and the centroid of the user's cluster in a multidimensional space. The risk score indicates the level of deviation from the physical access pattern of the peer group. After

determining the number of users to be flagged as anomaly based on the company's operations and vulnerability to insider threats, the pre-determined number of users with the highest risk score will be highlighted to the security manager. These users are identified as people who are likely to have exhibited malicious physical access behaviour.

This algorithm also allows for an automatic selection of number of clusters. By comparing the values of a model-choice criterion across different clustering solutions, the procedure can automatically determine the optimal number of clusters. In addition, this algorithm is highly scalable. By constructing a cluster features (CF) tree that summarises the records, the Two Step algorithm enables the analysis of large data files. As there are large amount of physical access log data generated every day, it is important to have a system that is capable of analysing them in real-time.

4 Experiment Setup

We use the real-world data set collected from office buildings of a company with more than 5000 employees. There are 2 office buildings with a total of over 300 doors. In these buildings, most rooms require access other than areas like the toilet and the pantry. We estimate that there is an average of 27,000 accesses on a regular weekday and 12,000 accesses on a regular weekend. With such a huge number of accesses a day, it is difficult to identify any potentially malicious physical accesses manually.

We use the company's physical access log data form 1st April 2018 to 3rd July 2018 data. The data from 1st April 2018 to 30th June 2018 is used as training set, while July is the testing set with 3 days being selected as explanation in this paper. This allows us to evaluate the anomaly detection capabilities of the model for each of the three days since our use case focuses on the detection of daily anomalous activity.

5 Feature Engineering

In the area of physical access pattern, physical-world factors, such as time and space, directly impact the different access events. The time of access and physical access location are thus important inputs to our model.

Time and Location Variable. Most of the employees have a working hour of 8.30am to 6.00pm. However, there are also employees who work in shifts that may be classified into either night shift or weekend shift. The time pattern of access of the users are used as input for our model. Each location indicates one of the many door access points in a commercial building. The access pattern of the locations is also used in the model.

Job Profile Variable. As the job profile is an indicator of users' work schedule and locations, the job role and department of the users are also used as input for our clustering algorithm. Without which, we would not be able to find out whether the deviation in physical access pattern is simply due to a different job role and department. As such, the job profile variables are also important input to the model.

5.1 Data Pre-processing

The original physical access log is made up of access entries. The entries are processed to contain the following variables: count of location access (success and denied), count of weekday/weekend access (success and denied), count of day/night access (success and denied) and employees' job role and department.

For each employee, we identify the daily average number of accesses granted and denied for each location. These location access data points are physical access behavioral input to our clustering model. Other variables include the job role of the user, department of the user, the time pattern of the user's access behaviour, which include the access activities across time as defined in four periods including the day during a weekday, night during a weekday, day during the weekend and night during the weekend.

5.2 Monitoring of Anomalies

The following are monitoring measures used in our approach.

Risk Score. This measure is generated based on Cluster distribution. The following measures allow us to identify a smaller subset of the users for investigation.

(1) On a daily basis, most risky employees flagged based on his risk score.
(2) List of most risky employees based on risk score accumulated over a pre-defined period, (e.g. a month)
(3) Total risk score of all users in a day compared with previous day.

We can define a fixed number out of the 5000 users as anomaly based on the risk score of the users. This means that the effort required by the security manager to investigate the high-risk users would be reduced to this predefined number. In addition, we use rule-based violation pattern to help identify potentially malicious physical access behaviour.

Rule-based Violation Pattern. These are metrics to identify behaviour that may be considered anomalous regardless of the job profile of a user. Some of these metrics include:

(1) Staff tap in on day's off
(2) Staff not in duty roster tap in between 11pm to 6am,
(3) Staff tap in more than 10 times within 1-hour period,
(4) Staff tap in after terminated from service.

6 Applications

In this section, we illustrate the anomaly detection capabilities of our approach to physical access log data. The Two Step clustering algorithm is used for the identification of high-risk users. Among these users, we compare the user's physical access pattern with its peer group to evaluate the type of risk posed by the user.

From the 8 clusters formed, we are able to identify distinct pattern between of the clusters. Most of the clusters are formed by users from the same job role and department due to similar job tasks, and therefore, similar work schedule and access location. There are also distinct clusters that are made up of users with irregular work schedule, for example early morning and late-night shifts. The distinct patterns exhibited between the clusters align with our expectation based on the company's operations.

The following charts illustrate a few of the data visualisation we

use to identify the type of risk involved.

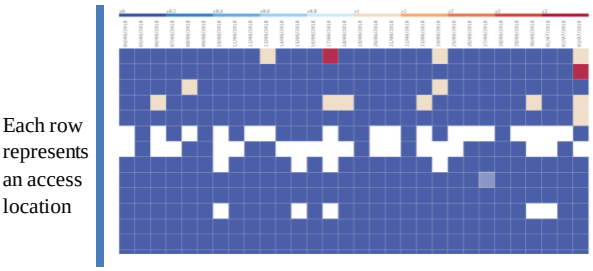

Figure 2: Heatmap showing access pattern of an employee for the last 30 days

Prior to anomaly detection analysis, the physical access pattern of the high-risk user is identified through a visual inspection of the access count data to different locations for each day as shown in figure 2. The access frequency in the heat map is highlighted across a range of colours from dark blue to dark red, highlighting the lowest access count to the highest access count of the day respectively. For 3rd July 2018, the most frequently accessed location is the main gate to the building since it is an access point that all employees pass through for work. Locations that have not been accessed on that day include areas like server room and storeroom, where users access only for specific reasons or locations like the designated carpark, where only a select few employees have access to. The initial statistical analysis is consistent with expectation based on the company's operations.

The visual inspection of other measurements for the comparison with user's peer group includes the access count for the past 30 days, access count for the frequently accessed locations, and access pattern across time as compared to a user's peer group as shown in figure 3, 4 and 5.

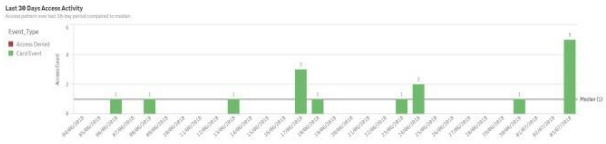

Figure 3 Access count for the same employee showing high level of door access on July 3 compared to his last 30 days

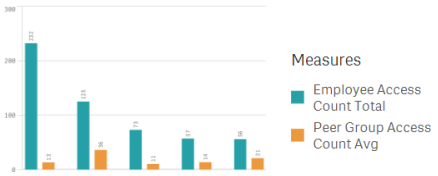

Figure 4: Access count per location as compared to peer group for last 30 days

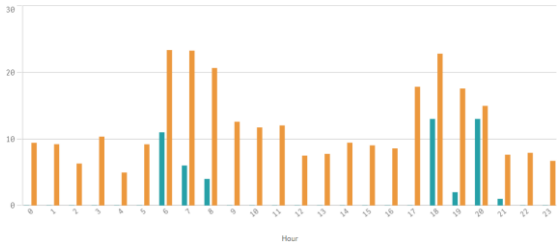

Figure 5: Access count across time as compared to peer group for the last 30 days

These visualisation charts can help identify any suspicious deviation in the user's behaviour. After assessing the access location and time of access, the security manager would be able to identify the type of risk posed and investigate the situation more thoroughly.

In the following case studies, we use real life data of 3 users based on data from 3rd July 2018 to illustrate our analysis using behavioral pattern and peer group comparison. They are users flagged as high-risk by our clustering algorithm.

For the first case, we detected an access card with access counts that are multiple fold as compared to its peers as shown in figure 4. This triggered an investigation where we found that the pattern is generated by a temporary pass that has been shared among different visitors. The pass has also been found to have access to one of our highly restricted area. In order to mitigate the possible insider threat, we reviewed the temporary pass policies and developed a stricter tracking of temporary pass.

In the second case, we identified a high-risk user with a distinctly different physical access pattern compared to the peers as shown in figure 5. The physical access pattern indicates that user accessed the building only on certain hours as compared to its peers. This could mean that his job tasks require him to be assigned to places outside of the building. Other possible reasons include performance issues or special assigned task. For such a case, we require more investigation to identify any possible threats.

The user for our last case has substantially higher access counts compared to the others within its peer group. We found out that the user has accessed the building even during days when he is not assigned any duties. This pattern may increase the vulnerability of the organisation to insider threat where by the user take advantage of the organisation's asset during non-scheduled working hour. This case prompted a review to investigate the need to have a restricted access policy during non-scheduled working shift for areas that are highly vulnerable to insider threats.

7 Comparison of Models

In the field of physical access security, the following are models that have been applied for anomaly detection.

A similar density-based model to the Two Step Clustering is the Expectation-Maximization (EM) algorithm. It is a way to find maximum-likelihood estimates for model parameters when there is incomplete data, missing data points, or has unobserved latent variables. It is an iterative way to approximate the maximum likelihood function. Although the model has high scalability, its iteration process towards maximum may be slow.

Two Step Clustering Algorithm is being chosen because of its ability to consider both categorical and continuous data and high scalability. As real time anomaly detection is required, EM Clustering's slow convergence speed makes it unsuitable for our framework.

In the field of physical access security, the following recent approaches have been applied for anomaly detection using physical access logs as shown in figure 6. Davis et al. [11] uses search labeled graphs for both structural and numeric anomalies and apply their approach to physical access logs in an office building. Another approach by Cheh et al. [12] uses knowledge of the system and its users to analyse physical access log for the detection of malicious behaviour. It uses Markov model and is implemented in a railway station, which has a highly restricted number of paths a user can take. The following illustrate the comparisons between our approach and these recent approaches

Method	**Cheh et al.**	**Davis et al.**	**Our Approach**
Model	Markov Model	Graph-based Anomaly Detection Algorithm YAGADA	TwoStep Clustering Algorithm
Setting	Railway station	Office Building	Office Building
Strength	- Highly scalable - Considers the profile of users - Measures degree of anomalousness	- Able to consider both structural anomalies (unusual paths through the building) and numeric anomalies (unusual timing data).	- Highly scalable - Considers the profile of users - Does not require the predefined rules or patterns - Measures degree of anomalousness
Limitations	- Requires knowledge of system layout	- No measure of degree of anomalousness	- Unable to consider structural anomalies

Figure 6: Recent approaches to anomaly detection using physical access log data

8 Discussion and Future Work

In an office building, the job roles of users are different in terms of work shifts, responsibilities and work location. The actual role for users of the same job title may also differ from one department to another. Users of the same job title and department may even have different physical movement behaviour within the building due to their assigned duties and personal habits. In addition, there are many users that do not have clearly labelled job role or department. As these variables are important inputs to the clustering algorithm, users with poorly labelled job role or department may result in improper clusters. This weakens the anomaly detection capabilities of the model.

In this paper, we only consider the behaviour of each user individually in the Two Step clustering algorithm. Our approach would not be able to handle colluding insider who exhibit normal behaviour but are able to achieve their malicious goal by working together. It may also be difficult to identify physical movements of users with certainty as there are many cases where movements within a building are not tracked. This occurs when readers fail, certain doors are not outfitted with card readers or when people enter by tailgating. We will not be able to determine a user's full movement in these cases. This makes it challenging to detect deviations in a user's movement behaviour.

9 Conclusion

In our paper, we proposed an unsupervised machine learning model, a Two Step clustering approach, to anomaly detection. In our model, we characterised the users based on their physical access history and job profile, which include their role and department within the organisation. Using the Two Step clustering approach, the model learns the users past physical access behaviour and group users based on similarity in terms of physical access behaviour and job profile. We use the level of deviation of a user from the peer group behaviour as input into the model and generate a risk score which measures the likelihood of a user access being anomalous. We apply our framework to a real-world data of physical access log in an office building. We then evaluate its effectiveness by comparing the other recent approaches for anomaly detection of physical access logs. The results from the deployment to a real-world environment showed that this framework is useful in providing a useful way of identifying potentially malicious physical accesses.

REFERENCES

[1] Louisa Tang. "Changi Airport technician illegally enters transit area to buy duty-free items, re-sell for profit," TODAYonline. [Online]. Available: https://www.todayonline.com/singapore/changi-airport-technician-illegally-enters-transit-area-buy-duty-free-items-re-sell-profit. [Accessed: 13-Dec- 2019].

[2] Varieto Insider Threat Report 2018 https://www.veriato.com/ resources/ whitepapers/ insider-threat-report-2018 [Accessed: 3-Jan-2020].

[3] A Frei and M. Rennhard. Histogram matrix: Log file visualization for anomaly detection. In Availability, Reliability and Security, 2008. ARES 08. Third International Conference on, pages 610–617, March 2008.

[4] Q. Fu, J.-G. Lou, Y. Wang, and J. Li. Execution anomaly detection in distributed systems through unstructured log analysis. In Proceedings of the 2009 Ninth IEEE International Conference on Data Mining, ICDM '09, pages 149–158, Washington, DC, USA, 2009. IEEE Computer Society.

[5] Juvonen A, Sipola T, Hamalainen T. Online anomaly detection using dimensionality reduction techniques for http log analysis. Comput Netw 2015;91;46-56

[6] Krugel C, Vigna G. Anomaly detection of web-based attacks. In: Proceedings of the 10th ACM conference on computer and communications security; CSS '03. New York, NY, USA: ACM; 2003. p. 251-61.

[7] Amor NB, Benferhat S, Elouedi Z. Naïve bayes vs decision trees in intrusion detection systems. In: Proceedings of the 2004 ACM symposium on applied computing, SAC '04. New York, NY, USA; ACM; 2004. P. 420-4.

[8] Yassin A, Cao F, Qian W, Jin C. Tracking clusters in evolving data streams over sliding windows. Knwl Inf Syst 2008;15(2):181-214

[9] Wurzenberger M, Skopik F, Landauer M, Greitbauer P, Fiedler R, Kastner W. Incremental clustering for semi-supervised anomaly detection applied on log data. In: Proceedings of the 12th international conference on availability, reliability and security. ACM; 2017. P. 31.

[10] Eberle, W., Holder, L.: Anomaly detection in data represented as graphs. Intelligent Data Analysis: An International Journal 11(6) (2007) 663–689

[11] Davis, M., Liu, W., Miller, P., Redpath, G.: Detecting anomalies in graphs with numeric labels. In: Proc. 29th ACM Conf. on Information and Knowledge Management. (2011) 1197–1202

[12] C. Cheh, B. Chen, W. G. Temple, and W. H. Sanders, "Data-Driven Model- Based

Detection of Malicious Insiders via Physical Access Logs," p. 16.
[13] David Hutter. Physical Security and Why It Is Important. SANS Institute Information Security Reading Room Available: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important -37120
[14] Harris, S. Physical and Environmental Security. In CISSP Exam Guide (6th ed., pp. 427-502). (2013). USA McGraw-Hill;
[15] Fitzgerald, Turkmen, Foley, O'Sullivan, Anomaly Analysis for Physical Access Control Security Configuration, Crisis 2012, V9
[16] IBM Knowledge Center. [Online]. Available: https://www.ibm.com/ support/knowledge center/SSLVMB_23.0.0 /spss/product_landing.html. [Accessed: 17-Dec-2019].
[17] IBM Support. [Online]. Available: https://www.ibm.com/support/pages/how-log-likelihood-distance-method-applied-twostep-cluster-analysis. [Accessed: 17-Dec-2019].