

סקירת ספרות: זיהוי וסיווג מתקפות סייבר בסביבות ענן באמצעות למידת מכונה

ספר שנהב ועופרי גראס

1. אבטחת מידע בסביבות ענן

סביבות מחושב ענן כגון AWS, Azure ו-GCP הפכו בעשור האחרון לתשתיית מרכזית וקריטית עבור ארגונים ומערכות מודרניות. המעבר לענן הביא עמו יתרונות רבים של גמישות וגידול, אך במקביל יצר מרחב תקיפה חדש ומורכב. סביבות אלו מייצרות לוגים מפורטים מאוד, כגון AWS CloudTrail המתעדים באופן רציף קרייאות API, זהויות משתמשים (IAM Users), שירותים (כגון S3, EC2) ואזרחים גאוגרפיים וזמן ביוצע.

למרות עושר וזמינות המידע, נפח הנתונים העצום והמורכבות ההתנהגותית של משתמשים לגיטימיים מחייבים מאוד על ניתוח ידני או מבוסס כללים פשוטים של הלוגים. כто札ה מכץ, זיהוי מתקפות בסביבות ענן הפך לאתגר מחקרי וטכנולוגי משמעותי. כפי שמציניהם (Sharma et al. 2017), האתגר המרכזי בענן אינו רק אישור הנתונים, אלא היכולת להבחין בין פעילות עסקית רגילה לבין דפוסי פעילות זדוניות המנסים להסתנות בפעולות תקינה. המחקר מדגיש כי מתקפות בענן הן לרוב התהליכים משתמשים ולא אירועים נקודתיים, מה שדורש גישות ניתוח מתקדמות.

2. גישות לזיהוי מתקפות מבוססות לוגים

2.1 גישות מבוססות חוקים (Rule-Based)

מערכות אבטחה מסורתיות, כגון מערכות IDS (Intrusion Detection Systems) קלאסיות, נשענות על חוקים או חתימות ידועות מראש לצורך זיהוי פעילות חשודה. חוקים אלו עשויים לכלול זיהוי של פעולות רגיסטרציה במילוי, ניסיונות הרשות חריגים (Unauthorized access) או דפוסי שימוש לא שגרתיים במשאבי מחשב.

למרות פשטותן ויכולת ההסבר הגבוה שלן (שכן קל להבין מידע חוק מסוים "קפץ"), גישות אלו סובלות מגבלות קשות בסביבות ענן דינמיות. הן מתקשות להתמודד עם מתקפות "יום אפס" (Zero-day) או עם שינויים קלים בהתנהגות התוקף, ודורשות תחזקה ידנית מתמדת של בסיס החוקים. בנוסף, כפי שמציניהם Sommer & Paxson (2010), מערכות מבוססות חוקים מתקשות לזהות מתקפות מורכבות המורכבות מרצפים של פעולות שנראות לגיטימיות כשלעצמם (Living off the Land) אך יחד הן מהוות וקטור תקיפה.

2.2 למידת מכונה (Machine Learning) לזיהוי מתקפה

כדי לגשר על פערו הגישות המסורתית, המחקר האקדמי והתעשייתי פנו לשימוש באლגוריתמים של למידת מכונה לנתח לוגים. לפי (Kim et al. 2018), שיטות אלו מאפשרות למדוד את ההתנהגות הנורמלית של המערכת ולזהות חריגות (Anomalies) באופן אוטומטי. הגישות נחלקות לשתי קטגוריות:

- **למידה לא-מנומחת (Unsupervised)**: שטרתה לזהות חריגות ללא ידע מוקדם או לייבלים, בדרך כלל באמצעות Outlier Detection או Clustering.
- **למידה מונחית (Supervised)**: שבה נעשה שימוש בתנונים היסטוריים הכלולים לייבלים המנסנים פעילות תקינה לעומת זדונית.

בלמידה מונחית, המודל לומד הקשר בין מאפיינים סטטיסטיים (Features) לבין סיווג האירוע. זהה הגישה שנבחרה לפROYיקט זה, שכן היא מאפשרת דיקוק גבוה בזיהוי סוגים מתקפות מוכרים וمتבססת על ידע מוקדם של דפוסי תקיפה בענין.

3. ניתוח התנהגותי מבוסס חלונות זמן

אחד התובנות המרכזיות במחקר של Lopez et al. (2019) היא שימושות ענן אינן מתרחשות לרוב כאירוע בלבד. תוקף המבצע סריקה (Reconnaissance) או תנועה רוחבית (Lateral Movement) מבצע סדרה של פעולות לאורך זמן. לכן, ניתוח של שורת לוג בודדת אינו מספק מספיק הקשר (Context) כדי לקבוע אם מדובר בתקיפה.

הפתרון המקביל הוא איחוד אירועים בודדים לתוך **חלונות זמן קבועים** (Time Windows). הניתוח מתבצע ברמת החלון, כאשר לכל חלון מופקים מאפיינים מצטברים כגון:

- מספר האירועים הכלול בחלון הזמן.
- מספר פעולות API ייחודיות (מגוון הפעולות של המשתמש).
- מספר השירותים והאזורים (Regions) השונים אליהם פנה המשתמש.
- מספר כתובות ה-IP השונות ששימשו לביצוע הפעולות.
- נוכחות של פעולות ניהול (Management events) או פעולות כתיבה/מחיקה רגיסטר.

גישה זו מאפשרת למודלים של למידת מכונה לזהות דפוסים מתמשכים ולהפחית רעש הנובע מפעולות בודדות, שאין מעידות על כוונה זדונית. בפרויקט הנוכחי יושמה גישה זו באמצעות חלונות זמן באורך של 20 דקות, שהוכחה במחקריהם קודמים כאיזון נכון בין זיהוי מהיר לבין צבירת מספיק תנאים לאפיון התנהגות.

4. מודלים לסיווג מתקפות – הרחבה והשווואה

במסגרת המחקר, הتمקדמו בהשוואה בין שני מודלים מרכזיים המיצגים גישות שונות בלמידה מונחית:

4.1 רוגסיה לוגיסטיבית (Logistic Regression)

רגסיה לוגיסטיבית היא מודל בסיסי (Baseline) נפוץ מאוד בתחום אבטחת המידע בזכות פשוטותו, מהירות האימון שלו ויכולת ההסביר (Interpretability). המודל מנסה קשרilinear בין המאפיינים (כמו מספר ה-IPs) לבין הנסיבות שהחלון הוא "תקיפה". בפרויקט זה, הרגסיה הלוגיסטיבית שמשה כקו בסיס. למורות שהשיגה

תוצאות סבירות, היא מוגבלת ביכולתה לזהות קשרים מורכבים – למשל, מצב שבו מספר פעולות הוא תקין באזור אחד אך נחשב לתקיפה באזור אחר.

Random Forest 4.2

מודל ה-Random Forest הוא אלגוריתם מסווג Ensemble המשלב מספר רב של עצי החלטה. לפי הספרות, מודלים מבוססי עצים מתאימים במיוחד לנוטרי לוגים של ענן מכמה סיבות:

1. **התמודדות עם נתוני הטרוגניטס**: לוגים מכילים ערכיים מספריים וקטגוריאליים גם יחד.
2. **עמידות לחוסר איזון (Data Imbalance)** : בעית יסוד בזיהוי מתקפות היא שרוב הדאטה הוא "תקין". Random Forest יודע להתמודד טוב יותר עם מחלקות מייעוט.
3. **זיהוי אינטראקציות לא-lienאריות**: המודל מסוגל לזהות שילובים מורכבים של מאפיינים המעידים על תקיפה. בפרויקט זה, ה-Random Forest נבחר כמודל המרכזי לאחר שהציג ביצועים עדיפים משמעותית, במיוחד במדד ה- F1 המאזן בין דיוק (Precision) לרגשות (Recall).

5. סיוג רב-מחלקי (Multi-class Classification) ואתגריו

מעבר לשאלת הבינהנית "האם יש תקיפה?", ארגונים זוקקים לדעת על סוג התקיפה כדי להגיב נכון. מחקרים מתקדמים מחלקים את התקיפות לפי מסגרות עבודה כגון **MITRE ATT&CK**. סוגי התקיפות שנבחנו כוללים:

- - Reconnaissance - סריקת הרשאות ומשאיים.
- - Cryptojacking - ניצול כוח עיבוד של EC2 לкриipt מטבעות.
- - Lateral Movement - ניסיון לעبور בין זהויות ושירותים.
- - Billing Attacks - יצירת משאיים יקרים כדי לגרום נזק כלכלי.

הסיוג הרב-מחלקי מציב אתגרים טכניים משמעותיים: חוסר איזון קיצוני (סוגי התקיפה נדירים מאוד) וחפיפה התנהגותית. בפרויקט זה בוצע עיבוד מקדים שככל Label Encoding וסינון רעים (הסרת התקיפות עם פחות מ-2 מופעים). המודלים הושוו באמצעות **Weighted F1 Score** כאשר ה-Random Forest הוביל עם ציון של 0.88 לעומת 0.82 של הרגרסיה הלוגיסטיבית, מה שמכיחה את עלילותו בטיפול בדאטה מורכב ולאamazon.

6. ייחוס תוקפים (Attribution) וניתוח פост-אנליטי

Zuech et al. (2015) מודגש במחקריהם של (2015) זיהוי של חלון זמן זדוני הוא רק תחילת האירוע. שלב קרייטי נוסף, המאפשר במחקריהם של (2015) זיהוי תוקף – Attribution (היכולת לקשר בין אירועי אירועים לבין זהות ספציפית או קומפין). בפרויקט זה יושמה שכבת ניתוח פост-אנליטית המבצעת איגום Aggregation של תוצאות המודל. במקרה להסתכל על כל חלון בנפרד, הסתכלו על רצף ההצלחות המשווים לכל משתמש. גישה זו אפשרה לנו:

- לזיהות את התוקפים המרכזיים במערכת.
- להבחן בין תוקפים "רועשים" (שמבצעים פעולות רבות בזמן קצר) לבין תוקפים "שקטים" שפעלים לאורך זמן. הממצאים הראו כי מתוך 11 זהויות שזוהו כחמודות, רק 5 היו אחראיות לרוב המכريع של הפעולות הזדונית. נמצא זה משמש את ההנחה המקראית כי מספר קטן של תוקפים מיומנים מוביל קומפינאים משמעותיים במערכות ענן.

7. סיכום והקשר לפרויקט הנוכחי

הפרויקט הנוכחי מישם הלכה למעשה לתובנות העולות מן הספרות האקדמית. שילבנו גישה מונחית המבוססת על חלונות זמן (20 דקות) עם מודלים של מידת מכונה (LR ו- RF). העבודה כוללה Pipeline מלא: החל מעיבוד מקדים StandardScaler (דרכן אופטימיזציה threshold להתרומות עם חוסר איזון, ועד לשכבה הייחס הפост-אנליטית. התוצאות, שהראו עדיפות ברורה ל- Random Forest מדגימות את החשיבות של בחירת מודל המສוגל להתרום עם המרכיבות הלא-ליניאריות של לוגי-CloudTrail. שילוב זה מאפשר מעבר מזיהוי נקודתי של אירועים בודדים להבנה מערכתית ומושכלת של איום סייבר בסביבת הענן.

#	מסקנה מההשוואה	תצאה (Score)	מדד הערבה	קובחת נתונים	מחל	שלב הניתוח
0.91	בער-קען מאדן בין איכון לוידציה מעוד מודול יציב.	0.91	(Train) F1-Score	סיווג בין-ארוי	Random Forest	
0.883		0.883	(Val) F1-Score			
0.98	תוצאות גבירות בשני השלבים, אך המודל בשוטה כדי לדפוסים מוכרים.	0.98	(Train) Accuracy		Logistic Regression	
0.976		0.976	(Val) Accuracy			
0.92	המודל מציאות להכליל טוב גם בשיש הרובה סוג תקיפה.	0.92	(Train) Weighted F1	סיווג רב-מחלקי	Random Forest	
0.883		0.883	(Val) Weighted F1			
0.84	ירידה ביציעים מעבר לר-מחלקי עקב ליגיאריות המודל.	0.84	(Train) Weighted F1		Logistic Regression	
0.822		0.822	(Val) Weighted F1			

מקורות :

Al-Zewairi, M., et al. (2020). "Deep Learning for Cloud Intrusion Detection Systems: A Survey."

AWS CloudTrail Documentation. Official technical guide.
<https://docs.aws.amazon.com/cloudtrail/>

Buczak, A. L., & Guven, E. (2016). "A Survey of Data Mining and Machine Learning Methods for Cybersecurity Intrusion Detection."

Chawla, N. V. (2009). "Data Mining for Imbalanced Datasets: An Overview."

Injadat, M., et al. (2020). "Multi-stage Optimized Machine Learning Framework for Intrusion Detection."

Kim, J., et al. (2018). "Detecting malicious activities in cloud environments using machine learning." *Computers & Security*.

Lopez, M., et al. (2019). "Behavior-based anomaly detection in cloud systems." *Future Generation Computer Systems (FGCS)*.

MITRE ATT&CK Framework. Cloud Matrix documentation. <https://attack.mitre.org/>

Sharma, A., et al. (2017). "Cloud security issues and challenges: A survey." *IEEE International Conference on Computing, Communication and Automation*.

Sommer, R., & Paxson, V. (2010). "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection." *IEEE Symposium on Security and Privacy*.

Zuech, R., et al. (2015). "Intrusion detection and Big Data Analytics - A Survey." *Journal of Big Data*.