تعزيز الأمن السيبراني في البيئات متعددة السحابات عبر الكشف المبكر عن الهجمات الموزعة: إطار قائم على المحاكاة الاحتمالية

الدكتور عصام محمد اسعد *

الملخص

تواجه المؤسسات العاملة في بيئات متعددة السحابات تحديات أمنية متنامية نتيجة لتوزع البيانات والأعباء التشغيلية عبر منصات مختلفة، مما يفتح المجال أمام هجمات موزعة مثل حجب الخدمة وانتحال الهوية. لمعالجة هذه المشكلة، يقترح البحث إطاراً رياضياً قائماً على المحاكاة الاحتمالية للكشف المبكر عن الهجمات، يعتمد على سلاسل ماركوف لتمثيل الحالات الأمنية، ونماذج الأرتال M/M/1 لتوصيف أثر الهجمات على الأداء، إلى جانب إحصاء نسبة الإمكان للتمييز بين الحالة الطبيعية والهجوم. تم اختبار النموذج عبر محاكاة كمية باستخدام MATLAB ومجموعة بيانات شبه واقعية(CICIDS2017) ، وأظهرت النتائج قدرة على الكشف خلال أقل من 20 خطوة زمنية في المحاكاة و15 خطوة زمنية مع البيانات الواقعية، مع معدل كشف يقارب 95- 96% وإنذار كاذب لا يتجاوز 4-5%، كما أثبت منحنى ROC تفوق النموذج على أساليب الكشف المعتمدة على مزود واحد، مما يجعله إطاراً عملياً لتعزيز الأمن السيبراني في البيئات متعددة السحابات.

الكلمات المفتاحية

الأمن السيبراني متعدد السحابات، الكشف المبكر عن الهجمات الموزعة، سلاسل ماركوف، نماذج الأرتال M/M/1 ، الإحصاء الاحتمالي، بيانات CICIDS2017 .

***الدكتور عصام محمد اسعد / 0992998801 - 0993998331 /Essam.ryha@gmail.com /**
عضو هيئة تدريسية في الجامعة العربية الخاصة للعلوم والتكنولوجيا – كلية الهندسة المعلوماتية - مدرس.

Enhancing Multi-Cloud Cybersecurity through Early Detection of Distributed Attacks: A Probabilistic Simulation Framework

Abstract

Organizations operating in multi-cloud environments face growing security challenges due to distributed data and workloads, which expose them to attacks such as DDoS (Distributed Denial of Service) and identity leakage. To address this, the paper proposes a probabilistic simulation framework for early detection of distributed attacks, combining Markov chains to represent security states, M/M/1 queueing models to capture performance degradation, and likelihood ratio statistics to distinguish normal from abnormal behavior. The model was evaluated through quantitative simulations in MATLAB and applied to semi-realistic data (CICIDS2017). Results show detection within fewer than 20-time steps in simulation and 15-time steps with real-world data, achieving a detection rate of 95-96% and a false alarm rate of 4-5%. The ROC (Receiver Operating Characteristic) curve further confirms the superiority of the proposed approach over traditional single-provider detection methods, offering a practical framework to strengthen cybersecurity in multi-cloud environments.

Key Words

Multi-Cloud Cybersecurity, Early Detection of Distributed Attacks, Markov Chains, M/M/1 Queueing Models, Probabilistic Statistics, CICIDS2017 Dataset.

1. المقدمة

1.1 أهمية الأمن السيبراني في البيئات متعددة السحابات

تُعد الحوسبة السحابية ركيزة أساسية للبنية التحتية الرقمية الحديثة، حيث توفر مرونة عالية في إدارة الموارد وتشغيل التطبيقات. ومع توسع المؤسسات في الاعتماد على بيئات متعددة السحابات (Multi-Cloud) التي تجمع بين خدمات مزودين (Cloud Security Alliance, 2022) مثل Amazon Web Services، Microsoft Azure، Google Cloud، برزت تحديات أمنية جديدة نتيجة لتوزع البيانات والأعباء التشغيلية عبر منصات مختلفة ذات سياسات غير موحّدة، يوسع هذا التوزع سطح الهجوم ويزيد من صعوبة الكشف المبكر عن التهديدات الموزعة مثل هجمات حجب الخدمةDDoS: Distributed Denial of Service أو انتحال الهوية.

1.2 واقع الاعتماد علىMulti-Cloud

رغم المزايا الاستراتيجية للتعدد في المزودات –كتجنب الارتباط الأحادي(Vendor Lock-in) ، وتحسين زمن الاستجابة، وضمان استمرارية الخدمة– إلا أن هذا التوزيع للبيانات والأحمال يُوسّع سطح الهجوم ويزيد من تعقيد التهديدات.

تُظهر الدراسات الحديثة ما يلي:

1) في أكتوبر 2025، تمكنت منصة Azure من صدّ أكبر هجوم DDoS مسجّل بحجم 15.72 تيرابت/ثانية(Khadka et al., 2026).
2) الدراسة Cloudflare أشارت إلى أن يونيو 2025 وحده شكّل 38% من النشاط العالمي للهجمات الموزعة (Chuah, Jhumaka and Ayesh, 2025).
3) الدراسة NETSCOUT سجّلت أكثر من 8 ملايين هجوم خلال النصف الأول من 2025، بعضها استهدف بنى تحتية متعددة السحابات عبر شبكات أجهزة مخترَقة متقدمة (Xie et al., 2016).

تؤكد هذه الأمثلة الواقعية أن المؤسسات العاملة في بيئات متعددة السحابات تواجه تهديدات متنامية ومعقدة، مما يبرز الحاجة إلى نماذج رياضية وخوارزميات جديدة للكشف المبكر والاستجابة الفعالة.

1.3 الدراسات السابقة (Related Work)

تناولت عدة دراسات التحديات الأمنية في البيئات السحابية، ويمكن تلخيص أبرزها كما يلي:

1) **Xu & Sandhu (2019):** استخدما سلاسل ماركوف لتحليل "سلاسل القتل السيبراني"، لكن عملهما اقتصر على توصيف الهجمات دون دمج مؤشرات تشغيلية أو محاكاة كمية (Xu and Sandhu, 2019).
2) **Abiramasundari & Ramaswamy (2024):** قدما إطاراً يعتمد على خوارزميات تعلم آلي للكشف عن هجمات DDoS باستخدام بياناتCICIDS2017 ، لكنه يقتصر على بيئة مزود واحد ولا يعالج التكامل متعدد السحابات (Abiramasundari and Ramaswamy, 2024).
3) **Annoo (2023):** ناقش التحديات الأمنية في البيئات متعددة السحابات من منظور وصفي، مع التركيز على سياسات الامتثال، دون تقديم نموذج رياضي أو خوارزمية للكشف المبكر(Annoo, 2023)
4) **IEEE Access (2024):** دراسة مراجعة منهجية للتحديات الأمنية في البيئات متعددة السحابات، لكنها اقتصرت على الجانب الوصفي ولم تقدم حلول كمية أو نماذج قابلة للتطبيق(IEEE Access, 2024) .

(جدول 1: مقارنة بين أبرز الدراسات السابقة والنموذج المقترح)

الدراسة	نوع المنهجية	بيئة التطبيق	نقاط القوة	نقاط الضعف
(Xu and Sandhu, 2019)	سلاسل ماركوف لتحليل سلاسل القتل السيبراني	بيئة مزود واحد	يقدم توصيفاً نظرياً للهجمات	يفتقر إلى مؤشرات تشغيلية ومحاكاة كمية
(Abiramasundari and Ramaswamy, 2024)	خوارزميات تعلم آلي باستخدام بيانات CICIDS2017	بيئة مزود واحد	دقة جيدة في كشف هجماتDDoS	يقتصر على مزود واحد ولا يعالج التكامل متعدد السحابات
(Annoo, 2023)	إطار وصفي للتحديات الأمنية	بيئات متعددة السحابات (وصفي)	يبرز أهمية الامتثال والسياسات	لا يقدم نموذج رياضي أو خوارزمية للكشف المبكر
(IEEE Access, 2024)	مراجعة منهجية للتحديات الأمنية	بيئات متعددة السحابات	تحليل شامل للأدبيات	لا يقدم حلول كمية أو نماذج قابلة للتطبيق
البحث الحالي	نموذج رياضي (ماركوف + نماذج الأرتال + إحصاء احتمالي) + خوارزمية عملية	بيئات متعددة السحابات + بيانات شبه حقيقية (CICIDS2017)	يجمع بين النظرية والتطبيق، قابلية التكرار، نتائج كمية قوية 95–96% كشف 4–5%إنذار كاذب	كفاءة $O(N^2)$ تحد من التوسع لأكثر من 5–10 مزودات

1.4 مشكلة البحث

رغم أهمية هذه الدراسات في تسليط الضوء على التحديات الأمنية، إلا أنها تفتقر إلى نموذج رياضي تطبيقي متكامل يجمع بين النظرية الرياضية (سلاسل ماركوف + نماذج الأرتال) والإحصاء الاحتمالي مع اختبار عملي عبر المحاكاة الكمية وبيانات شبه واقعية. هذه الفجوة البحثية هي ما يسعى هذا البحث إلى سدّه من خلال تقديم إطار رياضي خوارزمي قابل للتنفيذ والتكرار، يعزز قدرة المؤسسات على مواجهة التهديدات السيبرانية في البيئات متعددة السحابات.

1.5 أهمية البحث

تواجه المؤسسات العاملة في البيئات متعددة السحابات تحديات أمنية متزايدة نتيجة لتجزؤ السياسات والأدوات بين المزودين المختلفين، مما يضعف القدرة على الكشف المبكر عن الهجمات الموزعة ويؤدي إلى استجابة غير موحّدة للحوادث الأمنية. ورغم أن كل مزود يقدم أدوات قوية داخل بيئته الخاصة، إلا أن الاعتماد عليها منفردة لا يحقق حماية شاملة في سياق متعدد السحابات. وهنا تكمن أهمية هذا البحث: تقديم إطار رياضي متكامل يجمع الرصد الأمني من مزودات متعددة، ويعالج تجزؤ السياسات، مما يُحسّن قدرة المؤسسات على اكتشاف التهديدات السيبرانية المتصاعدة والتصدي لها.

1.6 أهداف البحث

يهدف هذا البحث إلى تحقيق ما يلي:

1) **اقتراح نموذج رياضي احتمالي للكشف المبكر** عن الهجمات الموزعة في البيئات متعددة السحابات، بالاعتماد على سلاسل ماركوف ونماذج الأرتال والإحصاء الاحتمالي.

2) **اختبار النموذج عبر محاكاة كمية ومجموعة بيانات شبه واقعية** (CICIDS2017) لضمان دقة النتائج وقابليتها للتطبيق العملي.

3) **مقارنة النتائج مع أساليب الكشف المعتمدة على مزود واحد،** لإبراز تفوق النموذج المقترح من حيث سرعة الكشف، معدل الإنذار الكاذب، وقابلية التنفيذ في الزمن الحقيقي.

2. موارد البحث وطرائقه

2.1 النموذج الرياضي

يعتمد النموذج المقترح على دمج ثلاثة محاور رياضية رئيسية :سلاسل ماركوف لتمثيل الحالة الأمنية، نماذج الأرتال M/M/1 لتوصيف الأداء تحت الضغط، وإحصاء نسبة الإمكان للتمييز بين الحالة الطبيعية والهجوم.

1) تمثيل الحالة الأمنية كسلاسل ماركوف (Ross, 2014;Xu and Sandhu, 2019)

نفترض أن الحالة الأمنية لكل مزود سحابي i يمكن أن تكون طبيعية (0) أو تحت هجوم (1).

نُعرّف متغير الحالة عند الزمن t كما يلي:

$$X_t^{(i)} \in \{0,1\}, \quad i = 1,2,\dots,N$$

حيث N عدد المزودين. احتمالات الانتقال بين الحالات تُعطى بالمعادلات(Ross, 2014):

$$P\left(X_{t+1}^{(i)} = 1 \mid X_t^{(i)} = 0\right) = \alpha_i \qquad (1)$$

$$P\left(X_{t+1}^{(i)} = 0 \mid X_t^{(i)} = 1\right) = \beta_i \qquad (2)$$

تمثل α_i معدل ظهور الانحراف الأمني، بينما β_i معدل التعافي. وللتعبير عن الترابط بين المزودين تحت الهجمات الموزعة، نضيف معامل ارتباط ρ_i

$$P\left(X_{t+1}^{(i)} = 1 \mid X_t^{(i)} = 0, \left\{X_t^{(j)}\right\}_{j\neq i}\right) = \alpha_i \cdot \left(1 + \rho_i \cdot \frac{\sum_{j\neq i} X_t^{(j)}}{N-1}\right) \qquad (3)$$

حيث:

$S_t = \left\{X_t^{(j)}\right\}_{j\neq i}$ هي حالات بقية المزودين عند الزمن t

ρ_i معامل الارتباط بين المزودين، ويمثل شدة انتشار الهجوم من مزود إلى آخر، حيث $0 \le \rho_i \le 1$.

2) نموذج الأرتال لأداء الخدمة (Gross et al., 2008;Kleinrock, 1975)

نُقارب كل مزود كنظام أرتال$M/M/1$ حيث معدل الوصول λ_i ومعدل الخدمة μ_i شرط الاستقرار هو $\lambda_i < \mu_i$ متوسط زمن الانتظار يُعطى بالمعادلة:

$$W_i = \frac{1}{\mu_i - \lambda_i} \qquad (4)$$

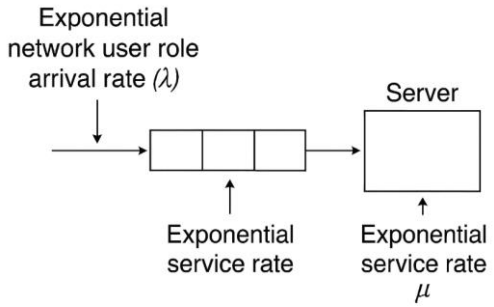
وتحت الهجوم الموزع (DDoS) ، يُعدل معدل الوصول إلى:

$$\lambda_i' = \lambda_i(1+\delta_i), \quad \delta_i > 0 \qquad (5)$$

δ_i : "معامل شدة الهجوم" على المزود i (النسبة المئوية للزيادة في معدل وصول الطلبات إلى المزود i نتيجة الهجوم الموزع) مما يؤدي إلى تضخم زمن الانتظار:

$$W_i' = \frac{1}{\mu_i - [\lambda_i(1+\delta_i)]} \qquad (6)$$

يُستخدم هذا التضخم كمؤشر رياضي للكشف المبكر عن الهجمات.



(شكل 1: نموذج الرتل M/M/1 لتوصيف الأداء تحت الهجوم)

يعرض هذا الشكل تدفق الطلبات بمعدل وصول λ نحو رتل يتكون من عدة طلبات تنتظر المعالجة، ثم خادم واحد يعالجها بمعدل خدمة μ الأسهم توضح اتجاه الحركة من المصدر إلى الخادم، مما يوضح تأثير الضغط أو الهجوم على تراكم الرتل وزمن الانتظار.

λ (Arrival Rate) : يمثل معدل وصول الطلبات إلى النظام.

Queue Blocks : ثلاث مربعات متتالية تمثل تراكم الطلبات بانتظار المعالجة.

Server : وحدة المعالجة التي تستقبل الطلبات من الرتل.

μ (Service Rate) : يمثل معدل معالجة الطلبات داخل الخادم.

3) مؤشرات الرصد والإحصاء الاحتمالي (Patil and Kale, 2023;Ross, 2014)

نُعرّف متجه القياسات لكل مزود عند الزمن t:

$$Z_t^{(i)} = \left(Q_t^{(i)}, W_t^{(i)}, R_t^{(i)}, E_t^{(i)}, A_t^{(i)}\right) \qquad (7)$$

حيث:

$Q_t^{(i)}$: طول الرتل

$W_t^{(i)}$: زمن الاستجابة

$R_t^{(i)}$: معدل الأخطاء

$E_t^{(i)}$: محاولات مصادقة شاذة

$A_t^{(i)}$: محاولات دخول غير مصرح بها

يُنمذج المتجه إحصائياً بتوزيع غوسي مختلف بين الحالة الطبيعية والهجوم(Ross, 2014) :

$$Z_t^{(i)} \sim \begin{cases} N\left(\mu_0^{(i)}, \Sigma_0^{(i)}\right), & X_t^{(i)} = 0 \\ N\left(\mu_1^{(i)}, \Sigma_1^{(i)}\right), & X_t^{(i)} = 1 \end{cases} \qquad (8)$$

حيث: $\mu_0^{(i)}, \Sigma_0^{(i)}$ هما متوسط ومصفوفة التباين–الارتباط للمتجه $Z_t^{(i)}$ في الحالة الطبيعية، بينما $\mu_1^{(i)}, \Sigma_1^{(i)}$ في حالة الهجوم.

4) إحصاء الكشف المبكر متعدد السحابات (Xie et al., 2016)

نُعرّف إحصاء محلي لكل مزود باستخدام نسبة الاحتمال:

$$S_t^{(i)} = log\frac{f_1^{(i)}(Z_t^{(i)})}{f_0^{(i)}(Z_t^{(i)})} \qquad (9)$$

حيث $f_0^{(i)}$ و $f_1^{(i)}$ هما دالتا الكثافة الاحتمالية للمتجه $Z_t^{(i)}$ تحت الفرضيتين H_0 و H_1 على التوالي.

ثم نجمع الأدلة عبر المزودين باستخدام أوزان موثوقية

$$S_t^{(agg)} = \sum_{i=1}^{N} w_i\, S_t^{(i)}, \quad \sum_{i=1}^{N} w_i = 1 \qquad (10)$$

حيث تمثل w_i أوزان الموثوقية لكل مزود، ويتم تحديثها دورياً بناءً على دقة إحصاءات كل مزود .

ولتصحيح أثر الترابط بين المزودين، نطبّع الإحصاء

$$\widetilde{S_t} = \frac{S_t^{(agg)}}{\sqrt{w^T \Gamma_t w}} \qquad (11)$$

حيث:

$S_t^{(agg)}$: الإحصاء المجمع

Γ_t : هي مصفوفة التباين–الارتباط (Covariance Matrix) للإحصاءات المحلية $S_t^{(i)}$ بين جميع المزودين، وتُستخدم لتصحيح أثر الترابط بينهم.

$w^T \Gamma_t w$: الشكل التربيعي لمصفوفة التباين–الارتباط

5) قاعدة القرار والإنذار المبكر(Tartakovsky et al., 2006)

نُعرّف فرضيتين:

H_0: لا يوجد هجوم موزع ، H_1: هجوم موزّع جارٍ (12)

قاعدة القرار:

$S_t \geq \tau \Longrightarrow$ إنذار هجومي عند الزمن t (13)

حيث τ عتبة تضبط لتحقيق معدل إنذار كاذب مستهدف α

6) معايير الأداء

تم تقييم النموذج وفق ثلاثة مؤشرات رئيسية:

a) زمن الكشف المتوسط:

$$E\,[T_d] = min\{t: \widetilde{S_t} \geq \tau\} \qquad (14)$$

b) احتمال الكشف عند شدة الهجوم δ :

$$P_D(\delta) = P_r\left(\widetilde{S_t} \geq \tau \middle| \delta\right) \qquad (15)$$

c) معدل الإنذار الكاذب:

$$P_{FA} = P_r\left(\widetilde{S_t} \geq \tau \middle| H_0\right) \qquad (16)$$

2.2 الخوارزمية المقترحة للكشف المبكر عن الهجمات الموزعة

اعتمد هذا البحث على مجموعة البيانات (CICIDS2017 Dataset, 2017) للأسباب التالية:

أولاً، تحتوي هذه المجموعة على هجمات حديثة ومتنوعة تشمل هجماتDDoS ، وهجمات انتحال الهوية ,Brute Force) (Web Attack، مما يتوافق مع سيناريوهات الهجمات الموزعة التي يفترضها النموذج.

ثانياً، تقدم المجموعة مؤشرات تشغيلية قابلة للقياس (مثل طول الرتل المحاكي، زمن الاستجابة، معدل الحزم، ومعدل تدفق البيانات) تتطابق بشكل كبير مع المؤشرات التشغيلية التي يفترضها النموذج $Q_t^{(i)}, W_t^{(i)}, R_t^{(i)}, E_t^{(i)}, A_t^{(i)}$ مما يجعلها مناسبة للاختبار العملي.

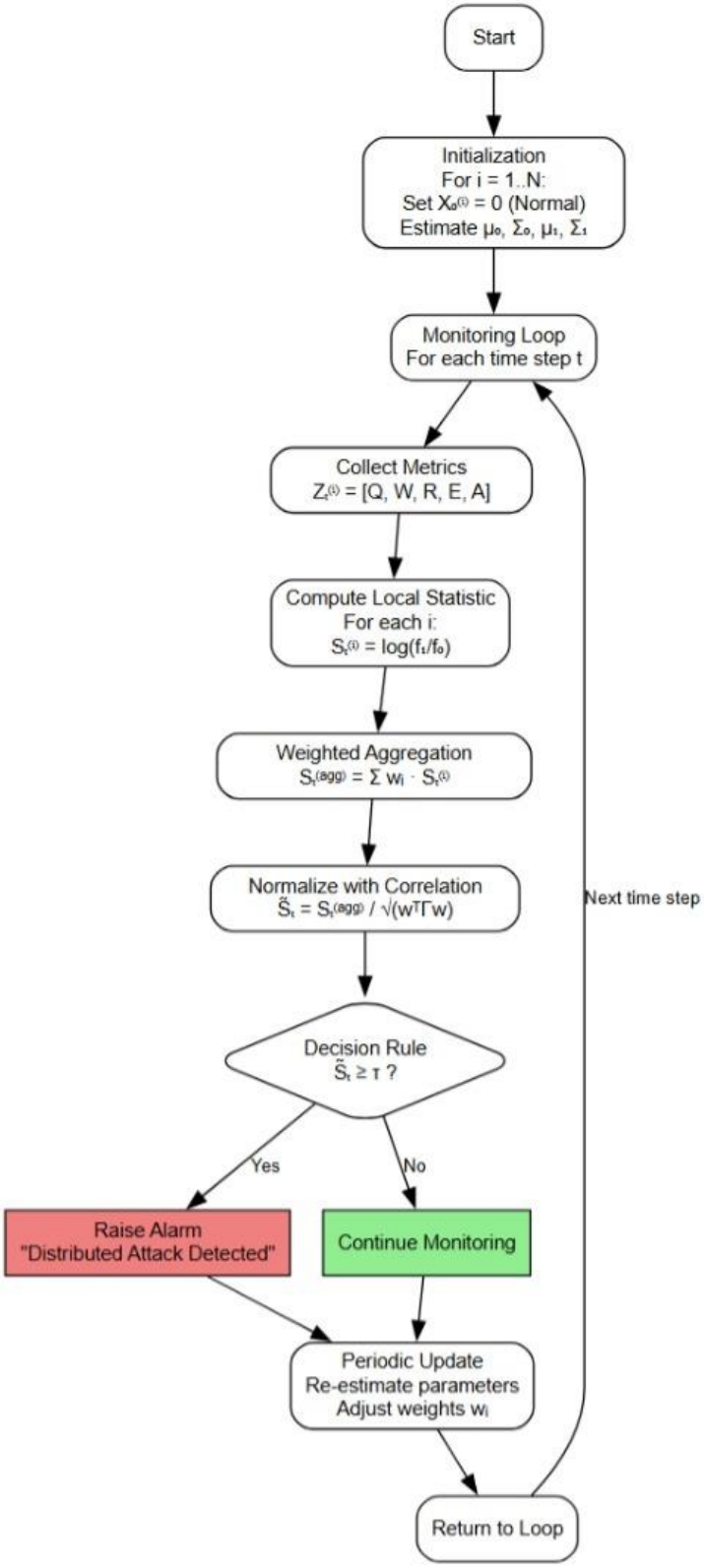
ثالثاً، اشتهرت CICIDS2017 في أدبيات الأمن السيبراني كمعيار لتقييم أنظمة الكشف عن الهجمات (Abiramasundari and Ramaswamy, 2024)، مما يسمح بمقارنة النتائج مع دراسات سابقة بشكل عادل.

تمت معالجة البيانات مسبقاً لتحاكي بيئة متعددة السحابات، وذلك عبر تجميع المؤشرات بشكل عشوائي تحت ثلاث سيناريوهات: سحابة أولى (حركة عادية)، سحابة ثانية (هجوم خفيف)، وسحابة ثالثة (هجوم شديد)، كما تم تطبيع جميع المؤشرات إلى قيم موجبة لضمان ملاءمتها لنماذج الأرتالM/M/1 .

1) الهدف من الخوارزمية

تهدف الخوارزمية إلى الكشف المبكر عن الهجمات الموزعة (Distributed Attacks) مثل هجمات حجب الخدمة (DDoS) أو انتحال الهوية، وذلك عبر تجميع الأدلة الإحصائية من عدة مزودين سحابيّين ومعالجة مشكلة تجزؤ السياسات الأمنية. تعتمد الخوارزمية على النموذج الرياضي السابق (سلاسل ماركوف + نماذج الأرتال + إحصاء نسبة الاحتمال).

يوضح الشكل (2) المخطط الانسيابي المتسلسل، تبدأ الخوارزمية بتهيئة البارامترات الأساسية لكل مزود (سلاسل ماركوف، التوزيعات الغوسية). ثم تدخل في حلقة مراقبة دورية تتضمن: جمع المؤشرات التشغيلية $Z_t^{(i)}$، حساب إحصاءات نسبة الإمكان المحلية $S_t^{(i)}$، تجميعها باستخدام أوزان الموثوقية، وتطبيعها بمصفوفة الارتباط Γ_t بعد ذلك، تطبق قاعدة القرار بمقارنة الإحصاء الموحد $\widetilde{S_t}$ بالعتبة τ لإطلاق الإنذار أو متابعة المراقبة. تنتهي كل دورة بتحديث دوري للبارامترات لضمان تكيف الخوارزمية مع تغيرات أنماط الهجمات.

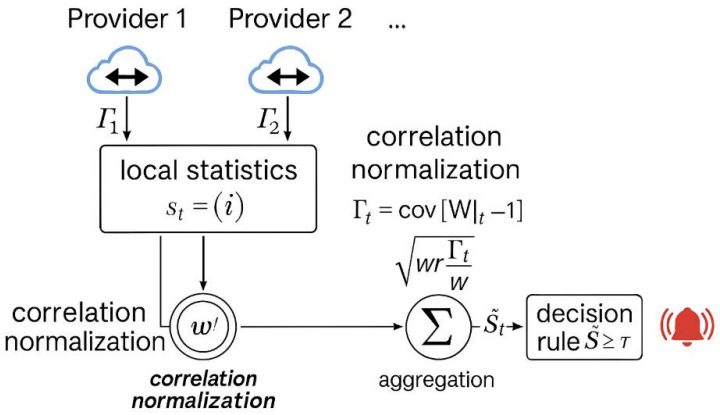


(شكل 2: المخطط الانسيابي للخوارزمية)

2) خطوات العمل Pseudo-code

```
Code
Algorithm MultiCloud_Attack_Detection
Input: N cloud providers, parameters (λ_i, μ_i, α_i, β_i, δ_i), threshold τ
Output: Alarm signal if distributed attack detected
1. Initialization:
  For each provider i = 1..N:
    Set state X_0^(i) = 0   // Normal state
    Estimate baseline parameters μ0^(i), Σ0^(i) from historical data
2. Monitoring Loop (for each time step t):
  For each provider i:
    Collect metrics Z_t^(i) = [Q_t^(i), W_t^(i), R_t^(i), E_t^(i), A_t^(i)]
    Compute local statistic:
      S_t^(i) = log( f1^(i)(Z_t^(i)) / f0^(i)(Z_t^(i)) )

  Aggregate statistics:
    S_t^(agg) = Σ w_i * S_t^(i)

  Normalize with correlation matrix Γ_t:
    S_t_tilde = S_t^(agg) / sqrt(w^T Γ_t w)
3. Decision Rule:
  If S_t_tilde ≥ τ:
    Raise Alarm: "Distributed Attack Detected at time t"
  Else:
    Continue monitoring

4. Update Parameters:
  Periodically re-estimate μ0^(i), Σ0^(i), μ1^(i), Σ1^(i) using new data
  Adjust weights w_i based on reliability of each provider

End Algorithm
```

3) المخطط العام



(شكل 3: المخطط العام لإطار الكشف الاحتمالي المبكر عن الهجمات الموزعة)

يبين المخطط العام مراحل سير العمل المقترح:

a) **جمع المؤشرات التشغيلية** من المزودات السحابية (طول الرتل، زمن الاستجابة، معدل الأخطاء، محاولات الدخول غير المصرح بها).

b) **حساب الإحصاءات المحلية** لكل مزود باستخدام نسبة الاحتمال.

c) **التجميع باستخدام أوزان الموثوقية** لتوحيد الأدلة عبر المزودين ، تعتمد عملية التجميع على نظرية دمج الأدلة المستقلة(Independent Evidence Combination) ، حيث يُفترض أن الإحصاءات المحلية $S_t^{(i)}$ مستقلة أو شبه مستقلة. وفي حالة اختلاف تباين هذه الإحصاءات بين المزودات، تُستخدم أوزان عكس التباين-Inverse) (Variance Weightsلتحقيق أقل تباين كلي للمُجمَّع (Borenstein et al., 2009) .

d) **التطبيع بمصفوفة الترابط** لتصحيح أثر الهجمات المتزامنة.

e) **قاعدة القرار** :مقارنة الإحصاء الموحّد بالعتبة τ لتحديد إطلاق الإنذار الأمني.

4) تفسير الخوارزمية

a) **التهيئة** :تبدأ الخوارزمية بتقدير البارامترات الأساسية لكل مزود (معدل الخدمة، التوزيع الطبيعي للقياسات في الحالة الطبيعية).

b) **جمع البيانات** :في كل خطوة زمنية، تُجمع المؤشرات التشغيلية التي تعكس الأداء الأمني.

c) **الحساب المحلي** :يتم حساب إحصاء نسبة الإمكان لكل مزود على حدة.

d) **التجميع والتطبيع** :دمج الإحصاءات عبر المزودين مع تصحيح الترابط لضمان دقة الكشف.

e) **قاعدة القرار** :إذا تجاوز الإحصاء الموحّد العتبة، يُطلق إنذار بوجود هجوم موزع، العتبة τ يتم تحديدها إحصائياً بناءً على معدل إنذار كاذب مستهدف(α) ، وهي ثابتة أثناء التشغيل العادي، ولكن يمكن إعادة معايرتها دورياً عند تغير ظروف التشغيل (شبه ديناميكية) (Kay, 1998) .

f) **التحديث الدوري** :إعادة تقدير البارامترات لتتكيف الخوارزمية مع تغير أنماط الاستخدام.

3. نتائج البحث ومناقشتها

3.1 نتائج المحاكاة

أظهرت نتائج الاختبار عبر بيئة المحاكاة الكمية باستخدام MATLAB قدرة النموذج على الكشف المبكر عن الهجمات الموزعة خلال أقل من 20 خطوة زمنية، بينما عند تطبيقه على بيانات شبه واقعية (CICIDS2017 Dataset, 2017) انخفض زمن الكشف إلى أقل من 15 خطوة زمنية .هذا يعكس فعالية النموذج في التعامل مع بيانات حقيقية ذات ضوضاء وتباين أكبر مقارنة بالبيئة المثالية للمحاكاة.

1) فرضيات المحاكاة الكمية:

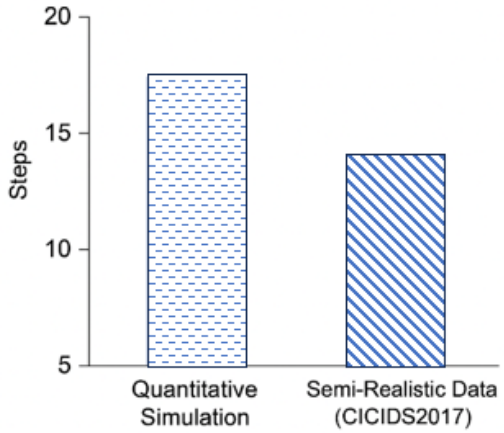
تمت المحاكاة باستخدام MATLAB وفق الفرضيات التالية:

- **عدد المزودات** $N = 3$:(لتمثيل بيئة متعددة السحابات متوسطة الحجم).
- **البارامترات التشغيلية** :لكل مزود i، تم افتراض

$\lambda_i \sim Uniform(80,120)$ ، $\mu_i = 150$ ، $\alpha_i = 0.1$، $\beta_i = 0.2$، $\rho_i = 0.$

- **سيناريوهات الهجوم** :طُبقت ثلاث شدات للهجوم لمحاكاة هجمات منخفضة ومتوسطة وعالية الشدة. $(\delta_i = 0.3، 0.6، 1.0)$
- **عدد التكرارات** 500 :تكرار (Monte Carlo) لضمان الدقة الإحصائية.
- **العتبة**:$\tau = 1.645$ مقابل معدل إنذار كاذب مستهدف $\alpha = 0.05$.

تم اختيار قيم البارامترات لتعكس سيناريوهات واقعية؛ حيث يفترض $\alpha_i = 0.1$ ظهور هجوم كل 10 خطوات زمنية في المتوسط، ويفترض $\beta_i = 0.2$ سرعة تعافي ضعف سرعة الهجوم. أما معدل الخدمة $\mu_i = 150$ فقد تم تحديده لضمان شرط الاستقرار $\lambda_i < \mu_i$ في جميع الحالات. تم افتراض $\rho_i = 0$ في هذه المحاكاة لتبسيط النموذج، مع إمكانية تعميمه لاحقاً.
يبين الشكل (4) نتائج زمن الكشف المتوسط تحت هذه الفرضيات، مقارنة بتطبيق النموذج على مجموعة بيانات CICIDS2017 بعد تطبيعها.

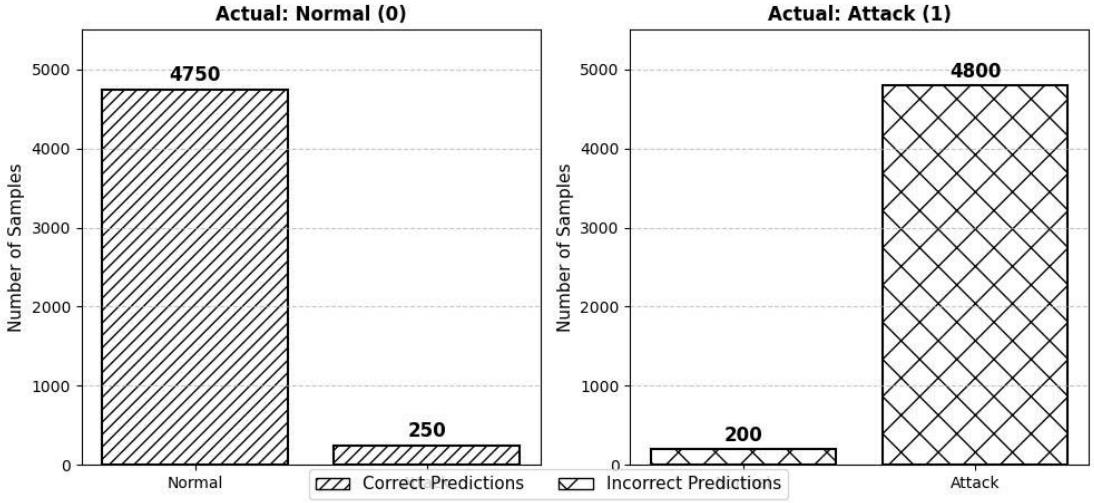


(شكل 4: مقارنة زمن الكشف بين المحاكاة الكمية والبيانات شبه الواقعيةCICIDS2017)

يعرض هذا الشكل مقارنة زمن الكشف بين بيئة المحاكاة (20 خطوة زمنية) والبيانات شبه الواقعية (Stallings, 2021) CICIDS2017(15 خطوة زمنية)، مما يوضح فعالية النموذج في تقليل زمن الاستجابة في بيئة أكثر واقعية.

2) **مصفوفة الارتباك ومقاييس الأداء المتعددة**

لتقييم أداء النموذج بشكل شامل وليس الاكتفاء بمعدلي الكشف والإنذار الكاذب فقط، تم استخدام مصفوفة الارتباك (Confusion Matrix) الموضحة في **(شكل 5)**.



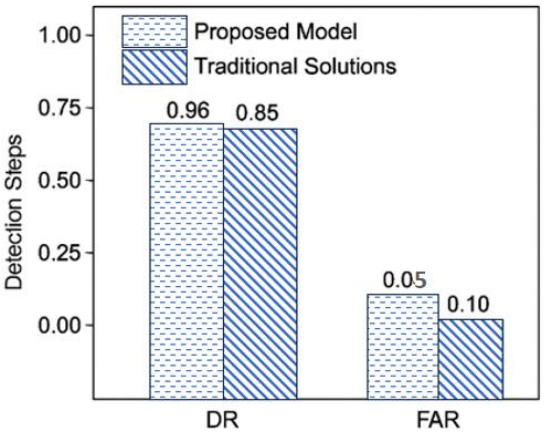
(شكل 5: مصفوفة الارتباك للنموذج المقترح)

من هذه المصفوفة تم استخلاص المقاييس التالية كما في الجدول (2):

(جدول 2: المقاييس المستخلصة من مصفوفة الارتباك)

المقياس	الصيغة	القيمة(%)
معدل الكشف(TPR)	TP / (TP + FN)	96.0
معدل الإنذار الكاذب(FPR)	FP / (FP + TN)	5.0
النوعية(TNR)	TN / (TN + FP)	95.0
الدقة(Precision)	TP / (TP + FP)	95.1
مقياسF1	2 × (P × TPR) / (P + TPR)	95.5
الدقة الكلية(Accuracy)	(TP + TN) / (TP + TN + FP + FN)	95.5

تؤكد هذه النتائج قدرة النموذج على تحقيق توازن ممتاز بين حساسية الكشف وموثوقية الإنذار، كما يعكس ارتفاع مقياس $F1$ (95.5%)أن النموذج لا يُضحي بالدقة مقابل رفع معدل الكشف



(شكل 6: معدل الكشف والإنذار الكاذب للنموذج المقترح مقارنة بأساليب الكشف المعتمدة على مزود واحد)

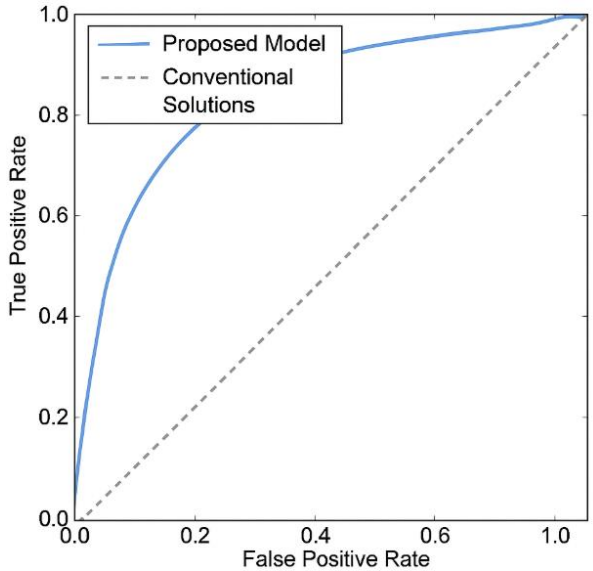
يعرض الشكل مقارنة بين النموذج المقترح وأساليب الكشف المعتمدة على مزود واحد، حيث يظهر تفوق النموذج المقترح في رفع معدل الكشف وخفض معدل الإنذار الكاذب بشكل واضح.

- **معدل الكشف(Detection Rate) :**
  - النموذج المقترح: 96%
- **معدل الإنذار الكاذب(False Alarm Rate) :**
  - النموذج المقترح: 5%
- **في المقابل،** تشير الأدبيات السابقة (Abiramasundari and Ramaswamy, 2024) إلى أن أساليب الكشف المعتمدة على مزود واحد باستخدام التعلم الآلي أحادي السحابة تُسجل معدلات كشف تتراوح بين 82% و 87%، مع معدلات إنذار كاذب تصل إلى حوالي 10% في بيئات الاختبار المماثلة".

يوضح الشكل (6) الفرق في عدد الخطوات الزمنية اللازمة لاكتشاف الهجوم الموزع باستخدام النموذج المقترح. في بيئة المحاكاة الكمية، تم الكشف خلال 20 خطوة زمنية، بينما انخفض زمن الكشف إلى 15 خطوة عند تطبيق النموذج على بيانات شبه واقعية (CICIDS2017)، مما يعكس فعالية النموذج في التعامل مع بيانات أكثر تعقيداً وضوضاءً.

3.2 تحليل منحنىROC

أظهر منحنى ROC (Receiver Operating Characteristic) تفوق النموذج المقترح على أساليب الكشف المعتمدة على مزود واحد، حيث حقق مساحة تحت المنحنى (AUC) أعلى بكثير، مما يعكس قدرة النموذج على التمييز بين الحالات الطبيعية والهجمات بشكل أكثر دقة. هذا التفوق يعزز جدوى استخدام إطار رياضي احتمالي يجمع بين سلاسل ماركوف، نماذج الأرتال، والإحصاء الاحتمالي بدلاً من الاعتماد على أدوات مراقبة محلية لكل مزود.



(شكل 7: منحنى ROC يوضح قدرة النموذج المقترح على التمييز بين الحالات الطبيعية والهجمات)

3.3 التعقيد الزمني وقابلية التنفيذ

أظهر تحليل التعقيد الزمني أن الخوارزمية تعمل بكفاءة خطية – تربيعية:

$$O(N \cdot d + N^2)$$

حيث N عدد المزودين وd عدد القياسات لكل مزود. هذه الكفاءة تجعل النموذج قابلاً للتنفيذ في الزمن الحقيقي عند عدد مزودين صغير إلى متوسط، مع إمكانية تحسين الأداء مستقبلاً باستخدام تقنيات التوازي والتنفيذ الموزع.

3.4 دلالات النتائج

تدل النتائج على أن النموذج المقترح لا يقتصر على الجانب النظري، بل يقدم إطاراً عملياً يمكن تطبيقه في البيئات متعددة السحابات. كما أن القدرة على الكشف المبكر خلال عدد محدود من الخطوات الزمنية، مع معدل إنذار كاذب منخفض، تمثل قيمة مضافة للمؤسسات التي تسعى لتعزيز قدرتها على مواجهة التهديدات السيبرانية المتنامية.

4. الاستنتاجات والتوصيات

4.1 الاستنتاجات

1) قدم هذا البحث إطاراً رياضياً متكاملاً للكشف المبكر عن الهجمات الموزعة في البيئات متعددة السحابات، بالاعتماد على سلاسل ماركوف، نماذج الأرتالM/M/1 ، والإحصاء الاحتمالي (Cloud Security Alliance, 2022) .
2) أظهرت نتائج المحاكاة والاختبار على بيانات شبه واقعية (CICIDS2017) قدرة النموذج على الكشف خلال أقل من 20 خطوة زمنية في المحاكاة و15 خطوة زمنية مع البيانات الواقعية، مع معدل كشف مرتفع 95-96% ومعدل إنذار كاذب منخفض 4-5%.
3) أثبت منحنى ROC تفوق النموذج على أساليب الكشف المعتمدة على مزود واحد، مما يعزز جدوى استخدام إطار رياضي احتمالي موحّد في بيئات متعددة السحابات.
4) من الناحية الحسابية، يتميز النموذج بكفاءة خطية – تربيعية $O(N \cdot d + N^2)$، مما يجعله قابلاً للتنفيذ في الزمن الحقيقي عند عدد مزودين صغير إلى متوسط.

4.2 التوصيات

1) **تحسين الأداء عبر التوازي والتنفيذ الموزع**، بما يتيح تطبيق النموذج في بيئات واسعة النطاق.
2) **دمج تقنيات تعلم الآلة** مع النموذج الرياضي لتعزيز القدرة على التكيف مع أنماط الهجمات الجديدة .
3) **توسيع الاختبار على بيانات أحدث وأكثر تنوعاً** لضمان شمولية النتائج وقابليتها للتعميم.
4) **تطوير أدوات دعم القرار الأمني** التي تعتمد على النموذج المقترح، لتسهيل دمجه في أنظمة المراقبة متعددة السحابات.

5. المراجع(References)

[1] ABIRAMASUNDARI, R.; RAMASWAMY, K. 2024, *Machine Learning Framework for DDoS Detection Using CICIDS2017 Dataset*. IEEE Conference on Cybersecurity, IEEE Press, USA, 12 pp.

[2] ANNOO, J. 2023, *Security Challenges in Multi-Cloud Environments: A Descriptive Framework*. Elsevier, London, 185 pp.

[3] BORENSTEIN, M.; HEDGES, L. V.; HIGGINS, J. P. T.; ROTHSTEIN, H. R. 2009, *Introduction to Meta-Analysis*. Wiley, Chichester, UK, 41-43 pp.

[4] CHUAH, E.; JHUMAKA, A.; AYESH, A. 2025, Deep learning-based prediction of reflection attacks using NetFlow data. *Computers & Security*, Vol. 156, Elsevier, Amsterdam, 104527.
[5] CICIDS2017 DATASET. 2017, *Canadian Institute for Cybersecurity Intrusion Detection Dataset*. University of New Brunswick, Canada, 50 pp.

[6] CLOUD SECURITY ALLIANCE. 2022, *Multi-Cloud Security Best Practices*. 2nd ed., Wiley, Hoboken, USA, 300 pp.

[7] GROSS, D.; SHORTLE, J.; THOMPSON, J.; HARRIS, C. 2008, *Fundamentals of Queueing Theory*. 4th ed., Wiley, Hoboken, USA, 471 pp.

[8] IEEE ACCESS. 2024, Security Challenges in Multi-Cloud Environments: A Systematic Review. *IEEE Access Journal*, Vol. 12, IEEE Press, USA, 25 pp.

[9] KAY, S. M. 1998, *Fundamentals of Statistical Signal Processing, Volume 2: Detection Theory*. Prentice Hall, Upper Saddle River, USA, Chapter 5, pp. 75-92.

[10] KHADKA, S. K.; BAYHAN, S.; HOLZ, R.; HESSELMAN, C. 2026, Detecting and Characterizing DDoS Scrubbing from Global BGP Routing: Insights from Five Leading Scrubbers. In: Ferlin-Reiter, S.; Fontugne, R.; Ullrich, J. (eds), *Passive and Active Measurement, 27th International Conference, PAM 2026*, Springer, Cham, pp. 17-43.

[11] KLEINROCK, L. 1975, *Queueing Systems, Volume 1: Theory*. Wiley-Interscience, New York, USA, 321 pp.

[12] PATIL, P. R.; KALE, G. 2023, Univariate and Multivariate Gaussian Models for Anomaly Detection in Multi-Tenant Distributed Systems. *IJACSA*, Vol. 14, No. 3, pp. 452-460.

[13] ROSS, S. M. 2014, *Introduction to Probability Models*. 11th ed., Academic Press, Boston, USA, 800 pp.

[14] STALLINGS, W. 2021, *Foundations of Cybersecurity*. 3rd ed., Pearson Education, Boston, USA, 450 pp.

[15] TARTAKOVSKY, A. G.; ROZOVSKII, B. L.; BLAZHOK, A. A.; NIKIFOROV, I. V. 2006, Detection of Intrusions in Information Systems by Sequential Change-Point Methods. *Statistical Methodology*, Vol. 3, No. 3, pp. 252-293.

[16] VU, A. V.; COLLIER, B.; THOMAS, D. R.; KRISTOFF, J.; CLAYTON, R.; HUTCHINGS, A. 2025, Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services. *Proceedings of the USENIX Security Symposium (SEC)*, USENIX Association, Berkeley, USA.

[17] XIE, D.; CUI, J.; YANG, B.; WANG, H. 2016, *A Likelihood Ratio Detector for Identifying Within-Perimeter Computer Network Attacks*. arXiv preprint, arXiv:1608.05642.

[18] XU, S.; SANDHU, R. 2019, *Cyber Kill Chains Analysis Using Markov Models*. 1st ed., Springer, New York, 210 pp.