

# حماية البيانات الضخمة: الأساسيات والتوجهات

الدكتور : بازارا باري

# الدكتور : بازارا باري



- أكثر من 10 سنوات من الخبرة القيادية في مجال الأمن الإلكتروني وفضاء تكنولوجيا المعلومات والاتصالات.
- دكتوراه في الأمن الإلكتروني ، شهادة PMP ، و شهادة CISSP
- استشهد بدراساته من قبل العلماء والممارسون أكثر من 200 مرة
- محاضر في القارات الخمس
- حاصل على جوائز (4 جوائز دولية لأفضل ورقة وشهادة اعتراف من الاتحاد الدولي للاتصالات)
- عضو نشط في IEEE و PMI و (ISC) 2

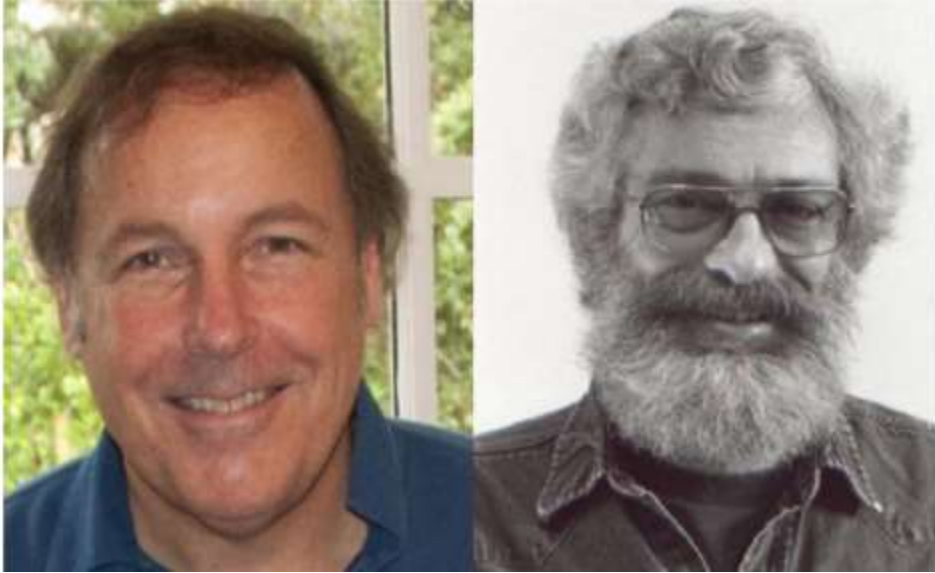
## محتوى المداخلة



- الأصل والمفهوم والأساسيات
- تحديات أمن البيانات الضخمة
- الهجمات الخاصة بالبيانات الضخمة
- الحلول لتأمين البيانات الضخمة
- التوجهات المتنامية
- الخاتمة

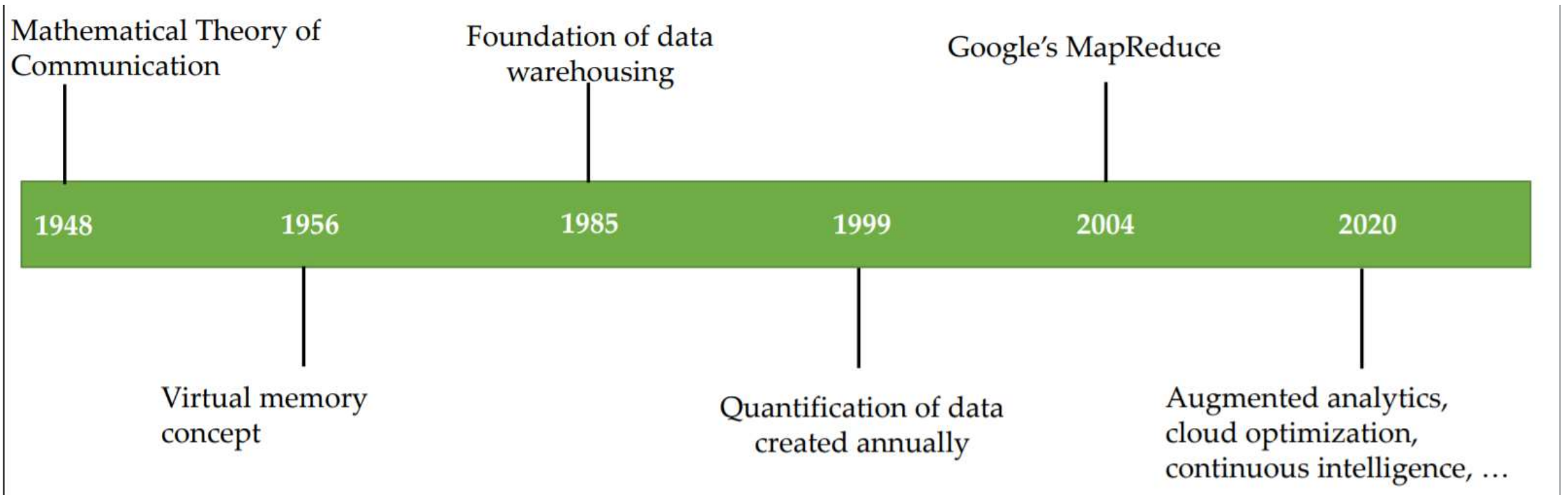
## الأصل ، المفهوم والأساسيات (3/1)

• في جويلية 1997 ، تم استخدام مصطلح "البيانات الضخمة" لأول مرة في مقال بقلم باحثي ناسا مايكل كوكس وديفيد إسورث



• وضع هذا البحث أسس لشكاليّة البيانات الضخمة  
": مجموعات البيانات الضخمة تتحدّى قدرات  
الذاكرة الرئيسية والقرص المحلي وحتى القرص  
الخارجي.

# الأصل ، المفهوم والأساسيات (3/2)



## الأصل ، المفهوم والأساسيات (3/3)

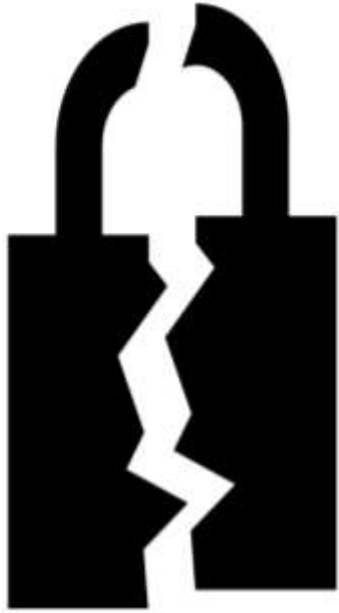


وفقاً لـ "العناصر الأساسية حول البيانات الضخمة" ، تُعرّف البيانات الضخمة بأنها "ظاهرة ثقافية وتكنولوجية وعلمية تعتمد على التفاعل بين:

- التكنولوجيا
- التحليل
- المنهجية

## تحديات أمن البيانات الضخمة (3/1)

• يعتمد نجاح مشاريع البيانات الضخمة على أساس أنظمة متوازية وموزعة مثل الكتلة والشبكة والحوسبة السحابية والإنترنت وشبكات الاتصالات والأنظمة الفيزيائية الإلكترونية (CPS) وشبكات الاتصالات آلة-آلة (M2M)



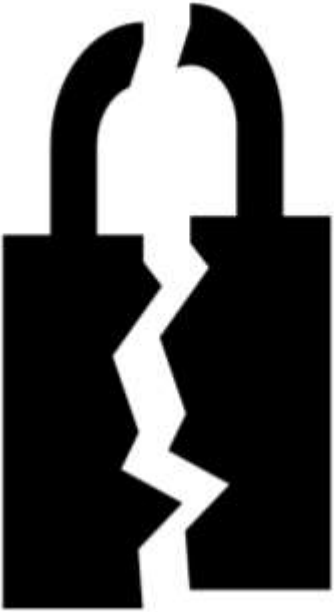
• في الوقت الذي توفر الأنظمة المتوازية والموزعة فرصاً لتحسين التوسعة، والإدارة، والكفاءة، والموثوقية، فإنها تسجل مستوى غير مسبوق من نقاط الضعف الأمنية.

## تحديات أمن البيانات الضخمة (3/2)

. نظرًا لأن أجهزة النظام متصلة على نطاق واسع ، فهي تتقاسم نقاط الضعف الخاصة بها من قبل النظام بأكمله.

• يجب أن يكون مهندس الأمن على دراية بتأثيرات « قوّة المضاعفة » التي تجلبها هذه الأنظمة إلى المؤسسة.

• عدم وجود حل متكامل لإدارة البيانات والأنظمة مع مجموعة مشتركة من السياسات والضوابط.





## تحديات أمن البيانات الضخمة (3/3)

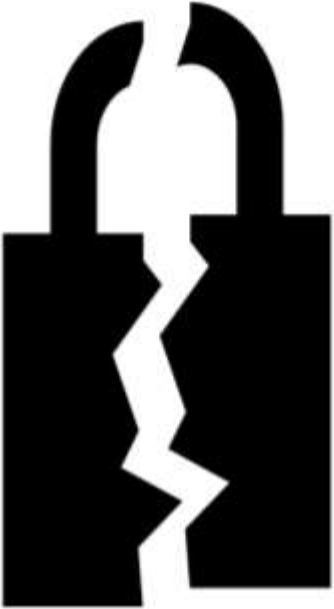
ظاهرة البيانات الضخمة مدفوعة بتقاطع ثلاثة اتجاهات:

- كمّية مهولة من البيانات التي تحتوي على معلومات قيمة

- وفرة موارد الحوسبة وزهادة أثمانها

- أدوات تحليل "مجانية"

غالبًا ما يثير العنصر الأخير مخاوف أمنية عندما يتعلّق الأمر بأمن بيئات البيانات الضخمة.



# الهجمات الخاصة بالبيانات الضخمة (3/1)

- يجمع مستودع البيانات بيانات من قواعد بيانات المختلفة في حاوية بيانات واحدة كبيرة.



- مجموع النظام البيئي الذي يدعم ويخلق مستودع البيانات أكبر بكثير ، ويحتمل أن يكون أكثر قيمة للمهاكر ، من الأجزاء الفردية التي يتكون منها مستودع البيانات.

- بالمقارنة مع قواعد البيانات التقليدية ، يعتبر الأمان أكثر أهمية لمخازن البيانات. يجب وضع ضوابط السرية والنزاهة والاتاحة المناسبة وفقاً لذلك.

## الهجمات الخاصة بالبيانات الضخمة (3/2)

• الاستدلال هو القدرة على استنتاج (تخمين) معلومات حساسة أو مقيدة من خلال مراقبة المعلومات المتاحة.



• قد يتمكن المستخدمون من تحديد المعلومات غير المصرح بها من خلال المعلومات التي يمكنهم الوصول إليها وقد لا يحتاجون أبدًا إلى الوصول المباشر إلى البيانات غير المصرح بها.

• سيحتاج مهندس الأمن إلى تطبيق فهم عميق لنماذج الأعمال المحيطة بمهمة المنظمة للتقليل من هذه المخاطر.

## الهجمات الخاصة بالبيانات الضخمة ( 3/3 )

- التجميع هو تجميع البيانات غير الدقيقة من مصادر منفصلة لإنشاء وتكوين معلومات دقيقة



- يمكن أن تكون دقة البيانات المجمعة أكبر من دقة الأجزاء الفردية.

- يجب أن يفهم مهندس الأمن التوليفات المحتملة ( التركيبات الممكنة) للمعلومات بما في ذلك التوليفات التي قد تؤدي إلى الترفيع في دقتها.

# حلول أمن البيانات الضخمة (3/1)

تشمل الحلول توفير الثقة ما يلي:

• مخططات التحقق الرئيسية

• التخفيف من هجمات DoS

القائمة على الثقة

• كشف تسرب المحتوى



# حلول أمن البيانات الضخمة (3/2)

تشمل الحلول لتوفير الخصوصية ما يلي:

- أنظمة المصادقة عن بُعد للوصول إلى البيانات عبر الشبكة اللاسلكية
- إخفاء حركة التدفق لتعتيم البيانات



- إخفاء الهوية لمجموعات البيانات واسعة النطاق

- حلول ضوابط الدخول اللامركزية للولوج إلى البيانات المستندة إلى السحابة

# الحلول أمان البيانات الكبيرة (3/3)

• تشمل الحلول لتوفير الأمن العام للبيانات ما يلي:

• آليات الاستجابة لمواجهة نواقل الاقتحام سريعة الانتشار / سريعة المفعول

• سياسات ترخيص ملائمة و/ أو بيانات اعتماد المستخدم داخل قواعد البيانات الموزعة التي يتم الوصول إليها بواسطة الأنظمة القائمة على السحابة

• مشاركة البيانات بأمان وفعالية ومرونة باستخدام أنظمة تشفير رئيسية مشتركة.



# التوجهات المتنامية : إخفاء الهوية عن طريق التصميم (3/1)

• إنترنت الأشياء ( IoT ) لديه القدرة على الدخول في العديد من الاحتمالات بما في ذلك حالة المراقبة.



• الشركات التي تطور أنظمة إنترنت الأشياء التي قد تجمع معلومات معرفة الشخصية تتوجه نحو طلب موافقة المستخدم كشرط أساسي.

• ومع ذلك ، هناك توجه جديد متزايد للتأكد من أن مثل هذه الأنظمة لا تنتهك خصوصية الناس



## التوجهات المتنامية : إخفاء الهوية عن طريق التصميم (3/2)

- يهدف إخفاء الهوية عن طريق التصميم إلى جعل من المستحيل على صانع الجهاز التعرف على الأشخاص في المقام الأول بدلاً من إخفاء هوية البيانات بعد وقوعها.



- مع إخفاء الهوية حسب التصميم ، لا يمكنك التخلي عن معلومات تحديد الهوية الشخصية ، لأنك لا تملكها.

- يجب على الشركات التي تقوم بتطوير مثل هذه الأنظمة تضمين عدم الكشف عن هويتها في الحل من اليوم الأول لأنه من الصعب تعديلها.

## التوجهات المتنامية : إخفاء الهوية عن طريق التصميم (3/3)

- قد تفقد الشركات التي تروج لإخفاء الهوية عن طريق التصميم مجموعة كبيرة من البيانات المفيدة.



- يمكن استخدام هذه البيانات لتدريب نماذج التعلم الآلي المستقبلية من أجل تحسين أداء الأجهزة.

- بعض الشركات تتغلب على هذا القيد من خلال جعل الموظفين / الأصدقاء يتطوعون ببياناتهم للتدريب ، بينما تختار شركات أخرى عدم الدخول في سوق التحليلات تمامًا.

## خاتمة

- يجب أن يكون الأمن مترسخًا في أنظمة البيانات الضخمة عن طريق التصميم بدلاً من أن يكون فكرة متأخرة.

- لذلك ، من المهم جعل مهندسي الأمن جزءًا من فرق التصميم في أقرب وقت ممكن.

- يجب الانتباه إلى المقدار المتزايد من تشريعات الخصوصية الشاملة في جميع أنحاء العالم (على سبيل المثال ، اللائحة العامة لحماية البيانات الأوروبية ، قانون الخصوصية الأسترالي وقانون خصوصية المستهلك الأمريكي)



# أسئلة ونقاش