تقييم اجراءات وتدابير الأمن السيبراني الحالية في منصة بازاري-اليمن

فاطمة أنور عسكر [1]
أية علي الحبشي [1]
نصر السقاف [1*]
ود سعيد محمد [1]
غدير محسن احمد [1]
مروى محمد إبراهيم [1]
ميمونة ناصر محمد [1]
نوف يعقوب أحمد [1]
هاجر عصام محمد [1]

الاستـــلام: 03/ابريل/2025
التحكيم: 15/ اغسطس/2025
القبـــــول: 16/ اغسطس /2025

[1] قسم الحاسبات-جامعة العلوم وتكنولوجيا عدن -اليمن
* عنوان المراسلة: ust.edu@n.alsaqqaf

تقييم اجراءات وتدابير الأمن السيبراني الحالية في منصة بازاري-اليمن

نصر السقاف
قسم الحاسبات-جامعة العلوم وتكنولوجيا
عدن -اليمن
ust.edu@n.alsaqqaf

أية علي الحبشي
قسم الحاسبات-جامعة العلوم وتكنولوجيا
عدن -اليمن
ayah.ali2@icloud.com

فاطمة أنور عسكر
قسم الحاسبات-جامعة العلوم وتكنولوجيا
عدن -اليمن
fatimaaskar005@gmail.com

مروى محمد إبراهيم
قسم الحاسبات-جامعة العلوم وتكنولوجيا
عدن -اليمن
marwahsmanymail@gmail.com

غدير محسن احمد
قسم الحاسبات-جامعة العلوم وتكنولوجيا
عدن -اليمن
deergh002002@gmail.com

ود سعيد محمد
قسم الحاسبات-جامعة العلوم وتكنولوجيا
عدن -اليمن
wisoline5656@gmail.com

هاجر عصام محمد
قسم الحاسبات-جامعة العلوم وتكنولوجيا
عدن -اليمن
hageresam040@gmail.com

نوف يعقوب أحمد
قسم الحاسبات-جامعة العلوم وتكنولوجيا
عدن -اليمن
noofalyafei7@gmail.com

ميمونة ناصر محمد
قسم الحاسبات-جامعة العلوم وتكنولوجيا
عدن -اليمن
maymonanaser9@gmail.com

الملخص:

في عالم يتسارع فيه التحول الرقمي، أصبحت البنوك هدفًا رئيسيًا للهجمات السيبرانية، وخاصة في الدول النامية ذات البنية التحتية الهشة. هذا البحث يكشف النقاب عن التحديات التي تواجه القطاع المصرفي في اليمن، ويركز على قصة نجاح ملهمة لبنك عدن الأول، الذي استطاع بفضل أنظمة أمانه المتقدمة أن يصمد في وجه الهجمات اليومية.

هل تساءلت يومًا كيف تحمي البنوك أموالك وبياناتك من قراصنة الإنترنت؟ هذا البحث يأخذك في رحلة استكشافية داخل أنظمة الأمن السيبراني لبنك عدن الأول، ويكشف عن الاستراتيجيات التي يستخدمها للتصدي للتهديدات المتزايدة. ستتعرف على كيفية تطبيق أفضل الممارسات الأمنية في بيئة مليئة بالتحديات، وكيف يمكن للبنوك الأخرى في الدول النامية أن تستفيد من هذه التجربة

الكلمات المفتاحية *الامن السيبراني، امن المعلومات، بنك عدن الاول، المخاطر السيبرانية في الدول النامية، القطاع المالي المصرفي، منصة بازاري..*

Evaluating the Effectiveness of Digital Forensic Investigations in Combating Cybercrime

***Abstract*— Assessing Current Cybersecurity Procedures and Measures in the Bazzarry Platform - Yemen In a world where digital transformation is accelerating, banks have become a primary target for cyberattacks, especially in developing countries with fragile infrastructure. This research reveals the challenges facing the banking sector in Yemen. It highlights the inspiring success story of Aden First Bank, which, thanks to its advanced security systems, has successfully withstood daily attacks. Have you ever wondered how banks protect your money and data from internet pirates? This research takes you on an exploratory journey inside Aden First Bank's cybersecurity systems, revealing the strategies it employs to counter increasing threats. You will learn how best security practices are applied in a challenging environment, and how other banks in developing countries can benefit from this experience. Keywords: Cybersecurity, Information Security, First Aden Bank, Cyber Risks in Developing Countries, Financial Banking Sector, Bazari Platform.**

Keywords— *digital forensic investigations, cybercrime countermeasures, digital evidence recovery, perpetrator identification, digital forensic tools*

I. المقدمة

في عصر تكنولوجيا المعلومات والاتصالات الحالي، شهد قطاع التجارة الإلكترونية تطوراً ملحوظ، مُحدثًا ثورة في كيفية تفاعل الشركات والمستهلكين وإجراء المعاملات من خلال التعاملات الالكترونية من خلال طرق البيع والشراء والدفع الالكتروني ة والاستلام والتسليم للمنتجات. ومع ذلك التطور الكبير، فقد عرّض هذا التطور السريع منصات التجارة الإلكترونية لمجموعة واسعة من تهديدات الأمن السيبراني، مما جعلها هدفاً رئيسياً للمهاجمين (الهاكر) الذين يسعون إلى استغلال الثغرات الأمنية. يُشكّل التعقيد المتزايد

للهجمات الإلكترونية والطبيعة المتطورة للتهديدات تحدياً كبيراً لحماية البيانات الحساسة والحفاظ على سلامة المعاملات الإلكترونية.[1]

تواجه منصات التجارة الإلكترونية، بدءًا من الشركات الكبرى متعددة الجنسيات وصولًا إلى شركات التجزئة الصغيرة عبر الإنترنت، خطرًا مستمرًا لمواجهة تهديدات إلكترونية مثل هجمات التصيد الاحتيالي، التي تخدع المستخدمين لدفعهم إلى الكشف عن معلوماتهم الشخصية؛ والبرامج الضارة، التي يُمكن أن تُفسد الأنظمة وتسرق البيانات؛ واختراقات البيانات، حيث يُعرّض الوصول غير المُصرّح به المعلومات السرية للخطر. بالإضافة إلى ذلك، تُضيف التهديدات الداخلية والأشكال المُتطورة من برامج الفدية مستوياتٍ إضافية من التعقيد إلى مشهد الأمن السيبراني. تهدف هذه الورقة إلى تقديم نظرة شاملة على الاتجاهات الحالية لتهديدات الأمن السيبراني في قطاع التجارة الإلكترونية، واستكشاف استراتيجيات التخفيف الفعالة التي يمكن استخدامها لمواجهة هذه التهديدات. ستتناول الدراسة الاتجاهات الناشئة، مثل الاستخدام المتزايد للذكاء الاصطناعي من قبل مجرمي الإنترنت، ونقاط الضعف المرتبطة بأجهزة إنترنت الأشياء (IoT)، والتي يتم دمجها بشكل متزايد في منصات التجارة الإلكترونية.

والذي بدوره ألقى على عاتق المؤسسات مسؤولية تأمين هذه البيانات للحفاظ على ثقة العملاء والامتثال للمعايير التنظيمية. ولضمان الأمن السيبراني في المراكز الإلكترونية، يجب على المؤسسات التركيز على ثلاثة جوانب أساسية: التوافر والنزاهة والسرية.[2]

باتخاذ هذه الإجراءات، يمكن للمؤسسات ضمان الأمن السيبراني في المراكز الإلكترونية، وحماية البيانات الحساسة من التهديدات الرقمية المتزايدة، مما يعزز استدامة الأعمال ويضمن الانسيابية في العمليات التجارية.[3]

من خلال البحث سنتعرف على اجراءات وتدابير الامن السيبراني المتبعة في منصة بازاري وسيتم من خلالها تقييم فعالية الإجراءات والتدابير.

II. مشكلة الدراسة

تواجه منصة "بازاري" للتجارة الإلكترونية تحديات متزايدة في مجال الأمن السيبراني، حيث يشهد هذا المجال نموًا متسارعا وهجمات سيبرانية متطورة. تعتبر حماية بيانات المستخدمين الحساسة والحفاظ على سمعة المنصة أمرًا بالغ الأهمية، مما يستدعي إجراء دراسة لتقييم الإجراءات الأمنية الحالية واقتراح إجراءات وتدابير لتعزيز مستوى الأمن السيبراني.

تسعى هذه الدراسة للإجابة عن الأسئلة التالية:

- ما هي الإجراءات والتدابير الأمنية المتبعة حاليًا في منصة "بازاري"؟
- ما هي نقاط الضعف المحتملة في الإجراءات الأمنية الحالية لمنصة "بازاري"؟ وكيف يمكن تطوير إجراءات وتدابير لمعالجة هذه النقاط وتعزيز مستوى الأمن السيبراني وحماية البيانات الحساسة للمستخدمين؟
- ما هي أبرز التهديدات السيبرانية التي تستهدف المتاجر الإلكترونية، وخاصةً المنصات المشابهة لمنصة "بازاري"؟

III. أهمية البحث

من الناحية الأكاديمية، يساهم البحث في تعزيز الأدبيات المتعلقة بالأمن السيبراني والتجارة الإلكترونية، ويقدم أفكارًا جديدة حول التهديدات والتحديات التي تواجه منصات التجارة في الجمهورية اليمنية. مع تزايد الاعتماد على المنصات الرقمية وزيادة تعقيد التهديدات السيبرانية، تصبح الأبحاث في هذا المجال ذات أهمية متزايدة. تعالج هذه الدراسة الفجوات الموجودة في هذه الأدبيات من خلال تحليل كيفية تأثير الإجراءات الأمنية على حماية البيانات وسلوك المستهلكين.

أما من الناحية التطبيقية، يعزز البحث قدرة الشركات على تحديد نقاط الضعف في أنظمتها الأمنية وتطوير استراتيجيات فعالة لحماية البيانات الحساسة. حيث يقدم توصيات لتحسين مستوى الأمان، مما يُساعد في تعزيز ثقة العملاء في المنصات الإلكترونية. تستفيد الشركات العاملة في التجارة الإلكترونية، خاصة في الجمهورية اليمنية، من دراسة حالة منصة "بازاري"، حيث يمكنها التعلم من التجارب والتحديات التي واجهتها، مما يزيد من وعيها بأهمية الأمن السيبراني.

تحظى هذه الدراسة بأهمية كبيرة من الناحية الاقتصادية، حيث تساهم في تعزيز الاقتصاد الرقمي في الجمهورية اليمنية. مع تزايد الاعتماد على التجارة الإلكترونية، يتعين على الشركات وضع استراتيجيات فعّالة لإدارة المخاطر الأمنية لضمان استدامة العمليات وزيادة ثقة العملاء.

IV. اهداف الدراسة

تعد التجارة الإلكترونية، وخاصة عبر منصات مثل "بازاري"، جزءًا أساسياً من السوق الرقمي. وباعتبارها من المنصات الإلكترونية الرائدة التي تقدم تجربة تسوق شاملة، فقد تواجه تحديات كبيرة في مجال حماية البيانات والمعلومات الحساسة. ولهذا نسعى من خلال هذه الدراسة إلى:

1. التعرف على الإجراءات الأمنية التي تمارسها منصة "بازاري"
2. التعرف على التهديدات السيبرانية الأكثر شيوعًا التي تستهدف المتاجر الإلكترونية، وخاصةً منصات مثل "بازاري"؟
3. تقييم الإجراءات الأمنية المتبعة في منصة "بازاري" للتجارة الإلكترونية،
4. تطوير حلول مبتكرة لتعزيز اجراءات وتدابير الأمن السيبراني وحماية البيانات الحساسة للمستخدمين؟

V. منهجية البحث

تستند هذه الدراسة إلى منهجية بحث نوعي، تهدف إلى استكشاف الإجراءات والتدابير المتعلقة بالأمن السيبراني في المتاجر الإلكترونية، دراسة حالة: بازاري.

وذلك من خلال إجراء مقابلات متعمقة مع مدير تقنية المعلومات قس منصة بازاري.

تعتمد أدوات جمع البيانات على المقابلات المباشرة، حيث قام فريق البحث بتدوين وتسجيل المعلومات المقدمة من المشاركين لضمان الدقة والموثوقية. ويتم تحليل البيانات باستخدام التحليل الموضوعي، بهدف استخلاص الأنماط والموضوعات الرئيسية المتعلقة بموضوع البحث. إضافةً إلى المقابلات المتعمقة، استندت الدراسة إلى بحث شامل عبر الإنترنت لتوسيع نطاق فهمنا للأمن السيبراني في المتاجر الإلكترونية،

وذلك من خلال مراجعة الأدبيات الأكاديمية والتقارير الصادرة عن الجهات المتخصصة في اليمن وخارجه.

نظرًا لطبيعة البحث النوعي، يتم التركيز على استكشاف التجارب والممارسات بدلاً من اختبار الفرضيات، مما يقلل من القيود المحتملة. ومع ذلك، قد تظهر بعض القيود المتعلقة بتعميم النتائج على مجتمع أوسع، نظرًا لحجم العينة المحدود. يتم الالتزام بأخلاقيات البحث من خلال الحصول على موافقة المشاركين وضمان سرية المعلومات المقدمة.

VI. الدراسات السابقة

1. E-Commerce Supply Chains with Considerations of Cyber-Security [4]

يستعرض هذا البحث قضايا الأمن السيبراني في التجارة الإلكترونية. يهدف إلى تقييم التدابير الأمنية الحالية ومعرفة نقاط الضعف، واقتراح إجراءات وتدابير لتقليل المخاطر.

يركز البحث على:

1. تحديات الأمن السيبراني: تشمل تسرب البيانات وهجمات الفدية.
2. 2.الحلول: multi-factor authentication، Encryption، بوابات الدفع الآمنة.
3. أهمية تدريب وزيادة الوعي الموظفين بأهمية الأمن السيبراني.
4. دراسة القوانين والمعايير الدولية ومتطلبات الامتثال.
5. يسعى البحث لتعزيز الأمن السيبراني في سلاسل التوريد للتجارة الإلكترونية للحفاظ على البيانات وبناء سمعة قوية في السوق، مما يؤدي إلى نمو مستدام في الاقتصاد الرقمي.[4]

2. Cybersecurity and E-commerce in Free Trade Agreements [5]

البحث يركز على التحول الرقمي وتأثيره العميق على الاقتصاد العالمي. من خلال تحليل النمو الهائل في التكنولوجيا، وخاصة الإنترنت، الحوسبة السحابية، البيانات الضخمة، إنترنت الأشياء والذكاء الاصطناعي. يُسلط الضوء على كيفية ارتباط العالم المادي بكل نشاط بشري من خلال الأجهزة والشبكات، ويعرض تأثير الرقمنة على التجارة الإلكترونية والأمن السيبراني.

VII. أهداف البحث

تقديم إحصاءات حول كمية البيانات الضخمة المتدفقة عبر الإنترنت وتأثيرها على الاقتصاد.

كيفية تعزيز التجارة الإلكترونية وتحديد العوامل التي ساهمت في نموها.

تحليل التهديدات والفرص المتعلقة بالأمن السيبراني وأهمية التعاون الدولي لحماية الفضاء الإلكتروني.

تحديد التحديات والسياسات من خلال تقديم توصيات حول كيفية التعامل مع المخاطر في الفضاء الإلكتروني لضمان عدم عرقلة التجارة الإلكترونية.[5]

3. Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies [6]

تبحث هذه الورقة البحثية في تهديدات الأمن السيبراني السائدة التي تواجه التجارة الإلكترونية، وتستكشف الاتجاهات الحالية لهذه التهديدات. تُحدد الدراسة فئات رئيسية من التهديدات، مثل هجمات التصيد الاحتيالي، والبرامج الضارة، واختراقات البيانات، والتهديدات الداخلية، والتي يتميز كل منها بقدرات متزايدة التطور والتدمير. من خلال تحليل الحوادث البارزة الأخيرة والتهديدات الخاصة بالقطاع، تُقدم الدراسة فهمًا شاملاً لكيفية تأثير هذه التهديدات على مختلف قطاعات التجارة الإلكترونية. واستجابةً لتنامي مشهد التهديدات، تُحدد الورقة استراتيجيات تخفيف مختلفة. تُناقش التدابير التقنية، مثل التشفير، وبوابات الدفع الآمنة، وأنظمة كشف التسلل، إلى جانب الممارسات التنظيمية، بما في ذلك تدريب الموظفين، وتخطيط الاستجابة للحوادث، وسياسات التحكم في الوصول. تُشدد هذه الورقة على أهمية الامتثال القانوني والتنظيمي، مُسلِّطةً الضوء على ضرورة التزام الشركات بلوائح مثل اللائحة العامة لحماية البيانات (GDPR) وقانون خصوصية المستهلك في كاليفورنيا (CCPA). بالإضافة إلى ذلك، تستكشف الورقة دور التعاون وتبادل المعلومات بين الجهات الفاعلة في هذا القطاع لتعزيز دفاعات الأمن السيبراني الجماعية. من خلال دراسة التهديدات المتطورة والتدابير الفعالة لمواجهتها، تهدف هذه الورقة إلى تقديم رؤى قيّمة وتوصيات عملية لشركات التجارة الإلكترونية. تُؤكد النتائج على ضرورة اتباع نهج استباقي ومتعدد الجوانب للأمن السيبراني، يجمع بين التدابير التكنولوجية والتنظيمية والتنظيمية لحماية بيئات التجارة الإلكترونية من التهديدات السيبرانية المتزايدة التعقيد.

4. Exploring the Role of Cyber Security Measures (Encryption, Firewalls, and Authentication Protocols) In Preventing Cyber-Attacks on E-Commerce Platforms [7]

تسعى هذه الدراسة إلى دراسة أهمية تدابير الأمن السيبراني، وتحديدًا قوة التشفير (ES)، وتكوين جدار الحماية (FC)، وبروتوكولات المصادقة (AP)، في حماية منصات التجارة الإلكترونية من الهجمات الإلكترونية. وتضمنت عملية جمع البيانات إجراء استبيان لمحترفي تكنولوجيا المعلومات المسؤولين عن الإشراف على عمليات التجارة الإلكترونية في مجموعة من المؤسسات الموجودة في المملكة العربية السعودية. واستُخدمت طريقة أخذ العينات الملائمة لتوزيع ما مجموعه 300 استبيان، اختيرت منها 190 إجابة مكتملة للتحليل. وقد تم تقدير نموذج القياس، الذي شمل متغيرات مثل قوة التشفير (ES)، وتكوين جدار الحماية (FC)، وبروتوكولات المصادقة (AP)، والتدريب الأمني (ST)، وحوادث الهجمات الإلكترونية (CAI)، وثقة العملاء (CT)، ووقت الاستجابة للحوادث (IRT)، باستخدام نموذج المعادلة الهيكلية في Amos. وتقدم نتائج هذه الدراسة رؤى ثاقبة حول العلاقة بين تدابير الأمن السيبراني وتأثيرها على وتيرة الهجمات الإلكترونية. وتسلط الدراسة الضوء على أهمية التشفير، وتكوين جدار الحماية، وبروتوكولات المصادقة في تعزيز منصات التجارة الإلكترونية. بالإضافة إلى ذلك، تبحث هذه الدراسة في تأثير التدريب الأمني على تحسين الوضع العام للأمن السيبراني، وأثره اللاحق على ثقة العملاء. كما تأخذ الدراسة في الاعتبار مدة الاستجابة للحوادث كعامل حاسم في الحد من عواقبها. تُسهم نتائج هذه الدراسة في فهم أشمل لبيئة الأمن السيبراني في مجال التجارة الإلكترونية.

VIII. الخلفية النظرية

المبحث الأول:

- **منصة بازاري:[8]**

تأسست شركة "بازاري" في عام 2018 في مدينة عدن، اليمن. بدأت الشركة كمتجر إلكتروني يهدف إلى تقديم منتجات بأسعار معقولة. مع مرور الوقت، نجحت "بازاري" في توسيع نطاق عملها بفضل استراتيجياتها الفعالة في التسويق والابتكار، مما جعلها أكبر متجر إلكتروني في اليمن..

الهدف: نسعى لتغيير وبناء مستقبل صناعة التجارة الإلكترونية في اليمن من خلال تطوير الخدمات اللوجستية والعمليات والمدفوعات.

المهمة: توفير بيئة شراء سهلة وآمنة من خلال تسهيل عملية الدفع والاستلام وخدمة التوصيل للمنزل وسياسة استرجاع سهلة

طبيعة العمل: نربط بين البائع والمشتري عن طريق منصتنا الإلكترونية لخلق تجربة تسوق سهلة وسلسة من خلال نظام محكم لمتابعة رحلة العميل من البداية إلى النهاية

المنتجات والخدمات

الإلكترونيات :تقدم "بازاري" مجموعة متنوعة من الأجهزة الإلكترونية مثل الهواتف المحمولة، الأجهزة اللوحية، والتلفزيونات، وأجهزة الكمبيوتر.

أجهزة المنزل :تشمل الأجهزة المنزلية الصغيرة والكبيرة مثل المكانس الكهربائية، الميكروويف، وأجهزة التبريد.

ملحقات التلفاز :تقدم ملحقات متنوعة مثل أجهزة الاستقبال، السماعات، والكاميرات.

الجولات :تشمل الهواتف الذكية، الأجهزة اللوحية، والملحقات المتعلقة بها.

أجهزة لوحية :تقدم "بازاري" مجموعة متنوعة من الأجهزة اللوحية لأغراض متعددة.

الأزياء والإكسسوارات :تشمل ملابس نسائية ورجالية، بالإضافة إلى الإكسسوارات مثل الحقائب والمجوهرات.

الرياضة واللياقة البدنية :تقدم معدات رياضية للياقة البدنية والأدوات المتعلقة بالرياضة.

السيارات والدراجات النارية :توفر "بازاري" ملحقات السيارات والدراجات النارية المختلفة.

الصحة والعناية الشخصية :تشمل منتجات العناية بالبشرة، الشعر، وكذلك الأجهزة الخاصة بالعناية الشخصية مثل الماكينات الكهربائية.

منتجات منزلية :تشمل الأدوات المنزلية، والمستلزمات اليومية.

ألعاب وهوايات :تقدم "بازاري" مجموعة من الألعاب والمنتجات المتعلقة بالهوايات.

سوبر ماركت :توفر "بازاري" مجموعة واسعة من المنتجات الغذائية والمواد الأساسية.

السوق المستهدف

تستهدف "بازاري" جميع الفئات العمرية وجميع الأجناس. تسعى الشركة لتوفير منتجات متنوعة تلبي احتياجات الأفراد من جميع الأعمار، مما يجعلها جذابة للمتسوقين من مختلف الفئات..

الاستراتيجيات التسويقية

تستخدم "بازاري" استراتيجيات تسويقية مبتكرة، منها

التسويق عبر المؤثرين :- تتعاون مع مؤثرين مشهورين على منصات مثل إنستغرام وتيك توك لزيادة الوعي بالعلامة التجارية.

العروض الترويجية والخصومات :- تقدم الشركة خصومات مغرية وعروض ترويجية جذابة لجذب العملاء الجدد.

التفاعل مع العملاء :- تعتمد "بازاري" على استطلاعات الرأي ومراجعات العملاء لتحسين منتجاتها وتجربة التسوق.

مخطط رقم (1): منصة بازاري

المبحث الثاني:

- **تهديدات الأمن السيبراني للتجارة الإلكترونية:**

تواجه منصات التجارة الإلكترونية في اليمن مجموعة من التهديدات السيبرانية التي قد تعطل العمليات التجارية

وتعرض بيانات العملاء للخطر. تشمل التهديدات الرئيسية:

- **هجمات التصيد الاحتيالي (Phishing attacks)[9] :**

هجوم التصيد الاحتيالي هو وسيلة لإرسال رسائل بريد إلكتروني احتيالية تبدو وكأنها تأتي من مصادر موثوقة. الهدف الرئيسي من هذا النوع من الهجمات هو الحصول على معلومات شخصية وبيانات اعتماد. يُعتبر هجوم التصيد الاحتيالي شكلًا من أشكال الهندسة الاجتماعية والخداع التقني. يتجسد ذلك في شكل رسائل بريد إلكتروني تحتوي على روابط مدمجة يمكن أن تحمل برمجيات خبيثة إلى النظام. أحيانًا تقود هذه الروابط إلى مواقع غير شرعية تجعلنا نقوم بتنزيل برمجيات خبيثة أو كشف معلوماتنا الشخصية. تستخدم هجمات التصيد الاحتيالي مجموعة من الأدوات الإعلامية، مثل الرسائل والمكالمات. تشمل تقنيات التصيد المختلفة: هجمات "وايلينغ"، "سفير التصيد"، "فارمينغ"، والتصيد الخداعي. كما يوضح المخطط رقم (2) طريقة عمل التصيد الاحتيالي[10]

لتقليل خطر هجمات التصيد الاحتيالي، يمكن استخدام التفكير النقدي، التحقق من الروابط من خلال تمرير المؤشر عليها، تحليل رؤوس البريد الإلكتروني، واستخدام تقنيات "ساند بوكس". علاوة على ذلك، من خلال زيادة الوعي بين موظفي المؤسسات وكذلك الأفراد، يمكننا الحد من هجمات التصيد الاحتيالي إلى حد ما.[11]

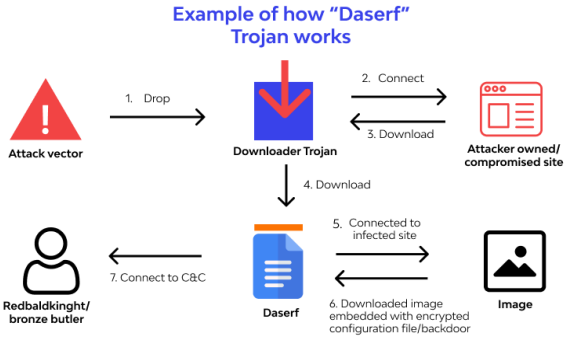
مخطط رقم (2): ألية عمل التصدي الاحتيالي

- **هجمات البرمجيات الخبيثة (Malware Attack):**

هجوم البرمجيات الخبيثة هو نوع من الهجمات السيبرانية يتم فيه تثبيت برامج ضارة على جهاز المستخدم دون موافقته. تشمل هذه البرمجيات ما يُعرف الآن بالفيروسات، والبرمجيات التجسسية، وبرمجيات الفدية، وغيرها. يتم ربط الشيفرة الخبيثة بالشيفرة الشرعية، وتنتشر وتُنفذ من تلقاء نفسها. يمكن للبرمجيات الخبيثة الوصول إلى الشبكات الخاصة، وتعطيل بعض العمليات الحاسوبية، وسرقة المعلومات الحساسة أو أي بيانات أخرى للمستخدم، وبالتالي تحقيق مكاسب غير مشروعة من الهدف. حاليًا، تهدف البرمجيات الخبيثة بشكل أكبر إلى استهداف المعلومات التجارية أو المالية بدلاً من أي معلومات شخصية.[12]

أكثر أنواع البرمجيات الخبيثة شيوعًا تشمل:

- الفيروسات: برامج ضارة ترتبط بأي برنامج كمبيوتر، تتكرر وتعدل الشيفرة عند التنفيذ. يمكن أن تنتشر عن طريق تنزيل ملف أو تشغيل برنامج.
- الدودة (Worms): تنتشر عبر أجهزة الكمبيوتر أو الشبكات من خلال مرفقات البريد الإلكتروني. قد يؤدي ذلك إلى هجمات حرمان الخدمة.
- التروجان (Trojans): واحدة من أخطر البرمجيات الخبيثة التي تحتوي على وظائف ضارة. تختبئ داخل برنامج مفيد ولا تتكرر مثل الفيروسات[13]. كما يوضح المخطط رقم (3) آلية عمل حصان طروادة[14].



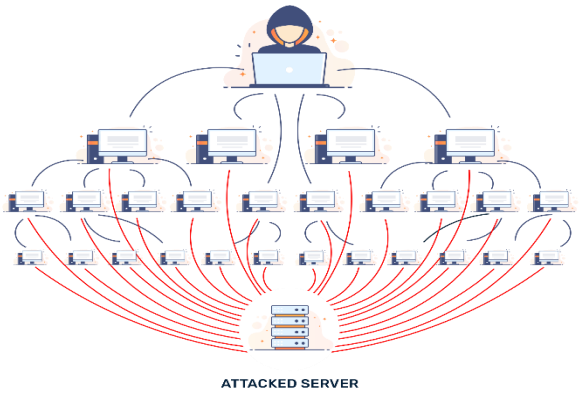
مخطط رقم (3): ألية عمل حصان طروادة

- برمجيات الفدية (Ransomware): نوع من البرمجيات الضارة التي تقفل بيانات المستخدم ما لم يتم دفع فدية. من الصعب جدًا منع هذا الهجوم على الرغم من أن الشيفرة بسيطة[15].
- البرمجيات التجسسية (Spyware):نوع من البرمجيات الخبيثة التي تراقب نشاط المستخدم دون موافقته وتبلغ المهاجم.[6]

- هجمات حرمان الخدمة (DoS) وهجمات حرمان الخدمة الموزعة (DDoS)[16]

هجوم حرمان الخدمة هو هجوم يقوم بتجاوز موارد النظام بحيث لا يمكنه الاستجابة لطلبات الخدمة. يتم إطلاق هجوم DDoS من قبل جهاز مضيف متأثر ببرمجيات خبيثة يتحكم بها المهاجم. في هذا النوع من الهجمات السيبرانية، يتم جعل موارد الجهاز أو الشبكة غير متاحة للمستخدم المستهدف من خلال تعطيل خدمة المضيف المتصل بالإنترنت. تشمل أنواع هجمات DoS وDDoS: هجوم TCP SYN flood، وهجوم teardrop، وهجوم smurf، وهجوم ping-of-death، والشبكات الروبوتية (botnets).

من الصعب جدًا منع هجوم DoS، حيث إنه من الصعب التمييز بين الطلبات المشروعة والطلب الخبيث نظرًا لاستخدامهما نفس المنفذ والبروتوكول. لحماية النظام من هجمات حرمان الخدمة، يجب التأكد من أن النظام يحتوي على نظام كشف التسلل (IDS) ومنتجات حماية DDoS. من الضروري أيضًا التأكد من وجود عرض نطاق إنترنت زائد في المؤسسة المعنية. حيث يساعد وجود عرض نطاق كبير لطلبات خدمة الحركة المرورية في الحماية من هجمات DDoS منخفضة الحجم. ويوضح المخطط رقم(4) طريقة هجمات حرمان الخدمة [17]



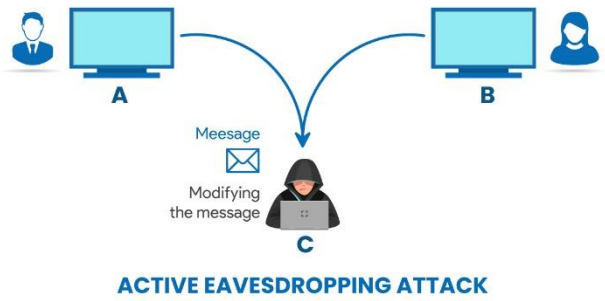
مخطط رقم(4): هجمات حرمان الخدمة

- **هجوم التنصت (Eavesdropping attack):**

يُعرف أيضًا بهجوم "sniffing" أو "snooping". يتعامل هجوم التنصت مع اختراق البيانات التي تُرسل عبر الأجهزة الرقمية. يستخدم المهاجم شبكة غير آمنة للتواصل ويفحص البيانات المرسلة والمستلمة. نظرًا لأن هذا النوع من الهجمات لا يظهر أي عمليات غير طبيعية أثناء النقل عبر الشبكة، فمن الصعب جدًا اكتشافه.

باستخدام هذه الطريقة، يمكن للمهاجم الحصول على معلومات متنوعة مثل رقم بطاقة الائتمان، وكلمات المرور، وغيرها من المعلومات الحساسة المرسلة عبر الشبكة. قد يقوم المهاجم بإدخال جهاز تنصت

(sniffer) على كمبيوتر أو خادم لتنفيذ هجوم التنصت والاستيلاء على البيانات أثناء النقل.كما يوضح المخطط رقم (5) طريقة هجوم التنصت[18]



مخطط رقم(5): هجوم التنصت

يمكن أن يكون هذا الهجوم من نوعين:

1. التنصت السلبي (Passive Eavesdropping): يحدث عن طريق الاستماع إلى نقل الرسائل في الشبكة، حيث يكشف المهاجم البيانات.
2. التنصت النشط (Active Eavesdropping): يحصل المهاجم على البيانات من خلال التظاهر بأنه وحدة صديقة وإرسال استفسارات للمستقبل.

يساعد استخدام برامج مكافحة الفيروسات، وجدران الحماية، والشبكات الخاصة الافتراضية (VPN)، والتشفير، وتجنب الشبكات العامة لنقل البيانات الحساسة في الوقاية من هجوم التنصت[19].

تحديات الأمن السيبراني في اليمن:

على الرغم من التركيز العالمي على الأمن السيبراني، تواجه اليمن تحديات مميزة:

- إطار تنظيمي ضعيف: تفتقر اليمن إلى قانون شامل لألمن السيبراني، مما يؤدي إلى ضعف تطبيق السياسات والمعايير الأمنية.
- وعي ضعيف بالأمن السيبراني: العديد من أصحاب الأعمال والمستهلكين في اليمن لديهم معرفة محدودة بالتهديدات الأمنية السيبرانية وأفضل الممارسات.
- بنية تحتية تكنولوجية ضعيفة: تزيد عدم استقرار الاتصال بالإنترنت في البالد، والأنظمة القديمة، والاعتماد
- على خدمات استضافة غير آمنة من مخاطر الأمن السيبراني.
- تطبيق القانون غير المتسق: غالبًا ما تمر الجرائم السيبرانية دون عقاب بسبب غياب القدرات الجنائية الرقمية وآليات تطبيق القانون المنسقة

إستراتيجيات الأمن السيبراني:

- أنظمة الكشف عن التهديدات المتقدمة: قامت الشركة بنشر أدوات أمان مدعومة بالذكاء الاصطناعي للكشف عن التهديدات المحتملة والتخفيف منها في الوقت الحقيقي.
- الدقيقات الأمنية المنتظمة واختبارات الاختراق: تقوم بازاري بإجراء اختبارات أمنية ربع سنوية واختبارات
- اختراق لتحديد الثغرات وتعزيز الدفاعات.
- مصادقة متعددة الطبقات وتشفير البيانات: يتم حماية جميع حسابات المستخدمين بمصادقة متعددة العوامل، ويتم تشفير البيانات الحساسة باستخدام معايير .AES-256
- برامج توعية الموظفين والعملاء: تستثمر الشركة في تدريب موظفيها وتثقيف العملاء حول أفضل ممارسات الأمن السيبراني.

التعاون مع الهيئات التنظيمية: تعمل بازاري عن كثب مع الوكالات المحلية والدولية لألمن السيبراني للبقاء على اطالع بالتهديدات الناشئة ومتطلبات الامتثال.

المبحث الثالث:

التدابير الأمنية المتبعة في بازاري:

وقد أشار مدير التقنية في منصة بازاري، "نلتزم بأعلى معايير الأمن السيبراني لضمان حماية بيانات المستخدمين وتأمين المعاملات الرقمية. استراتيجيتنا الأمنية مبنية على أفضل الممارسات في الصناعة وتشمل التدابير التالية:

1. تشفير البيانات :يتم تشفير جميع البيانات الحساسة باستخدام بروتوكولات تشفير متقدمة لحماية البيانات أثناء النقل وعند الراحة، مما يضمن الامتثال للمعايير الأمنية العالمية.
2. المصادقة متعددة العوامل :(MFA) يتم تطبيق المصادقة الثنائية (2FA)للمستخدمين والمشرفين لتعزيز أمان الحساب ومنع الوصول غير المصرح به.
3. إدارة الوصول والصلاحيات :يتم تطبيق نموذج الوصول بأدنى صلاحية (Least Privilege Access) لتقييد الأذونات إلى الوظائف الضرورية فقط، مما يقلل من المخاطر الأمنية الداخلية المحتملة.
4. مراقبة التهديدات والاستجابة للحوادث :يتم استخدام حلول إدارة معلومات الأمن والأحداث (SIEM) لاكتشاف التهديدات والاستجابة لها في الوقت الفعلي، مما يضمن التخفيف الاستباقي للحوادث الأمنية.
5. اختبار الاختراق الدوري :يتم إجراء اختبارات اختراق دورية بناءً على الأطر الأمنية المعترف بها لتحديد ومعالجة الثغرات قبل أن يتم استغلالها.
6. خطط النسخ الاحتياطي واستمرارية الأعمال :يتم تنفيذ النسخ الاحتياطي المشفر الدوري واستراتيجيات التعافي من الكوارث للحفاظ على استمرارية الخدمة وتقليل فترة التوقف في حال حدوث حوادث أمنية".

منصة بازاري بين التحديات والفرص: دراسة تحليلية

تستمر التهديدات السيبرانية في التطور، مما يتطلب تحسينات مستمرة في استراتيجيات الأمان. تشمل بعض المجالات الرئيسية للتحسين:

1. هجمات حشو بيانات الاعتماد والتصيد الاحتيالي

- الحل: تعزيز آليات المصادقة، توسيع استخدام المصادقة بدون كلمة مرور، وتحسين برامج التوعية للمستخدمين لتقليل مخاطر التصيد الاحتيالي.

2. أمان التطبيقات وواجهات البرمجة

- الحل: تنفيذ مبادئ أمان الثقة الصفرية (Zero Trust Security)، تعزيز اختبار الأمان الآلي، ومراقبة واجهات البرمجة باستمرار للكشف عن الثغرات.

3. هجمات رفض الخدمة الموزعة(DDoS)

- الحل: استخدام جدران الحماية لتطبيقات الويب (WAF) ودمج شبكات توصيل المحتوى (CDN) لتقليل تأثير الهجمات واسعة النطاق.

التهديدات السيبرانية الشائعة التي تستهدف منصة بازاري:

تواجه منصات التجارة الإلكترونية، بما في ذلك بازاري، مجموعة متنوعة من التهديدات السيبرانية. وتشمل التهديدات الأكثر شيوعًا:

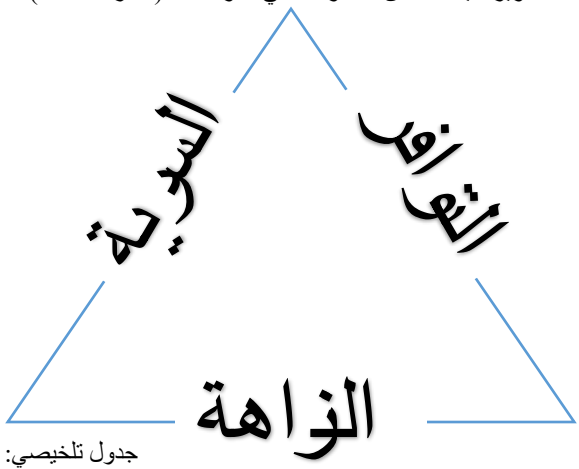
1. هجمات التصيد الاحتيالي –يحاول المجرمون الإلكترونيون سرقة بيانات اعتماد المستخدمين ومعلومات الدفع من خلال رسائل البريد الإلكتروني الاحتيالية.
2. هجمات – DDoS هجمات واسعة النطاق تهدف إلى إغراق وتعطيل الخدمات عبر الإنترنت.
3. استغلال واجهات البرمجة – (API) استهداف الثغرات في واجهات البرمجة للوصول غير المصرح به إلى البيانات الحساسة أو وظائف النظام.

IX. التوصيات:

- تعزيز تنظيمات الأمن السيبراني: يجب على اليمن تطوير وتطبيق قوانين الأمن السيبراني التي تحمي الأعمال التجارية الإلكترونية والمستهلكين.
- تشجيع أنظمة الدفع الآمنة: ينبغي على الشركات اعتماد بوابات دفع موثوقة تتمتع بقدرات كشف الاحتيال.
- تحسين البنية التحتية لتكنولوجيا المعلومات: تعتبر الاستثمارات في الاستضافة الآمنة، والإنترنت عالي.
- السرعة، وقدرات الطب الشرعي الرقمي أمرًا حيويًا.
- تشجيع برامج تدريب الأمن السيبراني: يجب توسيع المبادرات التوعوية لتثقيف الشركات حول أفضل ممارسات الأمن السيبراني.

طرق تعزيز إجراءات وتدابير الامن السيبراني في منصة بازاري:

يعتبر مثلث AIC (التوافر والسلامة والسرية) نموذجًا مصممًا لتوجيه تطوير سياسات أمن المعلومات في المؤسسات (انظر الشكل 1).



مخطط رقم(6): AIC Model

التوافر يعني ضمان توفر البيانات المطلوبة في جميع الأوقات لمن يحتاجها. النزاهة تعني ضمان صحة البيانات وحمايتها من التعديل غير المصرح به أو التلف غير المقصود. السرية تعني أن البيانات المخزنة على الحاسوب يجب أن تكون متاحة فقط لمن يملك الحق أو الحاجة إلى الاطلاع عليها. نموذج AIC مقبول على نطاق واسع في المؤسسات، ويُعتبر حجر الزاوية في الحفاظ على الأمن. يمكن استخدام أساليب مختلفة لدعم أهداف AIC. وتشمل هذه الأساليب المصادقة، والتشفير، والتحكم في الوصول، وجدران الحماية، وأنظمة كشف ومنع التسلل، وتلخيص الرسائل أو المجموع الاختباري، ومصائد العسل، والتوقيع الرقمي، والشهادة الرقمية. يوضح الجدول 2 الأساليب المستخدمة وكيفية ارتباطها بنموذج AIC [20].

تتلخص خطوات تعزيز الإجراءات والتدابير على النحو التالي:

1. **المصادقة:**

الهدف: ضمان يضمن وصول المستخدمين الشرعيين فقط إلى النظام. حيث تخدم السرية والنزاهة.

2. **التشفير:**

الهدف: يضمن عدم تمكن الأشخاص غير المصرح لهم من قراءة البيانات. حيث تخدم السرية.

3. **التحكم في الوصول:**

الهدف: يضمن وصول المستخدمين فقط إلى أجزاء النظام التي يحتاجونها. حيث تخدم السرية والنزاهة.

4. **ملخص الرسائل أو المجموع الاختباري:**

الهدف: يمكّن من فحص البيانات بحثًا عن أي تلاعب. حيث يخدم النزاهة.

5. **جدار الحماية:**

الهدف: يمنع المهاجمين من دخول النظام. حيث يخدم السرية والنزاهة والتوافر.

6. **أنظمة كشف ومنع التطفل:**

الهدف: يكشف ويحلل ويمنع عمليات التطفل من خارج النظام وداخله. حيث يخدم السرية والنزاهة والتوافر.

7. **مكافحة الفيروسات وبرامج التجسس:**

الهدف: اكتشاف الفيروسات وبرامج التجسس وحظرها وإزالتها. حيث يخدم السرية والنزاهة والتوافر.

8. **Honeypot:** آلية تم ضبطها للكشف عن محاولات الاستخدام غير المصرح به لأنظمة المعلومات أو صدها أو التصدي لها بطريقة ما [21]. حيث يخدم السرية والنزاهة والتوافر.

9. **التوقيع الرقمي والشهادة ـ البنية التحتية للمفتاح العام (PKI):**

يضمن عدم التنصل من المسؤولية وإرسال البيانات بأمان عبر الإنترنت باستخدام التشفير. حيث يخدم السرية والنزاهة.

جدول تلخيصي: تعزيز نموذج AIC في "بازاري"

الإجراء	السرية	النزاهة	التوافر	أداة التحسين
المصادقة	✓	✓	×	MFA + Zero Trust
التشفير	✓	×	×	AES-256 + TLS 1.3
التحكم في الوصول	✓	✓	×	ZTNA + Least Privilege
المجموع الاختباري	×	✓	×	SHA-3 + التوقيع الرقمي
جدار الحماية	✓	✓	✓	WAF + AI
IDS/IPS	✓	✓	✓	Hybrid IDS/IPS + Honeynets
مكافحة البرمجيات	✓	✓	✓	EDR + التعلم الآلي
مصائد العسل	✓	✓	×	Deception Networks
PKI	✓	✓	×	Automated PKI + ID-Based Cryptography

X. الخلاصة:

يتناول البحث "الإجراءات والتدابير المتعلقة بالأمن السيبراني بالمتاجر الإلكترونية في الجمهورية اليمنية" وضرورة أهمية الأمن السيبراني في التجارة الإلكترونية ،مركزاً على منصة "بازاري" و يعرض التهديدات السيبرانية مثل هجمات التصيد الاحتيالي والبرمجيات الخبيثة وايضاً يحدد عيوب الأنظمة الامنية و يستند البحث الى منهجية تحتوي دراسات ميدانية وتحليل الحوادث السابقة لمقارنة الممارسات مع المعايير الدولية بينما يبرز المشاكل الامنية التي تواجه اليمن مثل وعي محدود بالأمن السيبراني والبنيه التحتية الضعيفة و تشير الدراسة بدعم تنظيمات الأمن السيبراني وتعزيز البنية التحتية لتكنولوجيا المعلومات في النهاية، يؤكد البحث على اهميه اتخاذ إجراءات فعالة لضمان حماية البيانات الحساسة وتطوير استمراريه الأعمال.

XI. التوصيات:

توصيات لتحسين إجراءات الأمن السيبراني في "بازاري"

1. تعزيز آليات المصادقة والتشفير (السرية والنزاهة)

- التوصية:
  - تطبيق مصادقة متعددة العوامل (MFA) قائمة على FIDO2/WebAuthn بدلاً من المصادقة الثنائية (2FA) التقليدية، مع دمج المصادقة التكيفية لتقييم مخاطر السياق (مكان الدخول، سلوك المستخدم).
  - ترقية تشفير البيانات إلى AES-256-GCM مع تنفيذ إدارة مفاتيح دورية مدعومة بـ HSM(Hardware Security Module).

2. تطبيق نموذج "الثقة الصفرية (Zero Trust) "(السرية والنزاهة)

- التوصية:
  - تنفيذ تقسيم الشبكة دقيق (Micro-Segmentation) لعزل أنظمة الدفع وقواعد البيانات.
  - اعتماد Zero Trust Network Access (ZTNA) للتحقق المستمر من هوية المستخدمين وحالة الأجهزة.

3. تطوير جدران حماية تطبيقات الويب WAF (التوافر والنزاهة)

- التوصية:
  - نشر WAFمدعوم بالذكاء الاصطناعي للكشف عن هجمات (SQLi, XSS)في الوقت الفعلي، مع تكامله مع شبكات CDNلامتصاص هجمات.DDoS
  - إجراء اختبارات اختراق دورية لواجهات برمجة التطبيقات (APIs).

4. تعزيز البنية التحتية والتوعية (التوافر)

- التوصية:
  - الاستثمار في بنية تحتية مرنة (مثل خوادم موزعة جغرافيًا) لضمان استمرارية الخدمة أثناء هجمات.DDoS
  - تطوير برامج توعوية للموظفين والعملاء حول التصيد الاحتيالي، باستخدام محاكاة هجمات شهرية.

5. تعزيز الامتثال التنظيمي (النزاهة)

- التوصية:
  - تبني معايير PCI-DSS لأنظمة الدفع،و ISO/IEC 27001 لإدارة أمن المعلومات.
  - إنشاء فريق استجابة للحوادث (CIRT) متكامل مع هيئات الأمن المحلية.

XII. المراجع:

[1] R. Gupta, "Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies," *Journal of Advanced Management Studies*, vol. 1, no. 3, pp. 1-10, 2024.

[2] NIST, *SP 800-53 Revision 5*. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[3] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," *Security and Privacy Controls for Information Systems and*

[13] I. Lee, "Trojan horse attack," *Wallarm*, Jan. 30, 2025. [Online]. Available: https://www.wallarm.com/what/trojan-horse-attack

[14] J. Tailor and A. Patel, "A comprehensive survey: ransomware attacks prevention, monitoring and damage control," *International Journal of Research and Scientific Innovation (IJRSI)*, vol. 4, pp. 2321–705, 2017.

[15] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[16] "What are Distributed Denial of Service (DDoS) Attacks?," *Bunny.net*. [Online]. Available: https://bunny.net/academy/security/what-are-distributed-denial-of-service-ddos-attacks/

[17] A. Singh, "What is eavesdropping: how to prevent it?," *Shiksha.com*, Sep. 14, 2023. [Online]. Available: https://www.shiksha.com/online-courses/articles/eavesdropping-how-to-prevent-it/

[18] W. Yang, Z. Zheng, G. Chen, Y. Tang, and X. Wang, "Security Analysis of a Distributed Networked System Under Eavesdropping Attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 7, pp. 1254-1258, Jul. 2020. doi: 10.1109/TCSII.2019.2928558

[19] A. James, W. Bulajoul, Y. Shehu, Y. Li, and G. Obande, "Security challenges and solutions for e-business," in *Institution of Engineering and Technology eBooks*, pp. 121–147, 2018. doi: 10.1049/pbse001e_ch6

[20] "Honeypot (computing)," *Wikipedia*, Nov. 8, 2024. [Online]. Available: https://en.wikipedia.org/wiki/Honeypot_(computing)

Organizations, vol. 5, no. 5, 2020. doi: 10.6028/nist.sp.800-53r5

[4] F. H. Zawaideh et al., "E-Commerce Supply Chains with Considerations of Cyber-Security," 2023 *International Conference on Computer Science and Emerging Technologies (CSET)*, Bangalore, India, 2023, pp. 1-8. doi: 10.1109/CSET58993.2023.10346738

[5] A. Becerril, "Cybersecurity and E-commerce in Free Trade Agreements," *Mexican Law Review*, vol. 13, no. 3, 2020. doi: 10.22201/iij.24485306e.2020.1.14808

[6] A. F. Al Naim and A. M. Ghouri, "Exploring the Role of Cyber Security Measures (Encryption, Firewalls, and Authentication Protocols) in Preventing Cyber-Attacks on E-Commerce Platforms," *International Journal of eBusiness and eGovernment Studies*, vol. 15, no. 1, pp. 444-469, 2023. doi: 10.34109/ijebeg.2023150120

[7] "Homepage," *Bazzarry*. [Online]. Available: https://bazzarry.com/

[8] كاينابريس, "التجارة الإلكترونية والأمن السيبراني.. كيف تحمي متجرك وبيانات العملاء؟," *Kaynapress*, Oct. 4, 2024. [Online]. Available: https://kaynapress.com

[9] S. Shanice, "Complete Guide to Phishing: Techniques & Mitigations - Valimail," *Valimail*, Jun. 5, 2024. [Online]. Available: https://www.valimail.com/resources/guides/guide-to-phishing/

[10] H. F. Aboalhab and M. Farhat, "Social Engineering and Its Role in Maintaining Information Security And Privacy," *Scientific Research Journal of Engineering and Computer Sciences*, vol. 4, no. 2, pp. 1-10, 2024.

[11] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1938–1940, 2017. doi: 10.26483/ijarcs.v8i5.4021

[12] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan Attacks: threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014. doi: 10.1109/jproc.2014.2334493