NTU Journal for Administrative and Human Sciences (2024) : 154 - 179
DOI: https://doi.org/10.56286/ntujahs

IRAQI Academic Scientific Journals

JAHS NTU

P-ISSN: 2789-1240 E-ISSN:2789-1259

NTU Journal for Administrative and Human Sciences

Available online at: https://journals.ntu.edu.iq/index.php/NTU-JMS/index

Intelligent Optical Fraud Monitoring System: Smart Card as a Model.

Fahema Asleawa Haidoo Kas-Hana
Al – Farabi University College

Article Informations

Received:1. 05. 2024
Accepted:15.05. 2024
Published online: 01. 06. 2024

Corresponding author :
Name Fahema asleawa haidoo Al
Al – Farabi university college
Email:
Fahima.asliwa@alfarabiuc.edu.iq

Key Words:
Financial fraud,
Digital system,
Financial monitoring.

A B S T R A C T

Research abstract : The research includes five sections. The first section includes the research methodology, which includes the research problem with the presence of a control and monitoring system on the smart card, the effect of smart optical fraud, and the accounting importance in using the smart card. The goal of the research includes highlighting the monitoring system, the impact of fraud, and the role of the smart card economically and socially. As for the importance of the research, it highlights the role that Performed by the smart card. The research hypothesis was based on the fact that the presence of a smart card optical fraud control and monitoring system leads to reducing and controlling fraud and facilitating it for the citizen economically and socially.

The second section included the smart card, its origins and development, the challenges of its spread, its most famous types, operating systems and applications, and known problems. The third section includes the types of credit card fraud, the high costs of fraud, investment in fraud detection technology, and the role of the card in reducing risks. The fourth section includes the practical aspect, and the fifth section includes conclusions and recommendations.

نظام مراقبة الاحتيال البصري الذكي: البطاقة الذكية أنموذجا.

د : فهيمة اصليوة حيدو

كلية الفارابي / الجامعة

ملخص البحث:

يتضمن البحث خمسة مباحث يشمل المبحث الأول على منهجية البحث والتي تتضمن بمشكلة البحث بوجود نظام تحكم ومراقبة على البطاقة الذكية واثر الاحتيال البصري الذكي والاهمية المحاسبية في استخدام البطاقة الذكية ويتضمن هدف البحث ابراز نظام المراقبة واثر الاحتيال ودور البطاقة الذكية اقتصاديا واجتماعيا اما اهمية البحث ابراز الدور التي تؤديه البطاقة الذكية اما فرضية البحث استندت على ان وجود نظام تحكم ومراقبة الاحتيال البصري الذكي للبطاقة الذكية يؤدي الى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا ، اما المبحث الثاني اشتمل على البطاقة الذكية نشأتها وتطورها وتحديات انتشارها واشهر انواعها وانظمة تشغيل وتطبيقاتها والمشاكل المعروفة . اما المبحث الثالث يتضمن انواع الاحتيال في بطاقة الائتمان وارتفاع تكاليف الاحتيال واستثمار تقنية كشف الاحتيال ودور البطاقة في تقليل المخاطر . اما المبحث الرابع يتضمن الجانب العملي والمبحث الخامس يتضمن الاستنتاجات والتوصيات .

الكلمات المفتاحية : نظام مراقبة ، البطاقة الذكية ، الاحتيال

مقدمة البحث:

إن انتشار التقنيات والتقدم التكنولوجي في جميع مرافق الحياة اقتصاديا واجتماعيا . ومن ابرز سمات العصر الحديث البطاقة الذكية اذ تعتمد على نظام متكامل وطريقة حديثة من طرق الدفع السريعة المعتمدة بدلا من طريقة الدفع التقليدي وتحظى بقبول عام والثقة في التداول وتعتبر البطاقة الذكية هي بطاقة بلاستيكية تحتوي على شريحة حاسوبية مدمجة يمكن استخدامها لتخزين المعلومات مثل معلومات شخصية ومعلومات مالية ومعلومات طبية ويمكن استخدام البطاقة الذكية في التحقق من هوية الشخص ومنع الاحتيال في معاملات بطاقات الائتمان والبطاقة الذكية لها ميزة تتمتع بمستوى عال من الأمان وسهولة استخدامها وقابليتها للتوسع والتحديات التي تواجها هي التكلفة والخصوصية . ويعتبر نظام مراقبة الاحتيال البصري الذكي نظام يستخدم الذكاء الاصطناعي للكشف عن الاحتيال في الصور ومقاطع الفيديو ويستخدم خوارزميات التعلم الآلي للتعرف على أنماط التي تشير الى الاحتيال وهو نظام واسع جدا بحيث يشمل نموذج من البطاقة الذكية وسيتم التركيز عليها في هذا البحث وكذلك تستخدم على نطاق واسع في مجالات الاتصالات والتمويل والنقل والطب وغيره مثل بطاقات أجهزة انذار وبطاقات فتح الأبواب والكهرباء في الفنادق الحديثة وكذلك بطاقات التسوق عبر الانترنيت ويشمل البحث على خمسة مباحث يشمل المبحث الأول

المنهجية (المشكلة ، الاهمية ، الأهداف ، الفرضية ، مجتمع وعينة البحث ، منهج البحث واستنادا الى فرضية البحث مفادها وجود نظام تحكم ومراقبة الاحتيال البصري للبطاقة الذكية يؤدي نظام المراقبة الى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا . اما المبحث الثاني تناول نشأة البطاقة الذكية وتطورها ومفهومها وتحديات انتشارها واشهر أنواعها في حين تناول المبحث الثالث أنواع الاحتيال في بطاقة الائتمان ودور البطاقة الذكية في تقليل المخاطر . اما المبحث الرابع تناول الجانب التطبيقي . وتوصل البحث الى اثبات الفرضية الأساسية التي تنص على (يؤدي نظام المراقبة للبطاقة الذكية الى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا.

المبحث الاول

منهجية البحث :

اولا : مشكلة البحث :

تتبلور مشكلة البحث بالتساؤلات الآتية :

هل يوجد نظام تحكم ومراقبة على البطاقة الذكية ؟

1- هل يوجد اثر على الاحتيال البصري الذكي ؟

2- هل توجد اهمية محاسبية في استخدام البطاقة الذكية ؟

ثانيا : أهمية البحث :

تبرز اهمية البحث في الدور الذي تؤديه البطاقة الذكية إلى المجتمع اقتصاديا واجتماعيا لانتشارها واتساع التعامل بها عالميا ومحليا والتي تبنتها المصارف لتسهيل عملياتها المصرفية .

ثالثا : هدف البحث :

يسعى البحث إلى تحقيق الاهداف الاتية :

1- ابراز نظام المراقبة على البطاقة الذكية والحد من الاحتيال البصري

2- تسهيل دور البطاقة الذكية اقتصاديا واجتماعيا للمواطن

رابعا : فرضية البحث : استندى البحث على فرضية الأساسية مفادها :(ان وجود نظام تحكم ومراقبة الاحتيال البصري الذكي للبطاقة الذكية يؤدي الى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا) . وتتفرع الى فرعين :

1- لا توجد فروقات ذات دلالة إحصائية في المتغير (يؤدي نظام المراقبة تحكم ومراقبة الاحتيال البصري الذكي للبطاقة الذكية الى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا .

2- توجد فروقات ذات دلالة إحصائية في المتغير (يؤدي نظام المراقبة تحكم ومراقبة الاحتيال البصري الذكي للبطاقة الذكية الى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا و**اجتماعيا** .

خامسا: مجتمع وعينة البحث : يشمل عدد من أساتذة الجامعة ونخبة من حملة شهادة البكلوريوس وشهادة **الدبلوم من موظفي في عدد من المصارف التجارية .**

سادسا : منهج البحث : اعتمد أسلوب الاستقصاء من خلال استمارة الاستبيان

المبحث الثاني

الجانب المفاهيمي لنظام الاحتيال البصري الذكي (البطاقة الذكية)

اولا : البطاقة الذكية نشأتها وتطورها :

في عام 1914 كانت بدايتها عندما قام عدد من الفنادق والشركات التجارية بعمل بطاقة تشبه بطاقة الائتمان الحالية (credit card) وتمنحها لعملائها ليتمكنوا بموجب هذه البطاقة الحصول على مزايا خاصة عند التعامل مع هذه الشركة وكذلك تمنح لهم ائتمان يمكنهم السداد خلال فترة معينة ، وكانت هذه البطاقة تقبل فقط في هذه الشركات وفروعها . واستمر العمل بها إلى عام 1945 عندما بدأ نادي دينرز بتقديم بطاقة بلاستيكية للحصول على السلع والخدمات من الفنادق والمحلات بضمان مصدر البطاقة وفي عام 1958 قام بنك امريكا وبنك تشيزمانهاتن باصدار بطاقة American وانتشرت بشكل واسع في انحاء الولايات المتحدة الامريكية مما ادى الى ظهور مجموعة بنوك اتخذت لتكون جمعية اصدرت بطاقة تسمى ماستركارد Master card . (عوض ، 1988 : 429) .

اما في المانيا تم ابتكار واختراع البطاقات الذكية بواسطة عالم الصواريخ الألماني هيلموت جروتروب وزميله العالم جورجين ديثلوف في عام 1968 ، وتم اعتماد براءة الاختراع في عام 1982 وأول استخدام جماعي للبطاقات في التليفونات المدفوعة بفرنسا عام 1983 وسجل رولاند مورينو براءة ابتكار تصوره لبطاقة الذاكرة في عام 1974 وفي عام 1977 ابتكر هونيويل بول أول بطاقة ذكية مزودة بمعالج دقيق ، وفي عام 1978 سجل بول براءة اختراع الحاسب الدقيق ذي الشريحة الواحدة القابل للبرمجة spom مع تعريف البنية الضرورية لبرمجة الشريحة تلقائيا ، بعد ذلك بثلاث سنوات صنعت موتورولا أول بطاقة بمعالج دقيق وفقا لهذا الاختراع ثم سجل بول ما يقرب 1200 براءة اختراع مرتبطة بالبطاقات الذكية . (petin : 1999)

أما في فرنسا جاء الاستخدام الثاني للبطاقات الذكية مع دمج الرقائق الصغيرة في بطاقات الخصم الفرنسية (البطاقة الزرقاء carte Bleue) في عام 1992 حيث يقوم المستهلك بسداد المدفوعات بإدخال البطاقة في ماكينة التاجر ثم يدخل الرقم الشخصي قبل قبول العملية . وفي منتصف التسعينات أزدهرت في جميع دول

اوربا أنظمة المحافظ الالكترونية التي تعتمد على البطاقات الذكية وتحتوي رقائقها الالكترونية على القيمة المالية التي لا تخزن في حساب خارجي بحيث لا تحتاج التي تقبل البطاقة إلى الاتصال بالشبكة ومن اشهر هذه الدول المانيا والنمسا وبلجيكا وفرنسا وهولندا وسويسرا والسويد وفلندا وبريطانيا والدنمارك والبرتغال . ثم حدث الازدهار الاكبر في البطاقات الذكية في نهاية التسعينات مع طرح شريحة خط المحمول الذكية ومع انتشار وذيوع الهواتف المحمولة في اوروبا اصبحت البطاقات الذكية ايضا شائعة وفي عام 1993 وافقت ماركة الدفع العالمية ماستركارد وفيزا ويوروباي على التعاون معا لتطوير المعايير لاستخدام البطاقات الذكية مع بطاقات الائتمان أو بطاقات الخصم وتم اطلاق الإصدار الأول من اصدار EMV (الحروف الاولى من Europay , Mastercard , visa) في عام 1994 ، وقامت شركة EMVCO المسئولة عن صيانة النظام على المدى البعيد بترقية المعيار في عام 2000 ثم إلى 2004 . (chiedozie:1999)

ويجري حاليا استخدام البطاقة الذكية على نطاق واسع في نظام الهوية الشخصية على المستويات الاقليمية والقومية والدولية وذلك في بطاقات هوية المواطنين وتراخيص القيادة وبطاقات المرضى وغيرها كما يجري حاليا تركيب البطاقات الذكية اللاتلامسية في جوازات السفر الالكترونية المزودة بالبيانات الحيوية لتحسين الأمان في صناعة السفر والسياحة الدولية .

(ar.m.wikipedia.org)

ثانيا : مفهوم البطاقة الذكية (الاحتيال البصري) :

تعتبر البطاقة الذكية من احدث البطاقات البلاستيكية المنتجة على صعيد العالم وتستخدم فيها تكنولوجيا متطورة حيث تضاف شريحة الكترونية بالشريط المغناطيسي الموجود عادة في بطاقات الائتمان . تضم هذه الشريحة في طياتها معالج رقائق صغير يعطي قدرة على خزن المعلومات داخل حافظة خاصة مثل المعلومات الشخصية لحامل البطاقة (الاسم ،الرقم ، تاريخ الميلاد ، الصورة ، العنوان) ، الملف الطبي ورخص القيادة ووجواز السفر وسجل الاسرة والحسابات البنكية .....الخ وفي الشريحة ايضا تطبيقات مثل الرقم السري ومطابقة البصمة والتوقيع الالكتروني وكلمة السر ومفاتيح عامة وخاصة (pittaway:2001) . (إبراهيم ، 2006 :ص24)

للبطاقات الذكية امكانية خزن ومعالجة الاف البايت من البيانات الالكترونية تفوق بثمانين مرة على البيانات المخزونة في الشريط المغناطيسي الموجود في بطاقات الائتمان (الذي له قابلية الخزن فقط دون المعالجة) وذلك لكون الشريحة تحتوي على الرقائق الدقيقة مع الدوائر المتكاملة القادرة على عملية الخزن والمعالجة لهذا

الكم من البيانات . كما أن المعلومات والتطبيقات الموجودة في البطاقة قابلة للتحديث بدون الحاجة إلى تبديل البطاقة ، إن المعلومات الموجودة في البطاقة الذكية يمكن برمجتها في عدة تطبيقات ويمكن تفعيلها من اجل اضافة تطبيقات جديدة بعد ان يتم اصدارها والبطاقة يمكن تصميمها بحيث يمكن ادخالها في القارئ الخاص بها في الماكنة الاوتوماتيكية وهذه البطاقة يمكن ان ترمى أو يستغنى عنها أو يمكن تحميلها (تجديد المعلومات فيها من جديد لإستخدامات اخرى (meckley : 2001) .

ثالثا : تحديات انتشار البطاقة الذكية :

- التكلفة العالية للبطاقات الذكية مقارنة بالبطاقات المغناطيسية والفرق في التكلفة الاولية ولكن هذا الفرق يكون بشكل بارز عندما تتم مقارنة الفروق بينهما في العمر المتوقع والامكانيات وخاصة دعم العديد من التطبيقات وبالتالي تقليل التكلفة على مستوى التطبيق .
- نقص البنية الاساسية التي تدعم البطاقات الذكية .
- الطبيعة الحصرية لنظام تشغيل الشريحة حيث يجب على المستهلك ان يكون تقنيا ملم بتفاصيل انظمة التشغيل حتى يستطيع اختيار البطاقة المناسبة لتطبيق المطلوب .
- نقص المعايير لضمان التوافق المتبادل بين برامج البطاقات الذكية المتنوعة .
- المشكلات القانونية وسياسة الخصوصية المرتبطة بالخصوصية والسرية وقوانين الحماية للمستهلك . (meckley : 2001)

رابعا : أشهر أنواع البطاقة الذكية :

تتميز استخدامات البطاقة الذكية بأنها متنوعة كما تتنوع تكنولوجيات تصنيعها ووسائل تشغيلها وبالتالي كان لابد ان تتعدد انواعها ومسمياتها وفي الواقع تتنوع هذه الانواع وفقا لعدة معايير منها كيفية قراءة وكتابة البيانات على البطاقة ووفقا لهذا النوع لدينا البطاقات التلامسية واللاتلامسية ونوع الرقاقة المزروعة في البطاقة وامكانياتها وفيما يلي شرح لهذه الانواع : (Robinson: 2010)

1- البطاقات التلامسية contact card :

اشهر انواع البطاقات الذكية واكثر شيوعها وينبغي وضعها في جهاز القراءة بحيث يحدث تلامس مباشر على سطح مناطق الاتصال الذهبية في البطاقة ويحدث نقل الاوامر والبيانات وحالة البطاقة عبر نطاق التلامس المادى الكهربية ويستخدم في جميع احجام البطاقات وانواع الشرائح الالكترونية ، البطاقات ذات خاصية التلامس يجب ان تدخل في القارئ لكي تتم عملية نقل المعلومات ، تحتوي البطاقات من هذا النوع على شريحة ذهبية صغيرة طول قطرها حوالي نصف بوصة في مقدمة البطاقة بدلا من الشريط المغناطيسي

الموجود في الخلف في بطاقات الأئتمان ، عندما تدخل البطاقة في القارئ تتصل مع وصلات كهربائية وهي التي من خلالها يتم تنقل المعلومات من وإلى الشريحة . البطاقات التلامسية تستخدم ثمانية دبابيس الكترونية لتتمكن من الاتصال الفعلي بالقارئ .

2- البطاقات اللاتلامسية contactless card :

كل ما تتطلبه هو الاقتراب لمسافة معينة من جهاز القراءة حيث تحتوي كل من البطاقات الذكية وجهاز القراءة على هوائى لاسلكي قصير المدى وتتواصل الهوائيات لاسلكيا باستخدام ترددات الراديو اللاسلكية وتعتمد على تكنولوجيا التحقق من الهوية لاسلكيا RFID وبدلا من إدخال البطاقة في جهاز القراءة يتم تمريرة بالقرب من السطح الخارجي لجهاز القراءة وتعمل هذه البطاقات بذاكرة محدودة وبتردد 125 ميجا هرتز اما البطاقات اللاتلامسية التي يمكن قرائتها وتعديلها فتتواصل بتترد 13.65 ميجا هيرتز . ومن عيوب البطاقات اللاتلامسية تقييد وظائف التشفير وذاكرة المستخدم مقابل بطاقات المعالج الدقيق والمسافة المحدودة بين البطاقة وجهاز القراءة المطلوبة للتشغيل . (Robinson: 2010)

3- البطاقات المزدوجة :

وهي التي تمزج بين التكنولوجيا التلامسية واللاتلامسية في بطاقة واحدة وقد تحتوي هذه البطاقات على شريحتين مختلفتين بخلاف البطاقة ذي الوصلة المزدوجة التي تحتوي على شريحة واحدة مزودة بالوصلتين معا .

4- البطاقات وفقا للذاكرة والمعالج : (Kilili: 2001)

أ- البطاقات المزودة بشريحة ذاكرة : هي البطاقات التي تقتصر وظيفة شريحة الذاكرة المدمجة بها على التخزين والاسترجاع فقط وتشبه هذه الشريحة قرص صلب صغير مع سمات امنية اختيارية ولكنها تقل في الحماية المتوفرة لادارة البيانات وهناك ثلاثة انواع من بطاقات الذاكرة :

- بطاقة الذاكرة المباشرة : تخزن هذه البطاقات البيانات ولا تمتلك معالجة البيانات وهي اقل تكلفة وتعتبر بمثابة اقراص مرنة باحجام مختلفة مع امكانية الغلق .
- بطاقات الذاكرة المحمية المقسمة : تحتوي هذه البطاقات على المنطق الداخلي الخاص بها للتحكم في الوصول للذاكرة في البطاقة ويتم ذلك من خلال كلمة مرور أو مفتاح للنظام ولا يمكن بسهولة نسخ هذه البطاقات ويمكن تتيعها بواسطة معرف على الذاكرة .
- بطاقات الذاكرة ذات القيمة المخزونة : صممت هذه البطاقات لغرض معين وهو تخزين قيمة أو شفرة حماية معينة ويمكن التخلص من هذه البطاقات او إعداد شحنها وتتضمن اغلب البطاقات من هذا النوع إجراءات أمان دائمة في مرحلة التصنيع ومن امثلة هذه البطاقات التيلفون العام في الشوارع

والميادين حيث تحتوي البطاقة على عدد معين من خلايا الذاكرة كل خلية تحتوي على قيمة او وحدة معينة ومع إجراء الاتصال يتم مسح قيم وحدات هذه الخلايا حسب المدة والخلية التي لا تمسح من الصعب كتابتها مرة اخرى وهكذا حتى يتم مسح كل الخلايا وتصبح البطاقة عديمة الجدوى ويتم التخلص منها وفي حالة البطاقات القابلة للشحن يتم عكس هذه العملية فيتم إعادة القيم والبيانات المشفرة في خلايا الذاكرة .

5- البطاقات المزودة بمعالجات دقيقة :

وتحتوي هذه البطاقات على معالج دقيق او رقاقة تحكم دقيقة تدير عملية تخصيص الذاكرة والوصول للملفات ، ويشبه هذا النوع الشرائح الموجودة في كل الحاسبات الشخصية وعند زرعها في البطاقة الذكية تقوم بإدارة البيانات في هياكل ملفات منظمة من خلال نظام تشغيل البطاقة . فالبطاقات الذكية التي تحتوي على معالج دقيق مدمج تمتاز بالقدرة الفريدة على تخزين كميات كبيرة من البيانات وتنفيذ عمليات الحوسبة الخاصة بها مثل التشفير والتوقيعات الرقمية ويمكنها التفاعل بذكاء مع قارئ البطاقة الذكية ويتميز الجيل الحالي من البطاقات الذكية ذات المعالجات بمعالج 8 بت وذاكرة للقراءة فقط سعتها 16 كيلو بت وذاكرة وصول عشوائي سعتها 512 بايت وتتضمن هذه البطاقات القدرة التشفيرة الذاتية مما يتطلب التعامل مع ارقام كبيرة ولهذا تستخدم هذه البطاقات في تطبيقات الهوية الرقمية وهناك عدة امثلة لهذه البطاقات منها :

(oak: 2010) .

- البطاقات التي تحمل قيمة مالية .
- البطاقات التي تحمل قيمة مكافئة للمال (مثل بطاقات التعامل المتكرر في المتاجر والمستشفيات وغيرها) .
- البطاقات التي تتيح الوصول الآمن لشبكة معين .
- البطاقات التي تحمي التليفونات المحمولة من الغش والاحتيال .
- البطاقات التي تحمي اجهزة التليفزيون والدش من القرصنة .

6- بطاقات الذاكرة الضوئية :

(wiki,gttps;// ar.m.wikipedia.org)

تستطيع بطاقات الذاكرة الضوئية تخزين حوالي 10 ميجا بت من البيانات ولكن بمجرد تسجيل هذه البيانات لا يمكن تغييرها او إزالتها وهذا النوع من البيانات مثالي لحفظ السجلات مثل الملفات الطبية وسجلات القيادة وتاريخ السفر وهذه البطاقات لا تحتوي على معالجات خاصة بها واذا كانت البطاقات مشابهة في السعر

للبطاقات ذات الشريحة فإن اجهزة القراءة التي تتمكن من التعامل مع هذه البطاقات غير شائعة ومكلفة للغاية .

خامسا : أنظمة تشغيل البطاقات الذكية :

في حالة البطاقات المزودة بمعالجات دقيقة يلزمها وجود نظام تشغيل لإدارة الملفات والذاكرة والوصول للبيانات التي تخدم التطبيقات المختلفة وهو بديهيا ليس نظام تشغيل مثل الويندوز بالطبع ولكن هو برنامج صغير يتحكم في البطاقة ويدير اتصاله مع اجهزة القراءة في مختلف التطبيقات . ويوجد نوعان اساسيان من انظمة تشغيل البطاقات الذكية : (oak : 2010)

1- نظام البنية الثابتة للملفات ونظام التطبيقات المتغير، وكما هو الحال مع انواع البطاقات الذكية يعتمد اختيار نظام تشغيل البطاقة على التطبيق الذي يخدم البطاقة .
2- البنية الثابتة للملفات : يعامل هذا النوع هذه البطاقات على انه جهاز آمن للحوسبة والتخزين وتقوم الشركة المصنعة بتحديد الملفات والصلاحيات مقدما وهذه المعايير الثابتة مثالية وموفرة في التكلفة لنوع معين من البنية والوظائف الثابتة التي لم تتغير في المستقبل القريب .
3- نظام التطبيقات المتغير : يساعد هذا النوع منظم التشغيل المبرمجين على بناء واختيار وتشغيل تطبيقات مختلفة بشكل آمن وبسبب انفصال نظام التشغيل عن التطبيقات يمكن ترقية البطاقة بسهولة وبشكل متكرر ومن الأمثلة على ذلك شريحة المحمول التي تستقبل حزمة الترقية والحماية من شبكة المحمول ويتم تغيير تطبيقاتها بشكل تفاعلي .
4- التشفير في البطاقات الذكية : من المهام التي تقوم بها المعالجات الدقيقة في اغلب البطاقات الذكية تشفير البيانات بإستخدام لوغاريتمات معقدة وتستطيع البطاقات الذكية التشفيرية توليد ازواج المفاتيح لتجنب مخاطر وجود اكثر من نسخة من المفاتيح (رغم ان تصميم البطاقات الذكية لا يتيح استخراج المفاتيح الخاصة من البطاقة الذكية) ، وهذا النوع من البطاقات الذكية يستخدم في التوقيع الرقمي والهوية الآمنة .
5- اجهزة قراءة البطاقات الذكية : يصف مصطلح جهاز القراءة الوحدة او الجهاز التي تعتمد على الحاسب الشخصي في المعالجة اما الجهاز الطرفي فهو الجهاز الذي يكتفي ذاتيا ويحتوي على المعالج الخاص به وتقوم اجهزة القراءة والاجهزة الطرفية بالقراءة من البطاقات الذكية والكتابة عليها وتوجد اشكال واحجام عديدة من اجهزة القراءة حسب التنوع الكبير في التطبيقات ويمكن التفرقة بين اجهزة قراءة البطاقات الذكية حسب نوع الصلة بالحاسب الشخصي وهي إما المنافذ المتسلسلة آر إس

232 ومنافذ يو إس بي وفتحات PCMCIA وفتحات الاقراص المرنة والمنافذ المتوازية ومنافذ الاشعة تحت الحمراء ولوحات المفاتيح . (wiki,gttps;// ar.m.wikipedia.org)

سادسا : تطبيق البطاقات الذكية : تتميز البطاقات الذكية بتنوع الاستخدامات عوضا عن الكثير من المميزات الاخرى ومن تلك الطرق : (cott&jurgensen:1998)

1- الخدمات المصرفية والتجزئة :بعض الاستخدامات الاكثر شيوعا للبطاقات الذكية هي بطاقات الصراف الالي وبطاقات الائتمان وبطاقات الخصم ، العديد من هذه البطاقات هي كروت PIN g chip التي تتطلب من العميل تقديم رقم PIN من 4إلى 6 ارقام بينما يعرف البعض الاخر ببطاقات " chip and signature " التي تحتاج فقط إلى توقيع للتحقق من صحة البيانات .

وتشمل استخدامات اخرى مالية للبطاقات الذكية على سبيل المثال بطاقات الوقود وبطاقات الدفع العامة . كما يمكن استخدامها (كمحافظ الكترونية) او عندما يتم تحميل الشريحة بأموال لدفع ثمن المشتريات الصغيرة مثل محلات البقالة وخدمات كافتيريا الطعام والكافيهات وسيارات الاجرة .

2- الرعاية الصحية : مع زيادة سرعة بيانات الرعاية الصحية تساعد البطاقات الذكية في الحفاظ على كفاءة رعاية المرضى وضمانات الخصوصية تسمح البطاقات للمرافق الطبية بتخزين المعلومات بأمان من حيث التاريخ الطبي للمريض والوصول الفوري إلى المعلومات وتحديثها إذا لزم الامر والحد من الاحتيال في مجال الرعاية الصحية يوفر التحقق الفوري من المريض معالجة فورية بالأضافة إلى ذلك تمكن البطاقات الذكية من الامتثال للمبادرات الحكومية مثل برامج التبرع بالأعضاء .

3- التحقق من الهوية والتحكم في الوصول : يمكن ايضا استخدام البطاقات الذكية للتحقق من الهوية في اماكن مثل المكاتب التجارية والجامعات كما يمكن لبطاقات الهوية الذكية القائمة على المعالجات الدقيقة متعددة الوظائف دمج الهوية مع امتيازات الوصول . بالنسبة إلى الشركات ذات الاحتياجات الأمنية العالية يمكن ان تكون البطاقة الذكية جهازا مضاد للعبث والسرقة لتخزين المعلومات مثل صورة المستخدم او بصمات الاصابع وقد ادرجت جميع مرافق الحكومة الامريكية والعديد من الشركات قارئات لا تلامسا كنقطة وصول إلى منشأتها وتضمنت بعض العناصر مكونا للقياسات الحيوية .

4- الاتصالات المتنقلة : بالنسبة للهواتف المحمولة يمكن ايضا استخدام البطاقات الذكية كأجهزة تحديد الهوية تعرف هذه البطاقات باسم بطاقات هوية المشترك (SIM) . تحتوي كل بطاقة SIM على معرف فريد يدير حقوق وامتيازات كل مشترك ويجعل من السهل تحديدها وفرضها بشكل صحيح .

5- الكمبيوتر وأمن الشبكات : بدأت Microsoft Windows الإصدارات الجديدة من Linux و sun Microsystems باستخدام البطاقات الذكية كبديل لأسماء المستخدمين وكلمات المرور .

من المفهوم ان امان البنية الاساسية للمفتاح العام (PKI) مطلوب تصبح شارة البطاقة الذكية هي المعيار الجديد باستخدام البطاقات الذكية يمكن مصادقة المستخدمين وتفويضهم بالوصول إلى معلومات محددة بناءا على امتيازات سابقة الإعداد .

سابعا : المشاكل السائدة التي تواجه البطاقة الذكية :

- لا يتوافق chrome مع الشهادة المتوفرة على البطاقة : هناك مشكلة على الأرجح في ضبط شهادات الجذر والشهادات المتوسطة . يرجى التأكد من اتباع التعليمات لضبطها بشكل صحيح وفي حال استمرار حدوث هذه المشكلة قد يكون من الافضل تقديم تقرير خطا يحتوي على مزيد من المعلومات .
- يبقى chrome الاتصال مفتوحا بعد إزالة البطاقة : إذا ازال احد المستخدمين بطاقته لن ينهي chrome الجلسة مع ذلك الخادم يتم تنفيذ هذه الاجزاء على النحو المنشود (وهو السلوك التلقائي على chrome على الانظمة الاساسية الاخرى ايضا) لن يحاول chrome المصادقة مرة اخرى إلا عندما يطلب الخادم ذلك وهذا إعداد أمان يحدده المشرف إذا كنت بصدد إجراء اختبار وبحاجة إلى فرض اعادة المصادقة مع الخادم حاول استخدام نافذه التصفح المتخفي التي لن تستخدم الجلسة السابقة ولن يتم الاحتفاظ بها في الطلبات اللاحقة .
- ما من ملاحظات على واجهة المستخدم بشأن رقم التعرف الشخصي غير الصحيح : إذا أدخل المستخدمون رقم تعريف شخصي غير صحيح لا يعرض تطبيق Drivelock أي ملاحظات مباشرة في مربع الحوار وعلى المستخدم الانتقال إلى الموقع الإلكتروني لكي يطلب منه إدخال رقم التعرف الشخصي مرة اخرى .
- لا تتم فلترت الشهادات المقدمة : يتم تقديم جميع الشهادات إلى النظام بصرف النظر عن نوعها على سبيل المثال يتم ايضا عرض شهادات توقيع البريد الالكتروني في مربع الحوار المنسدل يجب ان تكون على دراية بالشهادة المطلوبة لموقع ويب معين حتى تتمكن من اختيارها من القائمة المنسدلة قد يعني هذا تجربة اختيار الشهادة الاولى او الثانية او حتى الشهادة الثالثة المتطابقة ظاهريا من بطاقتك عند المصادقة على بعض مواقع الإلكترونية يظل النظام مستقرا اثناء إجراء المحاولات لذلك لن تحتاج إلى تنفيذ هذا الإجراء سوى مرة واحدة

(Rose& Hudgins 478: 477:2008)

المبحث الثالث

انواع الاحتيال في بطاقة الائتمان وارتفاع تكاليف الاحتيال واستثمارفي تقنية كشف الاحتيال ودور البطاقة الذكية في تقليل المخاطر

اولا : انواع الاحتيال في بطاقات الائتمان : يعرف الاحتيال في بطاقة الائتمان بأنه الاستخدام غير المصرح به لحساب بطاقة الائتمان للحصول على اموال او منتجات او خدمات للقيام بذلك يمكن لمرتكبي الجرائم عبر الانترنت سرقة معلومات حساب بطاقة الائتمان فعليا او الحصول عليها عبر اجهزة القشط الالكترونية او البرامج الضارة او حتى شراؤها على الانترنت المظلم .

وارتفع الاحتيال على بطاقات الائتمان بشكل كبير في السنوات الاخيرة ويكلف الآن المستهلكين والشركات مئات الملايين من الدولارات سنويا من بين 3.2 مليون حالة احتيال تم الابلاغ عنها في عام 2019 كانت سرقة الهوية هو الاحتيال الاكثر شيوعا حيث تمثل اكثر من 20 بالمائة وفقا للجنة التجارة الفيدرالية الأمريكية . يعد الاحتيال على بطاقة الائتمان اكثر انواع سرقة الهوية شيوعا يمثل اكثر من 271000 تقرير من المستهلكين الذين سرقت معلوماتهم للوصول إلى حساب موجود أو فتح حساب جديد . وقد ادت هذه الانشطة الاحتيالية إلى خسائر فاقت 135 مليون دولار امريكي .

ثانيا : ارتفاع تكاليف الاحتيال في بطاقات الائتمان : في حين ان الاحتيال على بطاقات الائتمان يمثل مشكلة متزايدة للمستهلكين وشركات البطاقات فإنه يؤثر ايضا سلبا على تجار التجزئة من خلال ما يلي :

- رسوم رد المبالغ المدفوعة .
- أضرار السمعة وفقدان ثقة المستهلك .
- احتمال إنهاء حساب التاجر بسبب ارتفاع معدلات رد المبالغ المدفوعة .

يكلف كل دولار من عمليات الاحتيال المرتكبة الآن لمتاجر التجزئة 3.36 USD ارتفاع من 3.13 USD في عام 2019 في حين ان الاحتيال على بطاقات الائتمان اخذ في الارتفاع لجميع تجار التجزئة فان اكبر عدد من الهجمات يحدث للمؤسسات المتوسطة والكبيرة التي شهدت زيادة تقارب 50 بالمائة منذ 2019 .

رسوم رد المبالغ المدفوعة التي يكون جزء كبير منها مدفوعا بالاحتيال " الودي " و "البطاقة غير موجودة " تكلف الآن ما بين 15 USD و 100 USD لكل حالة تكلف عمليات رد المبالغ المدفوعة تجار التجزئة عبر الانترنت 40 مليار USD سنويا وفقا ل 911 chargebacks .

1- يتم استخدام خمسة انواع من الاحتيال على بطاقات الائتمان لاستهداف تجار التجزئة بغض النظر عن كيفية حصول المجرمين على معلومات الحساب فإن جميع عمليات الاحتيال في بطاقات

الائتمان تؤثر في النهاية على تجار التجزئة على الانترنت لان هذا هو المكان الذي يتم فيه إجراء عمليات الشراء عادة تشمل اكثر انواع الاحتيال على بطاقات الائتمان شيوعا مايلي :

أ- احتيال التطبيق : تحدث هذه الطريقة الشائعة عندما يتمكن احد المجرمين من الوصول إلى المعلومات الشخصية لشخص ما ثم يفتح حساب بطاقة ائتمان جديدة باسمه .

ب-احتيال البطاقة غير موجودة (CNP) : هذا امر مقلق بشكل خاص لتجارة التجزئة عبر الانترنت يحدث ذلك عندما يحصل المجرم على رقم حساب وتاريخ انتهاء الصلاحية ورمز التحقق ثم يستخدمهم في إصدار أوامر احتيالية عادة عبر مواقع ويب او عبر الهاتف . يتم الحصول على هذه المعلومات عادة عبر الانترنت المظلم او عن طريق الوصول الفعلي إلى البطاقة .

ت-احتيال الهوية المفرض : يحدث هذا عندما يستخدم المحتال عنوانا مؤقتا ومعلومات خاطئة للحصول على بطاقة ائتمان جديدة ثم يقوم بعمليات شراء بها قبل ان تكتشف شركة البطاقة او ضحية المستهلك في حين ان البنوك عادة ما يكون لديها انظمة لمنع حدوث ذلك إلا ان بعض عمليات الاحتيال لا تزال تسقط من خلال الثغرات .

ث-احتيال الاستيلاء على الحساب (ATO) : أكثر انواع الاحتيال شيوعا لبطاقات الائتمان تحدث هجمات ATO عندما يتمكن مجرم من الوصول إلى حساب المستهلك ثم الاستيلاء عليه ، من هناك ينتحل المجرم صفة الضحية ويغير العنوان البريدي ويطلب بطاقة بديلة .

ج- الاحتيال الودي : مشكلة متزايدة لتجار التجزئة عبر الانترنت يحدث هذا عندما يشتري المستهلك سلعا او خدمات ثم يطلب استرداد الاموال من شركة بطاقة الائتمان عادة اثناء الادعاء بأنهم لم يصدروا الطلب او يستلمو السلعة .

ثالثا : الاستثمار في تقنية كشف الاحتيال في بطاقات الائتمان : يمكنك منع السرقة وردعها قبل حدوثها من خلال اعتماد استراتيجية منع الاحتيال التي تراقب نشاط المعاملات بشكل استباقي في الوقت الفعلي يساعد الاستثمار في تكنولوجيا إدارة الاحتيال على بطاقات الائتمان اعمال البيع بالتجزئة عبر الانترنت على تخفيف المخاطر وتقليل تكلفة الاحتيال وحماية سمعة علامتك التجارية . وفقا لتقرير الهوية العالمية والاحتيال لعام 2020 الصادر عن Experian يقول ما يقرب من 90 بالمائة من العملاء ان تصورهم للعمل يتحسن عندما تقوم الشركة باستثمار لتحسين تجربة العملاء والتي تشمل الامان . يمكن ان تساعد العديد من التقنيات الجديدة تجار التجزئة عبر الانترنت في تحديد نقاط ضعفهم والتخفيف من مخاطر الاحتيال على بطاقات الائتمان يستخدم الكثيرون الآن تخزين البيانات الآمن وتشفير البيانات للتأكد ان المعلومات التي يجمعونها امنة ايضا يمكن لادوات إثراء البيانات تجميع نقاط البيانات لمراقبة المعاملات المشبوهة .

ar- sa.https://dynamics.microsoft.com

رابعا : دور البطاقة الذكية في تقليل المخاطر :

لوحظ بأن نسبة الخطأ للشريط المغناطيسي لبطاقات القيمة المخزنة التي يتم تمريرها على قارئ البطاقات تصل إلى 250 خطأ لكل مليون معاملة (اثناء تمرير كل معاملة تصل نسبة الخطأ) في حين ان نسبة الخطأ الذي يحصل نتيجة استخدام البطاقة الذكية تصل إلى 100 خطأ لكل مليون معاملة . (Jones : 2010)

من المتوقع ان التطورات المستمرة في تقنية المعالجات في المستقبل القريب ستخفض قيمة نسبة الخطأ بصورة مستمرة لان المعالجات الموجودة في البطاقة الذكية تستطيع ان تتأكد من سلامة كل معاملة من الخداع وعندما يقدم حامل البطاقة الذكية البطاقة إلى البائع فان المعالج الدقيق الموجود في مسجل النقد الالكتروني للبائع يتأكد من وجود البطاقة الذكية من خلال قراءة التوقيع الرقمي المخزون في معالج البطاقة ويتم تكوين هذا التوقيع الرقمي من خلال برنامج يسمى بالخوارزمية الشفرية . وهي عبارة عن برنامج آمن يتم تخزينه في معالج البطاقة يؤكد هذا البرنامج لمسجل النقد الالكتروني بان البطاقة الذكية اصلية ولم يتم العبث بها او تحويرها لذلك فان صاحب البطاقة في نظام البطاقات الذكية المفتوح لتحويل الاموال الكترونيا لا يحتاج ان يثبت هويته من اجل البيع والشراء . وكون البطاقة الذكية بلاستيكية فان استخدامها كبطاقة تعريف بالشخص هو اول ما يمكن تطبيقه عليها وذلك من خلال طباعة البيانات الشخصية على البطاقة وفي نفس الوقت تطبع داخل الشريحة ان حماية البيانات تكون من خلال الرقم السري لحامل البطاقة او من خلال استخدام الأنماط الحيوية مثل البصمة بحيث لا يمكن الوصول إلى المعلومات المكتوبة عليها إلا من خلال مطابقة البصمة مع البصمة المخزنة في الشريحة فخاصية حفظ البيانات ظاهرة ومخفية بهذا الشكل تحد من عمليات التزوير فلو تمكن شخص من تعديل بيان من البيانات الظاهرة على البطاقة فلا يتمكن من تعديل نفس البيان المخزون في الشريحة كما ان وجود رقم خاص لكل بطاقة يميزها عن غيرها يحميها من العبث والتلاعب . بالاضافة الى الذكاء المميز لرقاقة الدارة المتكاملة الموجودة في الشريحة يسمح بحماية المعلومات التي تم تخزينها من الضرر او السرقة ولهذا السبب فان البطاقات الذكية الاحدث هي اكثر امانا من البطاقات ذات الشريط المغناطيسي التي تحمل المعلومات على السطح وبالتالي فمن السهل نسخ هذه المعلومات او محوها . ان هذه البطاقة تؤهل العملاء للقيام بالدفع دون ان يتطلب الاتصال بين التجار وشبكة معلومات بطاقة الائتمان المركزية مما يعني توفير للتكاليف العالية والجهد بالاضافة الى ان للرقاقة المدمجة في البطاقة امكانية معالجة البيانات المدخلة بسرعة فائقة مما يجعلها الاكثر سرعة في تنفيذ عمليات الدفع الالكترونية المنتشرة في الوقت الحاضر ، وتمثل البطاقة الذكية افضل حماية ضد اساءة الاستخدام التي قد يمارسها البعض من السراق والمحتالين وذلك للدور الاساسي والرئيسي للعامل التقني الذي يلعب دور تقليل سوء

الاستخدام لتلك البطاقة من خلال وجود برنامج يطلق عليه ارستون الذي فيه قواعد اساسية ومعايير معرفة في البرامجيات . (الشيخ ، 2003 : 135) (komer : 2006)

عندما تدخل المعلومات في الجهاز مطابقة لتلك المعايير فهي مقبولة لانه يتفحصها بشكل جيد واذا ما كانت غير مطابقة فيرفضها .

ان بطاقة الائتمان العادية مثلا تظهر بوضوح رقم حساب مالكها على وجه البطاقة ، رقم البطاقة مع التوقيع مزور يمكن لأي سارق ان يستخدمها ويشتري بها ولكن بالبطاقة الذكية غير ممكن سرقة الائتمان عمليا لان المعلومات مشفرة وهي داخل الشريحة الالكترونية يكون الرقم سري ، مفاتيح عامة وخاصة (خوارزميات تشفير معقدة) وليس رقم خارجي يتمكن السارق من التعرف عليه بالاضافة إلى عدم وجود توقيع مادي يمكن ان يزوره لهذا فهي توفر أعلى درجات الحماية ولا يمكن نسخها او تزويرها ويمكن حمايتها من الاحتيال وسوء الاستخدام .

(Burns : 2010) (الحسيني ، الدوري : 2008 :41)

المبحث الرابع الجانب التطبيقي

من اجل تحقيق اهداف البحث واختبار الفرضية تم اعتماد اسلوب الاستقصاء للحصول على البيانات من خلال استمارة الاستبيان المتضمنة المحور المتعلق بالظاهرة المدروسة وتم الاعتماد على بعض المقاييس والمؤشرات الاحصائية كاختبار الفا كرونباخ , والوسط الحسابي والانحراف المعياري , النسب المئوية ,تضمنت استمارة الاستبيان من (20) فقرة موزعة على محور متغير يؤدي نظام مراقبة البطاقة الذكية إلى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا وقد تم تصميم الاجابات على كل فقرة وفق مقياس ليكرت الخماسي

أولا : مقياس صدق ثبات أداة البحث :

قامت الباحثة باختبار صدق استمارة الاستبانة لغرض التأكد من مدى مطابقتها وصلاحيتها والاعتماد على بيانتاها لغرض اجراء عملية التحليل الاحصائي لها , وتم اجراء اختبار (Cronbach, Alpha) والذي يهدف الى قياس ثبات التقديرات التي نحصل عليها من الاستبانات او محاورها والتي تقيس موضوعا يفترض تجانس مفرداته, حيث تم اجراء اختبار الثبات على معلومات عينة الدراسة وتم الحصول على نسبة مقبولة وعالية جدا , ويمكن توضيح ذلك على وفق الجدول الاتي :

جدول رقم (1) **اختبار صدق ثبات اسئلة الاستبانة**

Reliability Statistics

Cronbach's Alpha	N of Items
.940	20

اتضح من نتائج الجدول اعلاه بأن قيمة اختبار الثبات والمتعلق بأسئلة المحاور الاستبيان ,وفقا لمقياس (الفا لكرو نباخ) , بلغت نسبة الثبات او المصداقية (94%) بدون استبعاد اي فقرة وهي نسبة عالية جدا ومنطقية جدا .

ثانياً – تحليل عينة البحث :

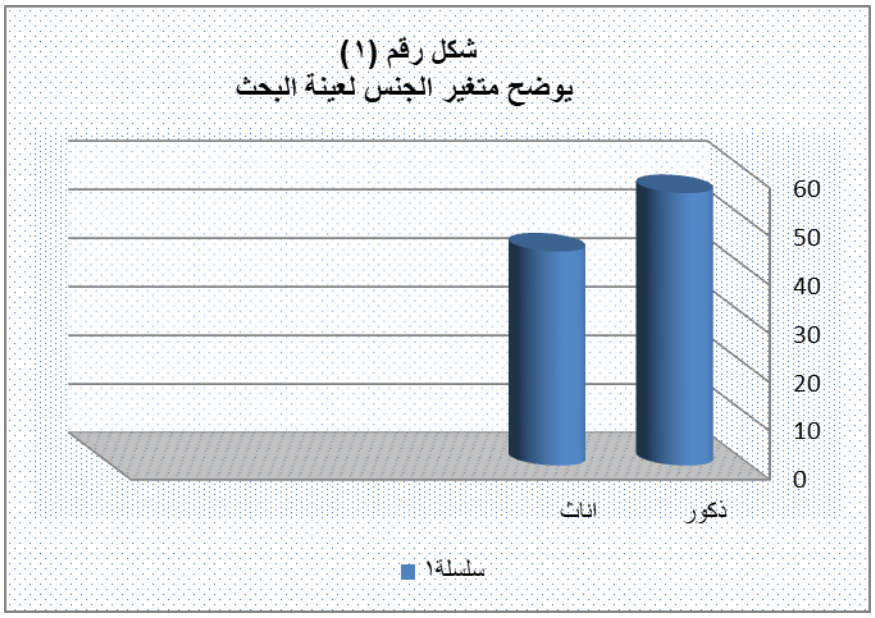
نرفق بعض الجداول والمعلومات المتعلقة بالأفراد المبحوثين وفقاً للمعلومات التي تم الحصول عليها من الاستمارات والمتضمنة اجابات الاشخاص المستجيبين وكما يأتي

اولاً– متغير الجنس :

جدول رقم (2) يوضح اجناس اشخاص عينة البحث

الجنس	التكرار	النسبة المئوية
الذكور	28	0.56
الاناث	22	0.44
Total	**50**	**100%**

تشير نتائج التحليل الاحصائي للجدول اعلاه, الى ان توزيع افراد عينة الدراسة حسب متغير الجنس , حيث بلفت نسبة الاشخاص المستجيبين من الذكور (**56%**) من اجمالي عينة الدراسة , بينما بلغت نسبة الاناث ب(**44%**) من اجمالي العينة المدروسة , ويمكن توضيح هذه النسب وفقاً للشكل البياني الاتي , والمتمثل بالشكل رقم (1).



المصدر من اعداد الباحثة بالاعتماد على مخرجات الحاسبة

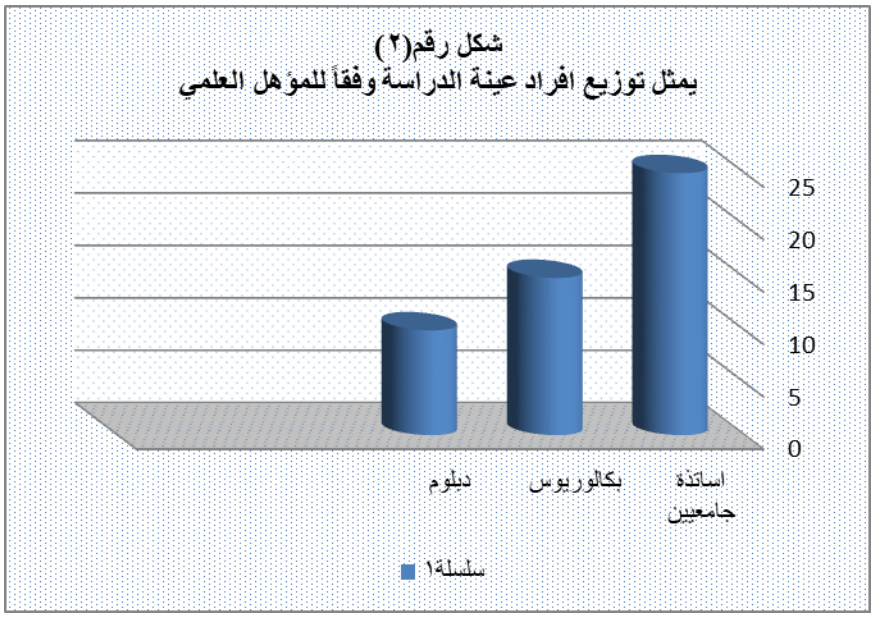
ثالثا – المؤهل العلمي للمستجيبين :

جدول رقم (3)

يمثل توزيع افراد عينة الدراسة وفقاً للمؤهل العلمي

المؤهل العلمي	اساتذة جامعيين	بكالوريوس	دبلوم	المجموع
التكرار	25	15	10	50
النسبة المئوية	%50	%30	%20	%100

تشير نتائج الجدول رقم (3) , الى أن توزيع أفراد عينة الدراسة وفقاً للمؤهل العلمي, اذ بلغت نسبة الافراد المستجيبين من فئة الاساتذة الجامعيين قد شكل ما نسبته (50) % من أجمالي عينة الدراسة , بينما بلغت نسبة الافراد المستجيبين من حملت البكالوريوس قد شكل ما نسبته (30) % من أجمالي عينة الدراسة اما حملت شهادة الدبلوم قد شكل ما نسبته(20%) . ويمكن توصيف بيانات عينة الدراسة وفقاً للتحصيل الدراسي من خلال الشكل البياني التالي :



المصدر من اعداد الباحثة بالاعتماد على مخرجات الحاسبة

رابعا – تحليل اجابات العينة على محور متغير دراسة سلبيات وايجابيات البطاقة الذكية

جدول رقم (4) :

ت	مضمون الفقرة	متوسط الاتجاه	الانحراف المعياري	معامل الاختلاف	الاهمية النسبية	الرتبة	اتجاه الفقرة
1	تحقق البطاقة الذكية مزايا اجتماعية للأفراد لاستخدامها في معظم انحاء العالم للشراء والسحب النقدي بكل سهولة .	4.52	0.677	%14.97	%96	4	اتفق
2	تستخدم البطاقة الذكية كضمان في حالة الشراء بالتقسيط	3.68	0.891	%24.21	%48	16	محايد
3	تقدم البطاقة الذكية فوائد	4.52	0.580	%12.83	%96	3	اتفق

	اقتصادية من خلال تواجد مكاتب الاستلام في المنطقة القريبة من سكناهم .						
4	البطاقة الذكية عرضة للاحتيال والسرقة عند استخدامها للتسوق عبر الانترنيت .	2.96	0.880	%29.72	%20	20	لا اتفق
5	البطاقة الذكية تحقق توفير اجور النقل والتكاليف الاخرى عند استلام الرواتب .	4.16	0.792	%19.03	%76	9	اتفق
6	البطاقة الذكية مفيدة للفرد وتوفر له الجهد والوقت عند استلام الرواتب .	4.45	0.679	%15.25	%76	8	اتفق
7	مكاتب البطاقة الذكية متوفرة وقريبة في مناطق سكناهم .	4.00	0.808	%20.2	%76	10	اتفق
8	تطور تكنولوجيا المعلومات ادى الى ظهور البطاقة الذكية .	4.64	0.485	%10.45	%96	2	اتفق
9	لا تعتبر البطاقة هوية تعريفية لحاملها لا مكانية استخدامها من قبل شخص اخر لديه الرقم السري .	5.00	0.100	%2.2	%96	1	اتفق بشدة

10	لا يمكن استخدام البطاقة الذكية من قبل شخص اخر اذا كانت تعمل ببصمة الاصبع .	4.44	0.760	%17.11	%84	6	اتفق
11	هل يجوز عمل بطاقة ماستر كارد باسم شخص ساكن خارج العراق ليستلم راتبه .	3.24	0.716	%22.09	%32	18	محايد
12	البطاقة الذكية امنة الاستخدام .	3.72	0.882	%23.70	%60	11	اتفق
13	عند استخدام البطاقة الذكية ماستر كارد اذا لم تعمل يجب الاتصال بالبنك .	4.12	0.659	%15.99	%84	5	اتفق
14	الانظمة البنكية متطورة وتستطيع اخبار المواطنين بالمشكلة .	3.94	0.978	%24.82	%68	14	اتفق
15	يستخدم المواطن البطاقة الذكية في مصارف مختلفة .	4.22	0.790	%18.72	%36	17	اتفق
16	تقلل البطاقة الذكية من عمليات السرقة	3.94	0.913	%23.17	%68	13	اتفق
17	لا تكشف البطاقة الذكية عن هوية الشخص الحقيقية الا اذا كانت تعمل ببصمة الاصبع	4.16	0.976	%23.46	%84	7	اتفق
18	تكشف البطاقة الذكية عن	3.16	0.738	%23.35	%24	19	محايد

	وجود افراد بشكل غير قانوني						
19	**لا يمكن استخدام البطاقة الذكية اذا كانت بالبصمة من قبل اشخاص مخولين .**	**3.84**	**0.976**	**%25.41**	**%44**	**15**	**اتفق**
20	**يمكن استخدام البطاقة الذكية ماستر كارد من اشخاص مخولين .**	**3.88**	**1.003**	**%25.85**	**%64**	**12**	**اتفق**

كشفت نتائج التحليل الاحصائي اجابات افراد العينة من خلال استخدام متوسط الاتجاه وبالاعتماد على معادلة كوبر, وكما موضح في الجدول رقم (4) بأن الفقرة التاسعة والمتمثلة " **لا تعتبر البطاقة هوية تعريفية لحاملها لا مكانية استخدامها من قبل شخص اخر لديه الرقم السري** . " والفقرة الثامنة والمتمثلة " **تطور تكنولوجيا المعلومات ادى الى ظهور البطاقة الذكية** " والفقرة الثالثة" **تقدم البطاقة الذكية فوائد اقتصادية من خلال تواجد مكاتب الاستلام في المنطقة القريبة من سكناهم** ,هي على التوالي (5.00 , 4.64 , 4.52) وبانحراف معياري (**0.100 , 0.485 , 0.580**) على التوالي وهذه المتغيرات تمثل اتجاها ايجابيا عاليا وهي تمثل الاكثر اهمية في التأثير على تحديد مستوى ادراك مؤسسات عينة البحث بأهمية هذا المتغير. وقد جاءت الفقرة الرابعة والمتمثلة " **البطاقة الذكية عرضة للاحتيال والسرقة عند استخدامها للتسوق عبر الانترنيت** " في المرتبة العشرين والاخيرة وهي ايضا تعكس اتجاهاً سلبيا في تحديد مستوى بطاقة الدفع الاليكترونية من وجه نظر الاشخاص المستجيبين من افراد العينة .

خامسا – اختبار فرضيات البحث

ينطلق البحث من فرضية اساسية مفادها " يؤدي نظام المراقبة للبطاقة الذكية إلى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا .

وبتالي يمكن صياغة فرضيات البحث على النحو الاتي :

الفرضية الاولى :

H_0 : لا توجد فروقات ذات دلالة احصائية في اراء عينة الدراسة (يؤدي نظام المراقبة للبطاقة الذكية إلى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا .

H_1: توجد فروقات ذات دلالة احصائية في اراء عينة الدراسة (يؤدي نظام المراقبة للبطاقة الذكية إلى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا .

ولتأكد من صحة هذه الفرضية سيتم اجراء بعض الاختبارات الاحصائية منها اختبار (F) من خلال الاعتماد على جدول تحليل التباين (ANOVA) وكما يأتي :

جدول رقم (5)

نتائج اختبار قيمة (F) لدلالة الفروق بين المستجيبين حول الفرضية التي تنص على (يؤدي نظام المراقبة للبطاقة الذكية إلى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا).

وفقاً لمتغير الجنس للمستجيبين .

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط مربعات الخطأ	قيمة F	P_{Value}	الدلالة الإحصائية
بين المجموعات	19.956	1	19.956	114.532	0.000	معنوي ذات دلالة
داخل المجموعات	8.364	48	0.174			
المجموع	28.320	49				

اتضح من خلال الجدول رقم (5) أعلاه , وجود فروق معنوية ذات دلالة إحصائية بين متوسط استجابات المبحوثين الخاصة بتحقيق هذا الافتراض, حيث بلغت قيمة (F) المحسوبة بـ (114.532) وهي اكبر من قيمة الجدولية , اضافة الى قيمة (P_{Value}) والبالغة (0.000) اقل من مستوى المعنوية (0.05) وعند ذلك نرفض فرضية العدم (H_0) القائلة بأنه لا توجد فروق معنوية ذات دلالة إحصائية , ونقبل بالفرضية البديلة (H_1) .

جدول رقم (6)

نتائج اختبار (t) لدلالة الفروق بين المستجيبين حول الفرضية التي تنص على (يؤدي نظام المراقبة البطاقة الذكية إلى تقليل الاحتيال والسيطرة عليه وتسهيلها للمواطن اقتصاديا واجتماعيا).وفقاً لنوع الجنس .

المجموعات	التكرار	قيمة t	P_{Value}	Chi - Square	P_{Value}	R^2	الدلالة

الذكور	28	20.307	0.000	42.424	0.000	0.89	الاحصائية
الاناث	22					معنوي	

كشفت نتائج التحليل الاحصائي في الجدول أعلاه , الى وجود فروق معنوية ذات دلالة إحصائية الخاصة بتحقيق هذا الافتراض, حيث بلغت قيمة اختبار(t) المحسوبة بـ (20.307) وهي اكبر من القيمة الجدولية , وايضا قيمة (P_{Value}) اقل من مستوى معنوية (0.05), بينما بلغت قيمة اختبار احصاءه مربع كاي والبالغة (42.424) فضلاً عن قيمة القوة التفسيرية للنموذج والبالغة (0.89) , وبتالي قرارنا سيكون رفض فرضية العدم (H_0) القائلة بأنه لا توجد فروق معنوية ذات دلالة إحصائية بين متوسطات الاستجابة على هذه الفقرة ونقبل الفرضية البديلة (H_1) .

المبحث الخامس

الاستنتاجات والتوصيات

اولا : الاستنتاجات

1- ان تطور تكنولوجيا المعلومات أدى الى ظهور البطاقة الذكية .
2- تقدم البطاقة الذكية فوائد اقتصادية من خلال تواجد مكاتب الاستلام في المنطقة القريبة من سكناهم .
3- تحقق البطاقة الذكية مزايا اجتماعية للأفراد لاستخدامها في معظم انحاء العالم للشراء والسحب النقدي بكل سهولة .
4- ان بطاقة الذاكرة المباشرة تخزن البيانات ولا تمتلك معالجة البيانات وهي اقل تكلفة وتعتبر بمثابة أقراص مرنة بأحجام مختلفة مع إمكانية الغلق .
5- ان حماية البيانات تكون من خلال الرقم السري لحامل البطاقة أو من خلال استخدام الأنماط لحيوية مثل البصمة بحيث لا يمكن الوصول الى المعلومات المكتوبة عليها الا من خلال مطابقة البصمة مع البصمة المخزونة في الشريحة فهذه تحد من عملية التزوير .
6- ان البطاقة المخزونة بمعالجات دقيقة تحتوي على رقائق تحكم دقيقة تحمل قيمة مالية وتحمي التلفونات المحمولة من الغش والاحتيال.

7- توجد استخدامات أخرى مالية للبطاقة الذكية مثل بطاقات الوقود وبطاقات الدفع العامة مثل ثمن المشتريات أو خدمات كافتيريا الطعام وسيارات الأجرة
8- يمكن استخدام البطاقة الذكية كوسيلة للدفع بدلا من الصكوك والمبالغ النقدية.
9- ان البطاقة لا تعتبر هوية لحاملها لامكانية استخدامها من قبل شخص اخر لديه الرقم السري .

ثانيا : التوصيات

1- نوصي بعمل ماستركارد لاشخاص موجودين خارج العراق ليتسلم راتبه
2- نوصي بكشف اشخاص موجودين بشكل غير قانوني
3- نوصي ان البطاقة الذكية لا تكون عرضة للاحتيال والسرقة عند استخدامها للتسوق عبر الانترنيت .
4- اصدار تشريعات بضرورة حمل البطاقة الذكية في التعاملات المصرفية بدلا من الوسائل التقليدية للحد من تلك الوسائل .
5- يمكنك منع السرقة وردعها قبل حدوثها من خلال اعتماد استراتيجية منع الاحتيال التي تراقب نشاط المعاملات بشكل استباقي في الوقت الفعلي .

المصادر :

المصادر العربية والاجنبية:

1- ابراهيم ، نادر شعبان ،2006 ، النقود البلاستيكية ، الدار الجامعة ، جمهورية مصر العربية .
2- عوض ، علي جمال الدين ، 1988 ، عمليات البنوك من الوجهة القانونية ، دار النهضة العربية ، القاهرة .
3- الشيخ ، بابكر ،2003 ، غسيل الاموال ، اليات المجتمع في التصدي لظاهرة غسيل الاموال ، دار مكتبة الحامد للنشر والتوزيع ، عمان
4- الحسيني ، فلاح حسن ، الدوري ، مؤيد عبد الرحمن ، 2008 ، ادارة البنوك / مدخل كمي واستراتيجي معاصر ، ط4 ، دار وائل للنشر عمان
5- Rose ,peter S.& Hudgins,Sylvia , 2008 , (Bank Management & Financial Services) McGraw – Hill Irwin Irwin Inc. 7ed U.S.A

مصادر الانترنت :

1- Brain Komer (planning your smart card deployment: the importance of policy and process) 2006 http://technet.microsoft.com/en-us/library/cc512006.aspx.

2- Neil Jones(protect yourself with smart card technology) 2010 http://www.buzzle.com/articles/protect-yourself-with-smart-card-technology.htm.

3- Sheila Robinson (Types of smart cards) 2010 http ://WWW.brighthub.com/computing/smb-security/articles/64180.aspx.

4- John meckley (smart cards) 2001 http://search security.techtarget.com/sDefinition/O,sid14-gc1213004,00 .htm.

5- Glenn pittaway (smart cards concepts) 2001 http://technet.microsoft.com/en-us/library/dd277376.aspx.

6- Sheila Robinson (Types of smart cards) 2010 http:// www.brighthub.com/computing/smb-security/articles/ 64180.aspx.

7- Steve petin (introduction to smart cards) 1999 http://www.opengroup.org/comm/the message/magazin/mmv5n5/smart cards, htm.

8- Tolga Kilili (smart card How to) 2001 http://www.fags.org/docs/linux- how To/smart-card-how To.htm.

9- Manali oak (Benefits of smart cards) 2010 http://www.buzzle.com/articles/benefits-of-smart-cards.htm.

10- Anjus chiedozie (History of smart cards) 1999 http://www.ehow.com/about-5468406-history-smart cards, htm.

11- Glenn pittaway (smart cards concepts) 2001 http://technet.microsoft.com/en-us/library/dd277376.aspx.

Sa.https://dynamic