

A Novel Multiple Session Payment System

Mohanad Faeq Ali, Nur Azman Abu, Norharyati Harum
Faculty of Information Communication Technology,
Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, Durian Tunggal, Melaka, MALAYSIA

Abstract—A wireless smartphone can be designed to process a financial payment efficiently. A user can just swipe his/her credit/debit card over the counter and all the processing needed shall be done seamlessly. A smartphone is a popular device to carry around. It is a hassle to carry and keep track on so many physical debit/credit cards in a wallet. An electronic debit/credit card on a smartphone is a more convenient alternative. This research project will embark on an electronic debit/credit card on a smartphone and migrate to an IoT money. A novel session payment system using IoT money has been introduced to minimise debit/credit card risk. The scope of this paper is confined to the security model for an easy payment system based on Internet of Things (IoT). Previously, each IoT money is unique and used once only on one-time payment. The session payment system will ease the burden on protecting the database of the payment system. This paper will extend the use of one-time payment to a multiple session payment system using an IoT money note.

Keywords—Easy payment system; internet of things; secure payment system

I. INTRODUCTION

Internet of things (IoT) defined as uniquely recognizable object or thing with virtual presentations through internet-like structure. IoT initially proposed in year 1998 [1]. In previous year, concept of IoT became famous through several applications for example smart electrical reading meter, greenhouse condition monitoring, telemedicine communication monitoring, and intelligence transportation. IoT consist of four major components. Components of IoT are for sensing, heterogeneous access, process information, service and applications. An extra component is also needed to cater for security and privacy. Recently, IoT has penetrated subsequent industry applications. IoT helped in terms of cyber-transportation systems (CTS), cyber-physical systems (CPS) and machine-to-machine (M2M) communications [2] [3]. In terms of security and privacy, IoT will encounter severe challenges. The challenges experience from security and privacy because IoT establish the networking with the help of traditional internet connection, mobile data and sensor from network. Next reason of facing security problem because of all 'things' is connected through mobile infrastructure. Lastly, reason facing security problem because of mobile device spreads and communicate faster between one and another. Eventually, latest security and privacy challenges will rise simultaneously at different places in the same time.

IoT technology is potent in the field of e-commerce. IoT has brought improvement in economic growth and provide a competitive element to e-commerce. Even though application

of IoT is relatively in early stages but this technology starts becoming established. In order to gain a significant the previous from IoT technology, the current development has moved on to mobile payment systems. A flexible one-time payment note system has been presented [4]. IoT technology application consists of three aspects, namely e-commerce database, payment and logistics. It is crucial to concentrates on the issues for e-commerce's security measures. This one-time note will save the need of protecting the database especially on the credit/debit card information. A more balanced approach shall be presented here for easy and friendly use of the IoT money. This paper will extend the use of one-time payment to a multiple session payment system using an IoT money note.

The IoT system will encompass on specific security issues in E-commerce business [5]. Issues rises from this research on authenticity, integrity and confidentiality from data obtained it IoT payment system should be given attention. Current phase, the autonomous control and ambient intelligence does not belong to original IoT concept. Through advance network technique development, cloud computing and distribution of multi – agent control, shift integration from IoT concept and autonomous control in M2M research exist. Autonomous controls in M2M research serve the purpose to create transformation of M2M in form of CPS. CPS focuses on better interactive application, interaction and real – time distribution in mobile control. Hence, new technology and method must be created to fulfil greater requirements in terms of privacy, reliability and security [6]. The rest of this paper shall be organized as follows. Section II will comes some key issues in cyber security and privacy. A review on online payment systems is given in Section III. Section IV will recapture a proposal on a session of IoT card which can be used once only. The one time card is extended to be on IoT note in Section V for multiple users.an evaluation set of criteria in proposed in Section VI the session IoT card and IoT note against used to evaluate monetary systems. Finally, this paper will give convulsive remarks in Section VII.

II. KEY ISSUES IN CYBER SECURITY AND PRIVACY

Internet has evolved from useful tool for research in universities into basic needs. Crime will always happen in the presence of valuable resource obtain through illicit usage of latest technology. The interrelated nature of internet is that resource from internet can be hacked from anywhere around the globe. Cyber security has the duty to overcome hacking issue. Cyber security circles around five keys namely confidentiality, cryptography, authentication, non – repudiation and access. Confidentiality means keep data

privately, so authorized users includes machines and human can access into data.

Authentication serves the purpose to verify either data have been tempered with so that data can be sent by authorised owner. Non-repudiation is a key to avoid denial from sender regarding shipment of purchase order from other user. Non - repudiation in some cases considered as unique key, however, in this paper, this key is included as one of cyber security key after authentication process. Access means provide entrance for authorized users to view and tempered with data, computing resources and communications infrastructure.

A survey of information security breaches conducted every year by UK Department for Business, Innovation and Skills with Price Water House Coopers. Result obtained shows increase from 81% in year 2016 to 90% in 2017 regarding the matter cyber breaches experience by big organization. Total of 74% experienced security breach among small sized organization. Forecast from this survey that there will be double – digit growth rate per year. Currently, internet is a need for modern business. Cyber security is a must organization to secure information systems. Nevertheless, as cyber security improved and overcome current issue of breaches, simultaneously, cybercrime transform to more extensive, destructive, sophisticated and comprehension activity.

III. AN ONLINE PAYMENT SYSTEM

The idea of online payment was coming from the previous payment process such as bank checks, travels checks and many orders. Nowadays, there are many online payments such as E-cash, E-purse internet payment system, E-checks, Amazon, ALIBABA and others. However, a typical online payment carries financial security. The previous network communication has been operating E-commerce prior to the arrival of internet of things (IoT) attending security problems such as privacy, identification, authentication, reification, certification, and personalisation. The previous research paper offers an extended design on the one-time payment system. Online payment is a transaction to purchase goods or service paid by human using Internet. Online payment results in lower costs in business because payments made electronically without using physical notes or postage. An online payment helps also to improve customer's retention because most likely customer would return to an e-commerce site where transaction's information already been input and kept [7]. In conjunction to an online payment, it is no longer relevant for customer to wait in queue just to make payment because everything is in the fingertip. This section shares various review on various online payments.

Credit Cards: Credit Card is a form of electronic money which can adapt and also used to perform online purchases. Though, people still disagree about simplicity of credit-card transactions because of security concerns, there are still risk where cards and money content were stolen, thus customers fear credit-card fraud from merchants or other parties [8]. Consequently, most of credit card issuers' strong security standards in order to provide fraud protection online.

Europay Mastercard Visa (EMV) is another secure international standard for purchase, fund withdrawal and for authenticating credit and debit card transactions [9]. Master card will manage to use EMV as standard security chip for online payment. At the same time, Visa, Discover, American Express and Europay will also join in and use EMV as global standards.

Virtual Credit Cards: Virtual credit card is an improvement from online credit cards. Virtual credit card is a recent idea provides unique number for users while using same current credit card number. This special number is used to make online transaction for purchases. This new feature allows users to use credit card for online purchase without releasing card number. Users now may give transaction number rather than credit card number to American Express or other merchandise which perform private payment [10].

Debit card: Debit card provides direct cash from personal account to purchase an item. The time duration for fund transfer between account holder and merchant may take 1 to 2 days [10]. The use Debit card is effective in decreasing credit card fraud which will get direct authorization from an account owner.

Smart cards: smart card physically resembles plastic payment card whereby microchip installed as a part on the surface of card. A smart card can carry more information rather than any credit cards that have magnetic strips. Also smart cards can carry another information such as identification, transportation, banking, health care, and others. In other hand A smart cards can also using for online payment but suppose to used reader to be able to read information of the cards for payment and the secure will be sending data throw internet [10].

E-Cheque: E-Cheque is actually an electronic version of cheque made from paper. E – Cheque contains the same copy of information as cheque made referring to legal framework. The procedure is the same as paper cheque but the advantage is more faster, cheaper and have high security [8]. To use e-cheque, account number is needed together with routing number generate from bank to be keyed in. Financial ponders allow permission to make payment via customer's bank, which either perform electronic funds transfer (EFT) or cheque printing.

Digital Cash: This cash is an example of digital currency. Digital cash allows users to shop online even though the users do not possess debit card. This digital cash procedure is the same as previous practice where people have to reload digital cash account by deposit money to purchase goods or service online. Digital cash is frequently link to another technology called digital wallets [8].

E-Wallets: Electronic wallet is software available in desktop. The users will have to download this software so that user may stores number of credit card and other user's information. If shop or restaurant accepts e-wallets, the owner of e-wallet will just click and all the formalities were filled up automatically. Currently credit card companies such as MasterCard and Visa offers e-wallet software application [10].

Peer-to-Peer Payments: P2P are type of payments which are growing rapidly because this payment allows two users to perform fund transfer among them [10].

Mobile Payments: Mentioned payments using wireless device such as smartphones supposed to make customer feel convenient, security of payment made electronic increase and transaction fee decrease [11], [12]. Mobile payment system gives ease to business personnel to gain information regarding the customers from the last purchased made. Mobile payment is highly suitable for mobile devices rather than other telecommunication medium due to amazing growth and big penetration to all brands of mobile devices [13], [14]. Mobile payment methods are suitable for offline micropayments as well as for online purchases. This method is a potential attraction for online traders due to an enormous user base of mobile phones. A mobile payment also offers better security and reduces the overall cost for all transactions being made [12]. Nevertheless, mobile payment came across several challenges to obtain significant customer base including inability to perform international transaction and issues related to privacy.

Mobile Wallets: A study regarding consumer usage of mobile wallet has been covered in [16]. A mobile wallet in a smartphone act as leather wallet equipped with digital cards, receipt, coupon and money. Mobile wallet is needed to be installed from online stores in smartphones for the purpose of making purchase either online or offline. Current technology connected the smartphones to QR codes, sound waves, and NFC (Near Field Communication) [15]. These waves and codes basically are solutions which are cloud-based. Mobile wallet is forecasted to give much more convenient payment environment for customers in near future [17].

Touch n Go: Touch 'n Go is a payment method by using an e-payment prepaid card [18]. This smartcard gives the users a fund anonymous account to make low value cashless payment in easy and comfortable way. Touch 'n Go is initially designed to pay the toll collection on selected Peninsular Malaysia's highways. Touch 'n GO is widely accepted for Common Ticketing Program (CTS) for general public transports located in Klang Region. Later, Contact 'n Go has been acceptable by car parking operators, in recreational areas and selected retail shops. Considering the convenience of customers, Touch n Go card can be reloaded at a selected of petrol stations, automated teller machines and Automated Reload Kiosks at train stations.

PayPal: PayPal belongs to one of the largest online payment processors worldwide. After growing and create partnerships with E-bay, a big number of online acceptance PayPal as one of accepted methods for payments.

Bitcoins and Other Cryptocurrencies: Bitcoin is a new online currency created by unknown person in the year 2009 [19]. Bitcoin is also known as cryptocurrency and digital payment system. This cryptocurrency is known recently created by Satoshi Nakamoto. The transaction used is between peer – to – peer whereby the users can perform transaction directly without intermediaries. This virtual currency has anonymity. Bitcoin is known as open – source software

starting year 2009. Bitcoin became important needs in marketing covers 90% among all transaction. After Bitcoin is launched, other competitor such as Ethereum, Filecoin, XRP, Gnosis tokens and Tezos emerge causes Bitcoin market share dip below 80% and dive straight until 50% left.

Samsung Pay: Recently, a new mobile payment app namely Samsung pay emerged. Samsung Pay is a wallet service provided by Samsung electronics that allows users to perform transaction with other Samsung devices. Samsung pay adapts new secure technology called Magnetic Secure Transmission which allows contactless payments. This contactless payment will be used on payment terminals which support magnetic stripe and normal contactless cards. Samsung Pay supports contactless payments using near-field communications such as NFC and MST. Samsung pay app is available on all Samsung devices, preinstalled or available for download as application update. Users must register to Samsung account with valid credit card. The procurer will verify users fingerprint to authorize any transaction made. Future transactions made will not be necessary to use credit card on any information from credit card. If merchant uses contactless NFC terminals, the user may touch mobile phones to NFC reader to perform transaction [20]. With this method, cashier may input payment details and users will swipe mobile phones at the card-swipe region on the card reader to perform transaction.

IV. A SESSION IOT CARD

A common online electronic payment system via debit/credit card payment system which is enables users to pay for purchases or services online. The system operates on three basic models namely; minimum security model, a third party broker model [21] with a simple encrypted payment system and security electronic transaction model such as SET [22]. Business personnel could misuse customer's information and make transactions, or owner can temper with the consumer's site. Information related to consumer can be stolen and misuse by other party. For example, a vendor can make a higher price quotation based on consumer's previous behaviour. Following are the risk rises based on customer's view:

- a) A consumer can evolve into a competitor who will adapt the prices and strategies learned.
- b) A customer could turn up and to be an imposter. They will not produce any bill payment.
- c) A consumer has the tendency to become a hacker so that the consumer able to: changing the order requested by customers; changing price; change on available goods; and illegally acquire contact information of customers.

Once a debit/credit card has been used in an online transaction, it becomes vulnerable to be used or abused for another transaction due to anonymity issue [23]. The transaction will be recorded and stored in a database. Since most of the databases are not securely encrypted, they are vulnerable to an open attack such as a ransomware. Other methods including the E-purse and E-check internet payment systems are also vulnerably subjected to the above problem.

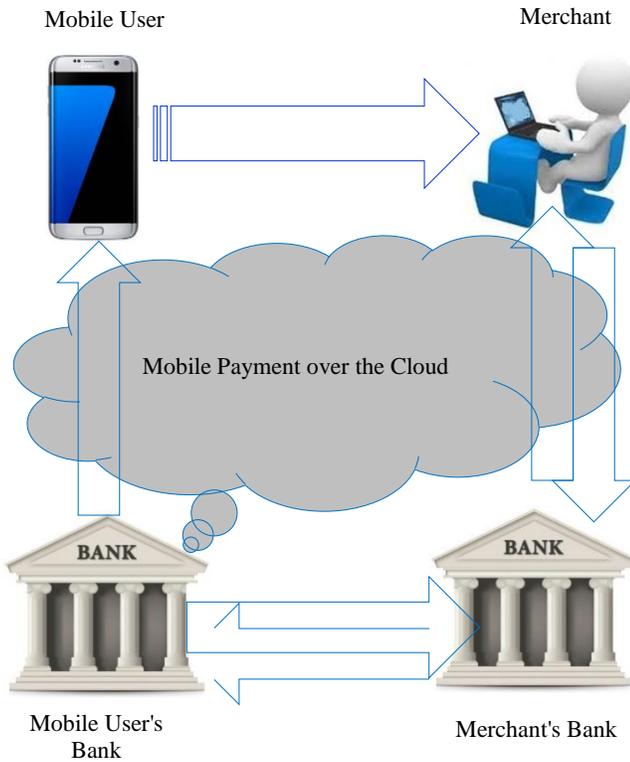


Fig. 1. Electronic cash payment process with E-cash.

A smartphone has become an essential part of life. It is not only an integral part of life but also a source of daily communication. An owner of the smartphone will carry and safeguard the security of the smartphone at any cost all the time. It is more personal to embed a debit/credit card electronically into a smartphone. This paper shall propose an electronic IoT note as part of a credit line a smartphone. A novel IoT payment system shall be introduced to minimise debit/credit card risk.

Fig. 1 illustrates the working of an IoT E-Commerce secure payment mode [24]. This new model will pay special attention to the new card session number. This IoT note will be dynamically changed and updated to the new number once the note is claimed from a user's bank or financial provider. Therefore, it will be a randomly unique number per note which is recognized by an IoT service provider. Each new session card number will also be individually digitally signed by the financial provider [25].

Once an IoT note from a user's smartphone is transferred to the merchant terminal, the payment system will first verify the digital signature of the session number. Once verified, the payment system will check all the transactions being carried out by this note until it is claimed to the merchant's bank. A threshold amount should be set on each IoT session card number. An encrypted update shall be prompted by the financial provider to deliver a new IoT note to the smartphone.

An e-commerce system can be viewed in three different dimensions. The dynamic control used for system upgrade, the real time detection, response and recovery and security coordination between various components.

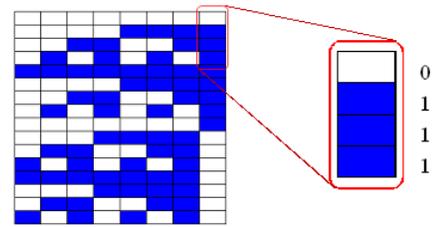


Fig. 2. The top right hand corner represents top right hand hexa value of $0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 7$ in Table I.

TABLE I. A SAMPLE OF AN IoT CARD NUMBER FOR 01 23 45 67 89 AB CD EF 12 34 56 78 9A BC DE F0 WRITTEN IN A STATE ARRAY OF HEXADECIMALS

01	23	45	67
89	AB	CD	EF
12	34	56	78
9A	BC	DE	F0

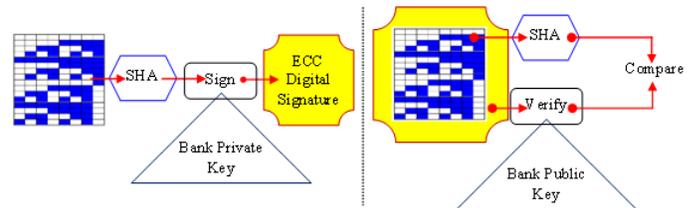


Fig. 3. The Session IoT card number will be signed by its financial provider.

A currently secure session number is 128-bit. It can be viewed as 16 bytes compared to the current 16 digit numbers on a debit credit card. This random Session IoT card number is proposed here as shown in Table I. A sample number is displayed as a state of byte array according the Advanced Encryption Standard (AES) written from left to right along each row of 4 bytes. A direct conversion of binary 2D barcode is generated and shown in Fig. 2. Each hexa has been converted to a column of 4-bit number. This basic 2D barcode can be set an efficient mode of transferring an electronic payment through a smartphone camera.

The research study has proposed new secure technique with a digital signature. Prior to issuing the Session IoT card number, the bank will hash and sign it. The digital signature will be wrapped around the Session IoT card number as shown on the right hand side of Fig. 3. The Session IoT card number will be accompanied by a digital signature. The digital signature must be signed using the private key of the issuing bank as the financial provider. An elliptic curve cryptosystem (ECC) will be light and compact [ECDSA]. A 256-bit ECC would be ideal here to accompany the 128-bit Session IoT card number. Meanwhile a merchant could validate digital signature from using the bank public key and compare to the hashed Session IoT card number.

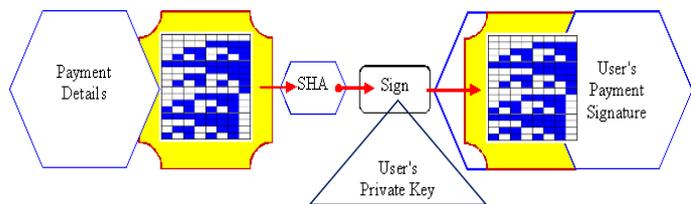


Fig. 4. An online payment on each transaction will be typically signed by the IoT session smart card owner.



Fig. 5. A nice sample of RM 100 note.

Each payment will also be signed digitally by the user as shown in Fig. 4. Practically, the digital signature will be exercised by a password keyed in by the user. It is imperative the password should not be stored in the smartphone. The password will be used to decrypt user's private key for signature signing. Since each IoT Session number will only carry certain amount, the user cannot spend more than the amount reserved on the number as if it is a currency note. For instances, a note could carry a value of 5, 10, 20, 50 and 100 Malaysian Ringgit. The barcode IoT Session number will also follow the traditional colour of the paper note, i.e. green, red, yellow, turquoise and purple, respectively.

The IoT note will also come along with the ECC digital signature as shown in Fig. 5. This note shall be honoured by the first merchant who claims its use once only. This note will also have a validity date on it as written on bottom left corner of the RM 100 in Fig. 5. Typically, it is valid for a month only. A larger value IoT note will have shorter validity period in order to minimise the risk exposure. The user will slide the note to the IoT payment application during a transaction.

The proposed model is based on a smartphone which becomes a mobile intelligent personal terminal for e-commerce businesses. Lightweight PC Tablet act as carrier embedded with RFID reader payment module instead of a physical debit/credit smart card. This mode of payment has the potential to be integrated into an online payment system. This payment application mode is secure and simple. An IoT PDA's payment resolved program which adapts that RFID reader module installed in a smartphone. This IoT program will make the user to avoid pay cumbersome online banking. There is portable handheld personal device and make the whole process completely contactless.

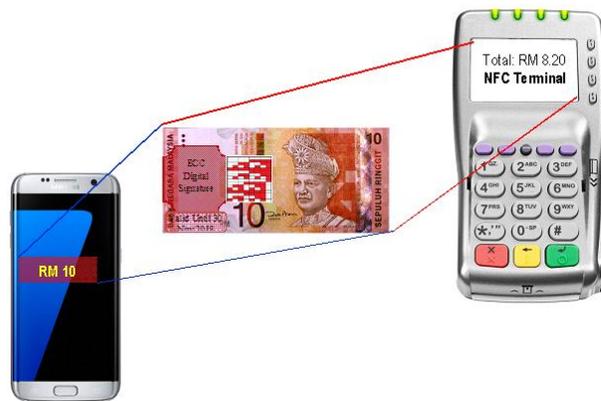


Fig. 6. A user will slide an RM 10 note from his pocket money to an NFC cashier terminal within his smartphone IoT application.

As visualized in Fig. 6, a user may use an RM 10 note from his pocket money to a cashier terminal within his smartphone IoT application to pay for a purchase less than RM 10 for example RM 8.20. The user will sign the transaction for RM 8.20. Thus, the merchant may claim only RM 8.20 from the RM 10 note he/she has received.

This electronic Session IoT card payment will also make use of an online payment tool, for example Alipay and Tenpay using latest IoT RFID contactless technology. In this case, an IoT payment is used during online shopping. A lightweight PC Tablet PC will act as carrier. A payment module installed in the RFID reader where secure and simple smart card payment method achieved by a friendly feature of sliding the note to a merchant iconic application. In IoT handheld payment, all funds were allocated by bank dedicated channel to avoid security risks through open internet. By using the AES algorithm, entire data are encrypted for card users and on data transmission from mobile devices to a clearing centre in order to guarantee maximum security during fund transfer. The bank will maintain a money database to detect double-spending and ensure the validity of this IoT note.



Fig. 7. Transfer money from user1 to user2.



Fig. 8. Transfer money from user2 to user3.



Fig. 9. Transfer money from user3 to merchant.

V. AN IOT NOTE

This paper will propose an easy flow IoT notes as new technique of payment. Traditionally, a user will use his/her debit/credit card to start use IoT session payment [4]. This paper will propose an extension to IoT payment notes to make it transferable between two users and more from one time IoT note. The first user can digitally sign one IoT note and give it to another registered user. The second user can further sign on same note to make a payment to the third or next registered user until the last his/her will give to a merchant to claim the money from the first user's bank account. However, the secure will use between first user to second user. After that second user to third user until the last his/her will give to a merchant base on ECC algorithm [26].

In the first case, the IoT notes in digitally signed by the IoT financial provider. Once the IoT note has been issued, the money is already taken out of the first owner account. When the first owner make a payment or pass the IoT note to a merchant or the new owner that shows in Fig. 7, the first owner will encrypt and digitally sign the IoT note to the new. The new owner can then check on the authentic of digital signature by the bank and first owner. The same process will be done by the second owner of the IoT note. When the second owner want to make a payment or transfer the IoT note to a merchant or the third owner that shows in Fig. 8, the second owner will encrypt and digitally sign the IoT note to the new owner. These IoT notes are expected to be in small dominance. The new third owner will check the bank digital signature, the first owner digital signature and the second owner digital signature following the block chain mode. The third user will signed the IoT notes to make transfer or payment to a merchant that shows in Fig. 9.

VI. EVALUATION CRITERIA OF MONEY

This research project will evaluate current online payment systems with IoT card and IoT note. The evaluate membership factors consist of Claimability, Transferability, Recognition, Anonymity, Denomination and Validity Date. Only an IoT note is expected to cover all evaluate factors.

A. Claimable Money

Second evaluation measures an ability of the owner or carrier of electronic money to claim it from the financial provider or bank. The first type of a payment transaction will be between a user to a merchant and then the merchant will be able to claim the money from a bank as shown in the third column of Table II. The second type of claimability will be between users and merchant that means the first user will give the money to second user without any claims from a bank. Also second user will give the same electronic money that he or she received from first user to another user without any claim from the bank. Finally, the end user will give same money to a merchant without claim from the bank. Finally, the merchant will be claimed from the bank.

B. Transferable Money

The third evaluation classifies whether electronic money is transferable or not. The first kind of money transferable will be between users. The second kind of electronic money transfer will be between users without claim from the bank.

After that end user will make a payment to a merchant and the merchant will be able to claim the money from the bank as shown in the fourth column of Table II. Non-transferable electronic money can only be used for one payment only.

C. Recognition of Valid Money

The fourth evaluation measure will classify the type of recognition given to the electronic money as a formal money or informal money by the central bank. The first type of recognition of money is accepted by the banking world as in the fifth column of Table I (Yes). Otherwise, the second type of recognition in the case when electronic money is rejected by banking world in the same column of Table II (No).

D. Anonymity

The next evaluation measure is to classify whether the electronic money is attached to the owner or carrier of the money. The money in a financial account belongs to the account holder. The financial provider can check to whom given money belongs to at a given moment. The carrier of the money may claim the ownership of the money without any reporting to the money issuer or financial provider that shows in Table II. Anonymity is an important element of privacy.

E. Denomination

Another element of money is denomination. Paper money always comes along in certain denomination. It is particularly crucial to introduce a fixed denomination on new electronic money in order to be successful and popular in a new electronic payment system. The last evaluation measure check on a fixed stable denomination in each electronic money rather than having an open amount depending on the transaction amount that shows in Table II.

F. Velocity of Money

This paper will also introduce and evaluate electronic monetary payments in terms of their velocity of money. It measures the frequency of use within the monetary payment system. The First type of payment will be used between users to merchants as shown in the second column of Table II. The electronic money can only be used once only as a payment money. The second type of payment will be using between the first user to second user and also from second user to the end user. Finally, the end user will be used to make a payment to a merchant and the merchant will claim from the bank as shown in Table II as multiple payments.

Velocity of money refers to the frequent usage of same currency to purchase goods produced and service available domestically within duration of time (money transfer between an owner to another). Alternatively, it can refer to the frequent of average unit currency utilized for any transaction of changing hands for both purchasing of goods and financial assets.

In this paper, the **velocity of IoT note** shall be used to further evaluate the effectiveness of an IoT note. Indirectly, the frequency of use of an IOT note will be used in measuring speed the money transfer from one holder to the next. In other words, number of times per unit money is transferred or expenses to purchase service and goods per unit note before it is claimed to the bank or financial provider.

TABLE II. COMPARISON BETWEEN TYPE OF MONEY WITH IOT NOTES USING EVALUATION IOT NOTES

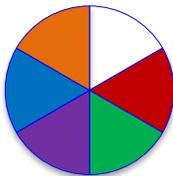
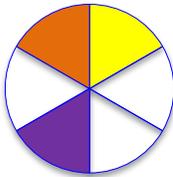
Type of Money	Claimable Money	Transferable Money	Recognition	Anonymity	Denomination	Validity Date	Velocity of Money
Currency	Yes	Yes	Yes	Yes	Yes	No	Multiples
Credit Cards	Yes	No	Yes	No	No	Yes	Once
Virtual Credit Cards	Yes	No	Yes	No	No	Yes	Once
Debit Cards:	Yes	No	Yes	No	No	No	Once
e-Checks	Yes	No	Yes	No	No	No	Once
Digital Cash	Yes	No	No	No	No	No	Once
e-Wallets	Yes	No	No	No	No	No	Once
Mobile Wallets	Yes	No	No	No	No	No	Once
Touch n Go	No	No	No	Yes	No	No	Once
Pay pal	Yes	Yes	No	No	No	No	Multiples
Bitcoins	No	Yes	No	Yes/ No	Yes/ No	No	Multiples
Samsung Pay	Yes	Yes	No	No	No	No	Once
Session IoT card	Yes	No	Yes	Yes	Yes	Yes	Once
IoT notes	Yes	Yes	Yes	Yes	Yes	Yes	Multiples

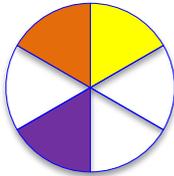
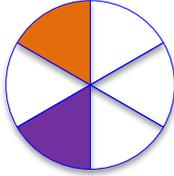
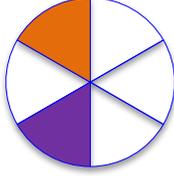
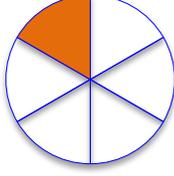
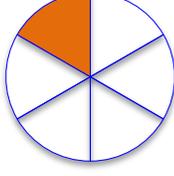
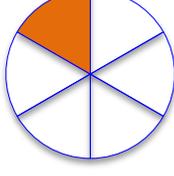
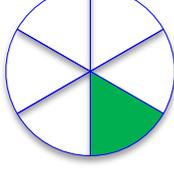
Several online payment systems have been reviewed. A colour scheme as a membership criterion has been given in Tables III and IV.

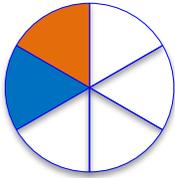
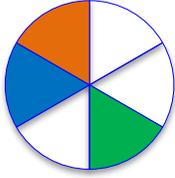
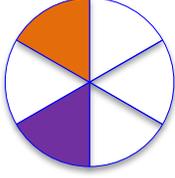
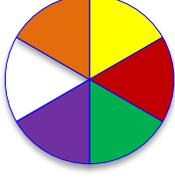
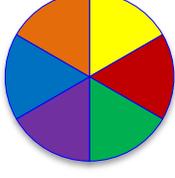
TABLE III. A MEMBERSHIP EVALUATION OF MONETARY SYSTEMS

Colour	Orange	Blue	Purple	Green	Red	Yellow
Note	Claimable	Transferable	Recognition	Anonymity	Denomination	Validity Date

TABLE IV. EVALUATION SCORES ON VARIOUS PAYMENT SYSTEMS

Type of money	Velocity of payment	Coverage
Currency	Multiples	
Credit Cards	Once	

Virtual Credit Cards	Once	
Debit Cards:	Once	
e-Checks	Once	
Digital Cash	Once	
e-Wallets	Once	
Mobile Wallets	Once	
Touch n Go	Once	

Pay pal	Multiples	
Bitcoins	Multiples	
Samsung pay	Once	
Proposed Session IoT card	Once	
Proposed IoT note	Multiples	

VII. CONCLUSION

A traditional banking system is presumably secure and stable. An ease of use has attracted the banking system to online and even mobile. A trade-of between an ease of use on online banking system and a traditional security protocol has to be made. An online banking has been operating outside a secure line at a user's end.

A user may send and make payment directly to a merchant with minimum security protocols. Recently, there are cases of hackers start to attack online banking accounts. The transaction details may be hacked during the process or even later at the merchant database. There is a need to have a new online payment system with minimum information details which can be related back to the original user or account owner.

A one-time note will save the need of protecting the database especially on the credit/debit card information. A more balanced approach has been presented here for easy and friendly use of the IoT money. This paper has extended the

use of one-time payment to a multiple session payment system using an IoT money note.

ACKNOWLEDGEMENT

The authors would appreciate UTeM Zamalah Scheme. This research study is supported by Universiti Teknikal Malaysia Melak (UTeM), to continue first author's study under UTeM Zamalah Scheme.

REFERENCES

- [1] M. T. Rose, L. H. Stein, N. S. Borenstein, C. M. D. Lowery and E. Stefferud, Computerized Payment System for Purchasing Goods and Services on the Internet, U.S. Patent, Washington, DC: U.S. Patent and Trademark Office, No. 5, pp. 757-917, 1998.
- [2] M. N. Al-Mhiqani, R. Ahmad, W. Yassin, A. Hassan, Z. Z. Abidin, N. S. Ali and K. H. Abdulkareem, Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems, International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, 2018, pp. 499-508.
- [3] J. Wan, H. Yan, H. Suo and F. Li, Advances in Cyber-physical Systems Research, KSII Transactions on Internet and Information Systems (TIIS), vol. 5, no.11, pp. 1891-1908, 2011.
- [4] M. F. Ali, N. A. Abu and N. Harum, A Novel Session Payment System via Internet of Things (IOT), International Journal of Applied Engineering Research, vol. 12, no. 23, pp. 13444-13450, 2017.
- [5] T. A. Kraft and R. Kakar, E-Commerce Security, Proceedings of the Conference on Information Systems Applied Research, Washington DC, 2009, pp. 1-11.
- [6] M. Chen, J. Wan and F. Li, Machine-to-machine Communications: Architectures, Standards and Applications, KSII Transactions on Internet and Information Systems, vol. 6, no.2, pp. 672-685, 2012.
- [7] R. Ding and J. Wright, Payment Card Interchange Fees and Price Discrimination, Journal of Industrial Economics, vol. 65, no. 1, 2017, pp. 39-72.
- [8] P. Zhang, Y. He and K. P. Chow, Fraud Track on Secure Electronic Check System, International Journal of Digital Crime and Forensics (IJDCF), vol. 1, no. 2, 2018, pp.137-144.
- [9] N. El-Madhoun, E. Bertin and G. Pujolle, An Overview of the EMV Protocol and Its Security Vulnerabilities, IEEE Fourth International Conference on Mobile and Secure Services (MobiSecServ), pp. 1-5, 2018.
- [10] E. Turban, J. Outland, D. King, J. K. Lee, T.P. Liang and D. C. Turban, Business-to-Business E-Commerce, Springer, Electronic Commerce, Cham, 2018, pp. 123-166.
- [11] J. Urban, Mobile Payments: Consumer Benefits and New Privacy Concerns, SocArXiv, 2016.
- [12] C. J. Hoofnagle, J. M. Urban and S. Li, Mobile Payments: Consumer Benefits and New Privacy Concerns, University of California, Berkeley, School of Law, pp.1-20, 2012.
- [13] Z. Bezovski, The Future of the Mobile Payment as Electronic Payment System, European Journal of Business and Management, vol. 8, no. 8, pp. 127-132, 2016.
- [14] B. U. I. Khan, R. F. Olanrewaju, A. M. Baba, A. A. Langoo and S. Assad, A Compendious Study of Online Payment Systems: Past Developments, Present Impact, and Future Considerations, International Journal Of Advanced Computer Science and Applications, vol. 8, no. 5, 2017, pp. 256-271.
- [15] S. Ghosh, J. Goswami, A. Kumar and A. Majumder, Issues in NFC as a Form of Contactless Communication: A Comprehensive Survey, IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), pp. 245-252, May 2015.
- [16] N. Doan, Consumer Adoption in Mobile Wallet: A Study of Consumers in Finland, vol. 2, no. 6, pp. 816-838, 2014.
- [17] T. Husson, The Future of Mobile Wallets Lies beyond Payments, Forrester Research, 2015, pp.127-132

- [18] A .S. I. Almselati, R. A. O. K. Rahmat and O. Jaafar, An Overview of Urban Transport in Malaysia, *Social Science*, vol. 6, no.1, pp. 24-33, 2011.
- [19] R.K. Webster, Challenges in Compensating Employees in Cryptocurrencies, *Mitchell Hamline Law Journal of Public Policy and Practice*, vol. 39, no.1, 2018, pp. 157-182.
- [20] K. Cao and A. K. Jain, Hacking Mobile Phones using 2D Printed Fingerprints, MSU Technical report, MSU-CSE, pp. 2-16, 2016.
- [21] J. Russell, N. Beitner, O. Dewdney, R. Underwood and W. Jordan, E-commerce Payment System, U.S. Patent Application, no. 09, pp. 810-836, 2002.
- [22] R. H. Weber, Internet of Things–New Security and Privacy Challenges, *Computer Law and Security Review*, vol. 26, no.1, pp. 23-30, 2010.
- [23] J. Siegal, S. Rowell and T. Hintz, Method and System for Providing Online Authentication Utilizing Biometric Data, Open Invention Network LLC, U.S. Patent, vol. 9, pp. 146-911, 2018.
- [24] G. G. Si, X. Zhao, J. Wang, X. Long and T. Hu, A Novel Mutual Authentication Scheme for Internet of Things, *Proceedings of IEEE International Conference on Modelling, Identification and Control (ICMIC)*, pp. 563-566, June 2011.
- [25] A. Abdollahi and M. Afzali, A Single Sign-on based Integrated Model for E-banking Services through Cloud Computing, *International Journal of Advances in Computer Science and Technology*, vol. 3, no.1, pp. 34-38, 2014.
- [26] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig and E. Wustrow, *Elliptic Curve Cryptography in Practice*, *International Conference on Financial Cryptography and Data Security*, Springer, pp. 157-175, March 2014.