International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 23 (2017) pp. 13444-13450

A Novel Session Payment System via Internet of Things (IOT)

Mohanad Faeq Ali
Universiti Teknikal Malaysia Melaka, Malaysia.

Orcid: 0000-0002-3242-9798

Nur Azman Abu
Universiti Teknikal Malaysia Melaka, Malaysia.

Orcid: 0000-0003-4624-3123
SCOPUS ID: 6506357105

Norharyati Harum
Universiti Teknikal Malaysia Melaka, Malaysia.

Orcid: 0000-0003-0068-6025,
SCopus ID: 55664980400

Abstract

A wireless method has been 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 debit/credit cards in a wallet. It is more convenient to carry a debit/credit card electronically on a smartphone. This paper will embark on an electronic debit/credit card on a smartphone and migrate to IoT money. A novel session payment system using IoT money shall be introduced to minimise debit/credit card risk. The scope of this paper is confined into the security model for an easy payment system based on Internet of Things (IoT). Since each IoT money is unique to each payment, this session payment system will ease the burden on protecting the database of the payment system.

Keywords: Easy payment system, Internet of Things, Secure Payment System

INTRODUCTION

The arrival of the Internet of Things (IoT) in the mid 90's did not only result into extensive and innovative research but also the upcoming of innovative ideas aimed at solving problems practically within the business context through the use of existing technology [1]. The IoT technology applications are very broad in e-commerce. IoT technology can be used in various aspects of e-commerce. It has brought not only a new economic growth but also provided a competitive element to an e-commerce. Even though the application of IoT technology is still at a relatively early stage, the relevant technology is starting to mature. In order to gain significant advantages from IoT technology, the current research should focus on the long term sustainable development. Only in this way, can make good use of this new IoT technologies, there is a huge impetus to the development of e-commerce. In this paper, the development trend of IoT applications has been analyzed and the problems in traditional e-commerce are presented.

In the IoT technology application, there are three important aspects, such as e-commerce inventory, logistics and payment. This research paper concentrates on the key technical issues of e-commerce security measures [2].

A traditional chip-and-pin credit card has been widely accepted for the last few decades. The new credit card with a chip physically in a wallet seems to be secure and convenient to its user. Nevertheless, the new credit card is still vulnerable. With a small modification to the current equipment, the chip-and-PIN protections can be bypassed to enable unauthorized payments [3].

The Internet of Things gained popularity in 2010 and has recently attracted the attention of most scholars and business decision makers. The IoT is a linking factor for various elements such as buildings, cars, different equipment and people. The IoT also works on linking offline objects to the e-commerce business models. A centralized IoT platform hosted by the firm's e-commerce will be responsible for mining data into valuable information to be used for making decisions in the e-commerce business. The e-commerce system is integrated with the IoT technology in three different aspects such as; inventory, logistics and payment systems [4].

The safety issue in e-commerce lies in the e-commerce asset protection which does not permit anything within the site to be altered or destroyed. However, the system does not guarantee the safety of the survivors within. Such security issues include; spamming, surfing, distributed denial of

service attack, viruses, worms, trojan horses, illegal access, masquerading or spoofing, sniffers, operating system loopholes and theft of data [5].

The research paper offers an improved design system to be used in the E-commerce based on Internet of Things. The new e-commerce based on the IoT system will encompass the following elements: overview of the E-commerce security and the different specific security issues in E-commerce business [6].

INTERNET OF THINGS

The internet was first developed in 1960 from the U.S military network (ARPANET). It was created to link computers around the world with the anticipation that the interconnection would allow sharing and quick access of data and information around the world. The World Wide Web was also developed to create a more user friendly interface for the internet. It was invented by a British scientist, Tim-Berners Lee at the European Physics laboratory (CERN). During this period, the internet used a GUI with web browsers like Netscape and Internet Explorer. Web browsers became available and free of charge in 1993 and it was called Mosaic, which was the precursor of Netscape. The web allows connection of different web pages through the use of a hyperlink which creates link to other pages on the same website or different websites from a different computer [7].

The revolution of the internet technology has brought in improvements in the business industry. It has made applications to be easily accessible and available. Hence, the use of e-commerce has become more predominant in the virtual community [8].

E-COMMERCE

E-Commerce describes all the transactions that are done over the internet with the help of digital technology. Mostly, there is an exchange of money for goods or services across boundaries of the organization. A commercial exchange or trade only occurs if there is a value exchanged with a product or service [9].

There has been a debate on the limits of e-commerce and e-business and the difference between the two. While some argue that e-commerce is a worldwide electronic based organization supporting activities in a firm market exchange infrastructure including the information system, others claim that e-business covered both the internal and external electronic based activities inclusive of e-commerce.

E-commerce comprises of seven unique features as mentioned by Laudon, Traver and Elizondo, 2007: Ubiquity, Global reach, Universal standards Richness, interactivity, information density, and personalization/customization [10].

SECURITY ISSUES IN IoT

Security is one of the key issues affecting the IoT technology. The technique has implemented various mechanisms to ensure that all data and transactions done over the internet are secure from vulnerability. An unsecured IoT system can be vulnerable to potential cyber-attacks and data intrusion. It is important to keep security in mind while outlining the design considerations for an IoT system. Individual privacy of users is an essential factor to consider. Therefore, strategies and mechanisms need to be implemented to enforce privacy of data and information for the users' operation over the IoT services [11].

IoT COMMUNICATION MODELS

Device to Device communications:

Wireless swipe for debit/credit card payment gateway [12].

Figure 1: Device to Device communications via Bluetooth, Z-Wave or ZigBee can be set up to switch on/off a light bulb [13]

The network devices in this set up rely on certain protocols for communication and exchange of messages across the platform. The model is mostly used in applications that use small data packets of information for communications such as home automation systems. The devices usually have a direct link with trust and security mechanisms. The figure 1 shows the communication between device to device [13].

Figure 2: Device-Cloud Communications may integrate 2 or more devices at the same time over a cloud by an application service provider [14]

Device to Cloud Communications

The setup uses existing communication mechanisms like Ethernet and Wi-Fi connections to create links between devices and the IP network and finally connect to the cloud that shows in figure 2 [14]. The model is widely used in consumer devices such as thermostat nests and Samsung smart TV. The connection allows users to get remote access to the thermostat devices via their cell phones. The technology gives users the ability to expand the original features in the tool. The platform allows for the integration of devices connected hence guaranteeing security [15].

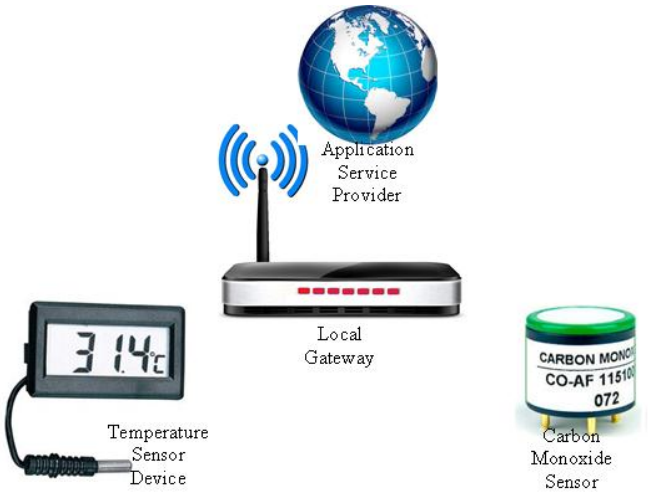

Figure 3: Device to a local gateway device may ease data delivery through a cloud service [16]

Device to Gateway Model

The devices use a model of device application layer gateway (ALG) [16]. The devices access the cloud services through the ALG system with the use of an intermediate software system between the devices and the cloud service which provide security and data protocol translation services. The local gateway device is usually a mobile phone through which the application runs and communicates with devices and ease data delivery to cloud services that shows in figure 3 [17].

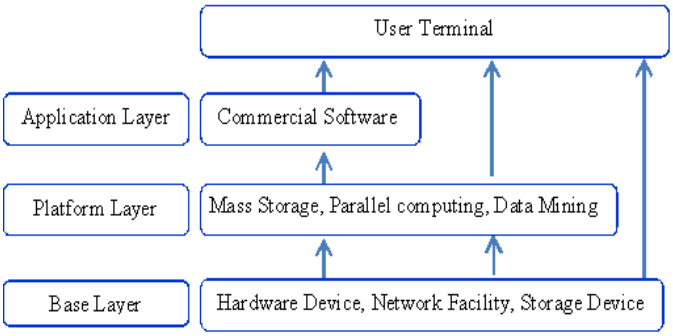

Figure 4: Exchange activities on an IoT based E-Commerce system [18]

FRAMEWORK FOR E-COMMERCE BASED ON IoT

The architecture allows users to make use of the network resources in a cost effective format that replaces the traditional architectural model. The figure 4 below describes an e-commerce model based on the IoT framework [18]. The base layer links the system to other service providers. The IoT enables access to data through the means of secure and flexible hardware resources. The platform layer handles mass storage, parallel computing and data mining while the application layer handle commercial software used in the e-commerce business.

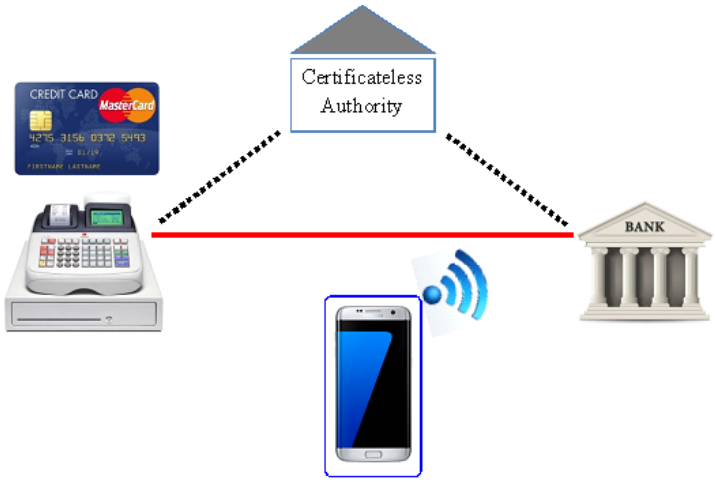

Figure 5: An E-commerce secure payment mode [19]

CURRENT PROBLEM

A common online electronic payment system via debit/credit card payment system which is enables users to pay for services online.The system operates on three basic models namely; minimun security model, a third party broker model [20] with a simple encrypted payment system and security electronic transaction model such as SET [21]. This paper will address specific problem on the use of debit/credit card on or offline. As illustrated in figure 5, 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[19]. 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.

A ransomware is a unique form of purposeful attack that encrypts computer files, network file and even databases, thereby preventing user access to important live data. In order to regain access to the data, the victim will be asked to pay a ransom [22]. The success of Wannacry ransomware [23] in the last few years shows that a well-guarded financial database is also vulnerable to an open attack. The WannaCry ransomware attack moved laterally within networks at an unprecedented level a normal database redundancy alone would not have prevented the WannaCry ransomware attack,

especially if there are time-delayed attacks that have been let loose and are waiting to activate.

Fortunately, this ransomware is not attacking individual information such as the credit/debit cards. A session IoT credit number would carry minimum risk for such an intrusion the database. Another electronic payment system is the E-Cash internet payment system. It is an efficient and popular system. At the same time, it provides anonymity, cost efficiency and flexibility. Other methods including the E-purse and E-check internet payment systems are also vulnerably subjected to the above problem.

BITCOINS AND OTHER CRYPTOCURRENCIES

A Bitcoin is new currency online money created in 2009 by an unknown person. Bitcoin is a cryptocurrency and a digital payment system invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto. The network system for Bitcon uses peer-to-peer and transactions take place between users directly without any intermediaries. It is virtual digital money with almost anonymity. It is released as open-source software in 2009. A Bitcoin has become important online marketing in the world that predominantly covers 90% of all cryptocurrencies. Once the idea of cryptocurrency becomes popular, new cryptocurrencies crops out such as Ethereum, Filecoin, XRP, Gnosis tokens and Tezos which cause Bitcoin market share to dip below 80% and dive straight down until it is now left with 50% only [24].

Figure 6: A payment swiping on the NFC terminal on the left or a touch on the MST terminal

SAMSUNG PAY

Recently, a new mobile payment system, namely, Samsung pay has been introduced. Samsung pay is wallet service by Samsung electronics that allows users make payments using compatible and other Samsung devices. Samsung pay using a new secure technology called Magnetic Secure Transmission that allows contactless payments to be used on payment terminals which support not only magnetic stripe but also normal contactless cards. The service supports contactless payments using near-field communications such as NFC and MST. Samsung pay application is available on all eligible Samsung devices, preinstalled in the device or as available for download as an application update. The users must have Samsung account and a valid credit card available for registration. The procurer will verify his/her fingerprint to authorize the transaction. Alternatively, the users must enter 4-digit Samsung Pay PIN if users have chosen not to use the fingerprint feature. Any further transaction after the registration will no longer use his/her credit card information. If the merchant uses a contactless NFC terminal, the user can simply touch his/her mobile device to the NFC reader to complete the transaction [25]. Otherwise, a cashier will key in the payment details and the user will just touch his/her mobile device to the card-swipe part of the card reader to complete the transaction as show in Figure 6.

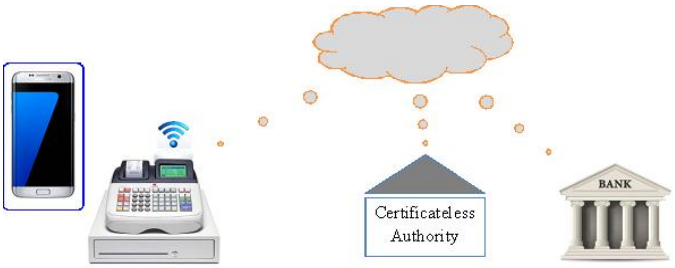

Figure 7: A basic payment system of IoT session card [26]

A SESSION IOT CARD

A smartphone has become an important part of life. It is a source of communication. An owner of the smartphone will protect and safeguard the security of the smartphone at any cost all the time. It is more practical to embed a debit/credit card electronically on a smartphone. This paper shall propose an electronic debit/credit card on a smartphone. A novel session payment system shall be introduced to minimise debit/credit card risk. In Figure 7 illustrates the working of an IoT E-Commerce secure payment mode [26]. This new model will pay special attention to the new card session number. This IoT card number will be dynamically changed and updated to the new number once a transaction has been executed. Therefore, it will be a randomly unique number per transaction which is recognized by an IoT service provider. Each new session card number will also be digitally signed by the financial provider [27].

Once a smartphone with an IoT session card is swiped at the service provider terminal, the payment system will first verify the digital signature of the session number. Once verified, the payment system will request for the transaction to the financial provider. 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 session card number 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.

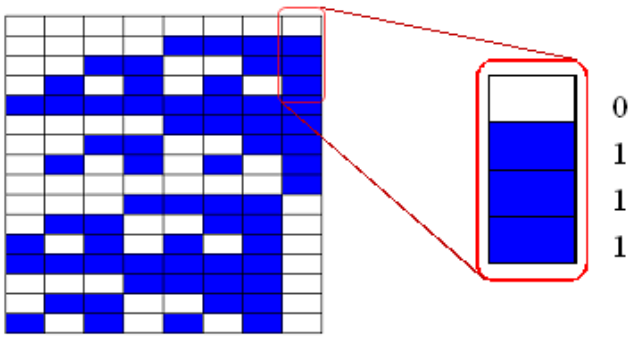

Figure 8: The top right hand corner represents top right hand hexa value of $0 \cdot 2^3+1 \cdot 2^2+1 \cdot 2^1+1 \cdot 2^0=7$ in Table 1

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 1. 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 Figure 8. 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.

Table 1: 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

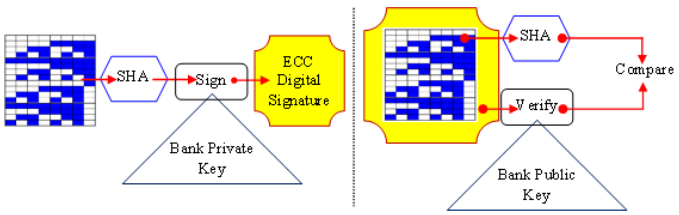

Figure 9: The Session IoT card number will be signed by its financial provider

The study will propose 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 Figure 9. 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 can verify the digital signature from using the bank public key and compare to the hashed Session IoT card number.

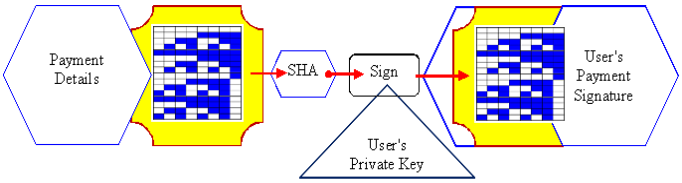

Figure 10: An online payment on each transaction will be typically signed by the IoT session smart card owner

Each payment will also be signed digitally by the user as shown in Figure 10. 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 RM 5, RM 10, RM 20, RM 50 and RM 100. The barcode IoT Session number will also follow the traditional colour of the paper note, i.e. green, red, yellow, turquois and purple respectively.

Figure 11: A nice sample of RM 10 note

The IoT note will also come along with the ECC digital signature as shown in Figure 11. 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 10 in Figure 11. 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 personal mobile intelligent terminal of the e-commerce businesses. Lightweight Tablet PC can also be used as a carrier with an embedded 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. It realizes a simple and secure payment application mode. An IoT PDAs payment resolved program is that RFID reader module is combined with a smartphone for the first time, the user does not need to pay by cumbersome online banking. There is just a portable handheld personal device and the entire process is completely contactless.

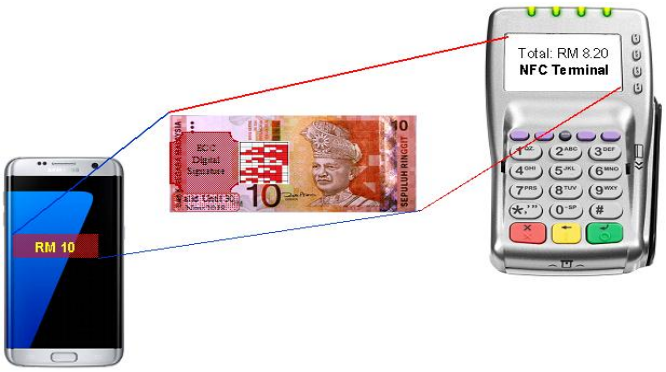

Figure 12: A user will slide an RM 10 note from his pocket money to an NFC cashier terminal within his smartphone IoT application

As visualized in Figure 12, 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.

This electronic Session IoT card payment is different payment with other online payment tool, such as Alipay and Tenpay as this payment is the innovation applications of the latest IoT RFID contactless technology. Internet shopping is combined together with IoT payment. A lightweight Tablet PC is used as a carrier. A payment module is embedded in the RFID reader where a simple and secure smart card payment application mode is achieved by a friendly feature of sliding the note to a merchant iconic application. In IoT handheld payment, all funds were allocated through a bank dedicated channel to avoid security risks through open Internet. By using the AES algorithm, all the data are encrypted for users on the card and on data transmission from mobile devices to a clearing center in order to ensure maximum security of the fund transfer. The bank will maintain a money database to detect double-spending and ensure the validity of this IoT note.

CONCLUSION

The IoT technology applications can potent in e-commerce. IoT technology can be used in various aspects of e-commerce. It has brought not only a new economic growth but also provided a competitive element to an e-commerce. Even though the application of IoT technology is still at a relatively early stage, the relevant technology is starting to mature. In order to gain a significant advantage from IoT technology, the current research should move on mobile payment system. Only in this way, can make good use of this new IoT technologies, there is a huge impetus to the development of mobile payment system. In this paper, a flexible mobile payment system has been presented.

In the IoT technology application, there are three important aspects, such as e-commerce inventory, logistics and payment. It is crucial to concentrates on the key technical issues of e-commerce security measures. A more balanced approach is called for here for easy and friendly use of the IoT money.

ACKNOWLEDGEMENT

The authors would like to thank the 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] X. Cui, "The internet of things," in *Ethical Ripples of Creativity and Innovation*, ed: Springer, 2016, pp. 61-68.

[2] R. Ramanathan, "The moderating roles of risk and efficiency on the relationship between logistics performance and customer loyalty in e-commerce," *Transportation Research Part E: Logistics and Transportation Review*, vol. 46, pp. 950-962, 2010.

[3] A. A. Z. Hudaib, "Banking and Modern Payments System Security Analysis," *International Journal of Computer Science and Security (IJCSS)*, vol. 8, p. 38, 2014.

[4] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, pp. 1497-1516, 2012.

[5] C. Anchugam and K. Thangadurai, "Classification of Network Attacks and Countermeasures of Different Attacks," in *Network Security Attacks and Countermeasures*, ed: IGI Global, 2016, pp. 115-156.

[6] T. A. Kraft and R. Kakar, "E-commerce security," in *Proceedings of the Conference on Information Systems Applied Research, Washington DC, USA*, 2009.

[7] J. Ryan, *A History of the Internet and the Digital Future*: Reaktion Books, 2010.

[8] Y. Lu, L. Zhao, and B. Wang, "From virtual community members to C2C e-commerce buyers: Trust in virtual communities and its effect on consumers' purchase intention," *Electronic Commerce Research and Applications*, vol. 9, pp. 346-360, 2010.

[9] M. Niranjanamurthy, N. Kavyashree, S. Jagannath, and D. Chahar, "Analysis of e-commerce and m-commerce: advantages, limitations and security issues," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, 2013.

[10] B. Xiao and I. Benbasat, "E-commerce product recommendation agents: use, characteristics, and impact," *MIS quarterly*, vol. 31, pp. 137-209, 2007.

[11] O. Dandash, Y. Wang, P. D. Le, and B. Srinivasan, "Fraudulent Internet Banking Payments Prevention using Dynamic Key," *JNW*, vol. 3, pp. 25-34, 2008.

[12] D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano, "Device-to-device communications with Wi-Fi Direct: overview and experimentation," *IEEE wireless communications*, vol. 20, pp. 96-104, 2013.

[13] R. Shahriyar, E. Hoque, S. Sohan, I. Naim, M. M. Akbar, and M. K. Khan, "Remote controlling of home appliances using mobile telephony," *International Journal of Smart Home*, vol. 2, pp. 37-54, 2008.

[14] M. Jo, T. Maksymyuk, B. Strykhalyuk, and C.-H. Cho, "Device-to-device-based heterogeneous radio access network architecture for mobile cloud computing," *IEEE Wireless Communications*, vol. 22, pp. 50-58, 2015.

[15] M. Shiraz, A. Gani, R. H. Khokhar, and R. Buyya, "A review on distributed application processing frameworks in smart mobile devices for mobile cloud computing," *IEEE Communications Surveys & Tutorials*, vol. 15, pp. 1294-1313, 2013.

[16] S. K. Datta, C. Bonnet, and N. Nikaein, "An IoT gateway centric architecture to provide novel M2M services," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, 2014, pp. 514-519.

[17] P. Desai, A. Sheth, and P. Anantharam, "Semantic gateway as a service architecture for iot interoperability," in *Mobile Services (MS), 2015 IEEE International Conference on*, 2015, pp. 313-319.

[18] A. Ordanini and G. Rubera, "How does the application of an IT service innovation affect firm performance? A theoretical framework and empirical analysis on e-commerce," *Information & Management*, vol. 47, pp. 60-67, 2010.

[19] E. J. Hogan and C. M. Campbell, "Method and system for secure payments over a computer network," ed: Google Patents, 2017.

[20] J. Russell, N. Beitner, O. Dewdney, R. Underwood, and W. Jordan, "E-commerce payment system," ed: Google Patents, 2001.

[21] M. T. Rose, L. H. Stein, N. S. Borenstein, C. M. Lowery, D. New, and E. Stefferud, "Computerized payment system for purchasing goods and services on the internet," ed: Google Patents, 1998.

[22] S. Khajuria, L. Sørensen, and K. E. Skouby, *Cybersecurity and Privacy-Bridging the Gap*: River Publishers, 2017.

[23] C. Kuner, D. J. B. Svantesson, F. H Cate, O. Lynskey, and C. Millard, "The rise of cybersecurity and its impact on data protection," *International Data Privacy Law*, vol. 7, pp. 73-75, 2017.

[24] J. B. A. M. J. Clark, A. N. J. A. K. Edward, and W. Felten, "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies."

[25] K. Cao and A. K. Jain, "Hacking mobile phones using 2D Printed Fingerprints," MSU Technical report, MSU-CSE-16-22016.

[26] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in *Modelling, Identification and Control (ICMIC), Proceedings of 2011 International Conference on*, 2011, pp. 563-566.

[27] A. Abdollahi and M. Afzali, "A Single Sign-on based Integrated Model for E-banking Services through Cloud Computing," *International Journal*, vol. 3, pp. 34-38, 2014.