2014

# Efficient M-Commerce Platform for Developing Countries

Lonell Liburd
*The University of the West Indies*, lonell.liburd@gmail.com

Patrick Hosein
*The University of the West Indies*, patrick.hosein@sta.uwi.edu

# 10P. Efficient M-Commerce Platform for Developing Countries

Lonell Liburd
The University of the West Indies
lonell.liburd@gmail.com

Patrick Hosein
The University of the West Indies
patrick.hosein@sta.uwi.edu

## *Abstract*

Mobile phones have become an integral part of a vast majority of people's daily lives. It is becoming rare to conduct any form of communication between individuals without a mobile phone. Research continues on the integration of mobile phones and e-commerce solutions. Developed countries already use systems for such commercial transactions however developing countries, for example those in the Caribbean, face challenges in adopting such systems. This paper proposes a system that would allow users to carry out financial transactions with their mobile phones as well as manage their financial activities. The system, which we call PayPhone, allows customers in developing countries to pay for items by tapping their phone against a terminal that supports Near-Field Communications (NFC). The system is compared to other systems such as the debit card based system, LINX, in the Caribbean and other systems in developing and developed countries. We also explore and discuss other possible short-range technology options.

## *Keywords*

Near-Field Communication, NFC, M-Commerce, Micro-payments, Smartphones, Security

## 1. Introduction

Mobile and micro-payments continue to be interesting research topics. Many companies have tried various implementation strategies and ways to profit from micro-payments to tap into what has become a multi-billion dollar industry (Warman, 2013). The Caribbean is no stranger to the power of mobile technology with very high mobile penetration rates. According to the International Telecommunications Union (ITU) (2012), Trinidad & Tobago had a mobile penetration rate of 140%, Jamaica 98%, St. Kitts & Nevis 156%, St. Vincent & the Grenadines 123% and Antigua & Barbuda 143%. With such access to mobile technologies, the Caribbean is more than ready to accommodate mobile-based transaction processing.

A problem, however, exists with current implementations of m-commerce systems. They are not tailored to suit developing countries where the financial infrastructure is not as accommodating of mobile payments, or credit card based (Visa, MasterCard, and the like) payments. In order to facilitate m-commerce on a profit worthy scale, requirements such as acquiring merchant accounts need to be met. Small to medium sized enterprises comprise the majority of business in the Caribbean (NEDCO, 2012), these businesses unfortunately may not have the resources to acquire such independent accounts for credit card based transactions. This approach, which is increasingly more difficult to achieve outside of North America, charges a per-transaction fee

and a percentage of each transaction. Acquiring such accounts through indigenous banks also proves quite difficult as these institutions rely also on an intermediary agency, which results in the merchant bearing additional service charges to conduct such business.

A system is needed to facilitate micro-payments and m-commerce within the Caribbean, with potential use in other developing countries. This system, first and foremost, must be easy to use, highly secure and truly low-cost. Thus, it must circumvent credit card based payments, which are, by comparison, very expensive. A system that is truly low-cost must maintain low fees on both sides of a transaction, the merchant and the customer. If a merchant does not incur high fees to use a system then there need not be higher fees attached to goods and services to offset those charges.

We propose the creation of a low-cost, micro-payment system, called PayPhone that utilises both Near-Field Communication (NFC) technology on a mobile device to facilitate transactions and a complete back-end processing system to facilitate management by both users and merchants. The system allows users to make and manage their purchases online and also for merchants to manage their business account as well.

Near-Field Communication is a form of short-range communication based on radio-frequency identification (RFID). It allows NFC-enabled devices to exchange small amounts of data. Because of the type of communication technology used, it can only process transactions over a small range, around 10cm (Madlmayr, Kantner, Grechenig, 2014). NFC can be used for a range of tasks such as service initiation, data exchange, ticketing and payment. The latter forms the basis of this paper. Although NFC is a relatively new technology we surveyed 100 smartphone users and found that 50% of these users' phones supported NFC.

The mPesa system (Mbiti & Weil, 2011) uses mobile phone credits issued by Telecommunications companies as the funding sources for customers. It is similar to implementations by companies such as Digicel, LIME (Cable & Wireless rebrand) and (bMobile/TSTT in Trinidad & Tobago) which offer e-TopUp and e-CreditU services. However, the eTopUp and e-CreditU services only allow customers to add airtime credit to their mobile phones and share any surplus with other customers on the same network. The credit can only be used to conduct telecommunication specific actions such as placing a call or sending a text message. Moreover, the sharing of airtime credit is limited to persons on the same network. Such services are inadequate to suit m-commerce requirements. The system was successful when used for money transfers between customers competing with more expensive merchants such as MoneyGram and Western Union. However, as a payment solution for daily transactions, it is not sufficiently efficient or user friendly. mPesa relies on Short Message Service (SMS) to complete any transaction. This platform can, at times, be unreliable especially when the mobile network becomes congested. Response times are not predictable and transaction completion times can be crippled pending SMS confirmation. Additionally, to conduct a transaction using the mPesa system, users are required to memorise complicated short codes. The Telecommunications provider uses these codes to differentiate user transactions but to the user they can be confusing. The system also presents the burden of retailers needing to handle financial accountability on a scale similar to that of banking and financial institutions as well as the security needed to transport large sums of cash on a daily basis. The system proposed in this paper remedies the

potential unavailability of SMS based connections by exploring other viable alternatives and providing a User Experience (UX) that supports users ranging from novice to expert.

Other systems (Mbiti & Weil, 2011; Eijman, Kendal & Mas, 2010; Balan et al., 2009) have been proposed for use in developing countries. However these implementations would not be suitable for the purposes addressed by PayPhone. mFerio is a peer-to-peer system for exchange of cash credit similar to mPesa. Its implementation is limited solely to the exchange of funds between two customers with no financial accountability between the users. PayPhone facilitates payment from customers to merchants and a total financial management aspect that these previous solutions lack. The PayPhone system provides additional features that extend the capabilities of the proposed designs and implementation.

The techniques explored by Chen and Adams (2004) utilises insecure technologies that are also not 100% reliable or easy to use. These techniques involve the use of Bluetooth and Infrared as a means of establishing connections for communications. Bluetooth has become burdensome to set up. Users must first search for each other then agree to some device-generated shared pin then connect. Such security protocols should be hidden from the user. There should be confidence in the security measures of the technology thus removing the need to carry out these procedures. Bluetooth connections also have a lower throughput than NFC, averaging 305kbps compared with 424kbps with NFC (Smith, 2011). Infrared, although much faster than NFC at around 1Gbps, requires a clear line of sight connection to maintain communications. Line of sight disruptions require re-initialization. Infrared connections also do not support encryption such as SSL (which NFC supports) thus giving it a significant disadvantage for financial use. These reasons make NFC a better choice for use in mobile payments.

Implementing a micropayment system through the use of smartphones gives users another alternative to conduct transactions. Choice plays a vital role in economics and more choices allow for greater competition within markets consequently reaping positive rewards for consumers. Moreover, it gives users another secure alternative to paying for items. The proposed system will be tested in Trinidad and Tobago where the present predominant system, called LINX, is based on debit cards. The LINX system handles 36 million transactions per year (InfoLinx, 2014). To demonstrate the proposed system's effectiveness we compared transaction times for the two alternatives.

# 2. LINX

LINX is a debit-card system put in place by four major banking institutions in Trinidad & Tobago, First Citizens Ltd., Republic Bank Ltd., RBC Royal Bank and Scotia Bank of Trinidad & Tobago Ltd. It is the only system that provides locally authorized transactions in the Caribbean region. The LINX payment system allows customers to conduct transactions on a daily basis through the use of their bank-issued, LINX-enabled debit card. A customer swipes their debit card at a merchant's outlet to trigger a transaction. The merchant must then enter their private security code to continue the transaction. The customer then confirms the amount entered on the LINX terminal and selects the appropriate account with which he wishes to debit the amount. He is then required to enter a 4-digit secret PIN to confirm his identity. The LINX system uses a dial-up data connection to transfer transaction details from the merchant to the

LINX operator. Once sufficient funds are available, the transaction is returned with an "Approved" notification signalling the completion of the transaction or a "Rejection" notification indicating insufficient funds. Figure 2 shows an overview of the transaction clearance process. The operator of the LINX network collates and sorts all transactions received though the Point of Sale (POS) terminals and ATMs then calculates the net settlement for the merchant bank. The operator then notifies the respective banks on the net settlement they are owed from LINX transactions and then notifies the settlement bank to pay the amount to the merchant banks (Central Bank of Trinidad & Tobago, 2009).

The LINX card is versatile as it also doubles as an ATM (Automatic Teller Machine) card. However, this presents a security risk to customers as these cards can not only conduct payments but also withdraw funds (although usually capped at a reasonable amount) from their respective accounts. The system proposed attempts to mitigate this threat by only allowing for payment of items and, given a sufficiently large adoption rate, there should be less of a need for cash withdrawals for everyday items. It should also be noted that merchants are required to pay a monthly rental fee for use of the LINX terminals, another cost that needs to be factored into merchant prices.

# 3. PayPhone

PayPhone is a low-cost, m-commerce system that fully supports transaction switching, connecting merchants, financial institutions and smartphone users to facilitate fast, reliable and secure payments. The system allows smartphone users to make payments at supported merchants without the need of a debit card. The users need only their smartphones and a cellular data connection to conduct their transactions. The PayPhone system is a transaction processing system with a fully automated back-end that allows customers to manage their spending activities. The system allows payments through the use of NFC "taps". NFC is the best technology for this system especially because of its security features. NFC-enabled smartphone users need only bring their device in close proximity to a NFC-terminal. The terminal would communicate the transaction amount to the user's smartphone allowing the customer to confirm or deny the amount for the sale. The customer would then be required to enter his secret PIN-code. Unlike regular 4-digit PIN codes, this code can be of varying length between 4 and 10 digits allowing for up to $10^{10}$ combinations. Once the PIN code has been entered, the user would then be prompted to tap their phone on the NFC tag. The merchant receives a confirmation message on their computer that alerts them to the completion of the transaction likewise updating the user's smartphone with the transaction. The system debits the customer's account and credits the merchant's account with the transaction amount. Figure 1 shows the steps needed to complete a transaction using the PayPhone system.


**Figure 1**: PayPhone Payment Process

A comparison of the clearance process of PayPhone and the LINX system is illustrated in Figure 2. Unlike the LINX system, which must go through both the cardholder and merchant banks as well as needing a settlement agent, PayPhone requires only the use of a financial institution simply to debit the cardholder's bank account. When the user makes a purchase a transaction is created which is collated at the financial institution and settled to the Merchant's bank.

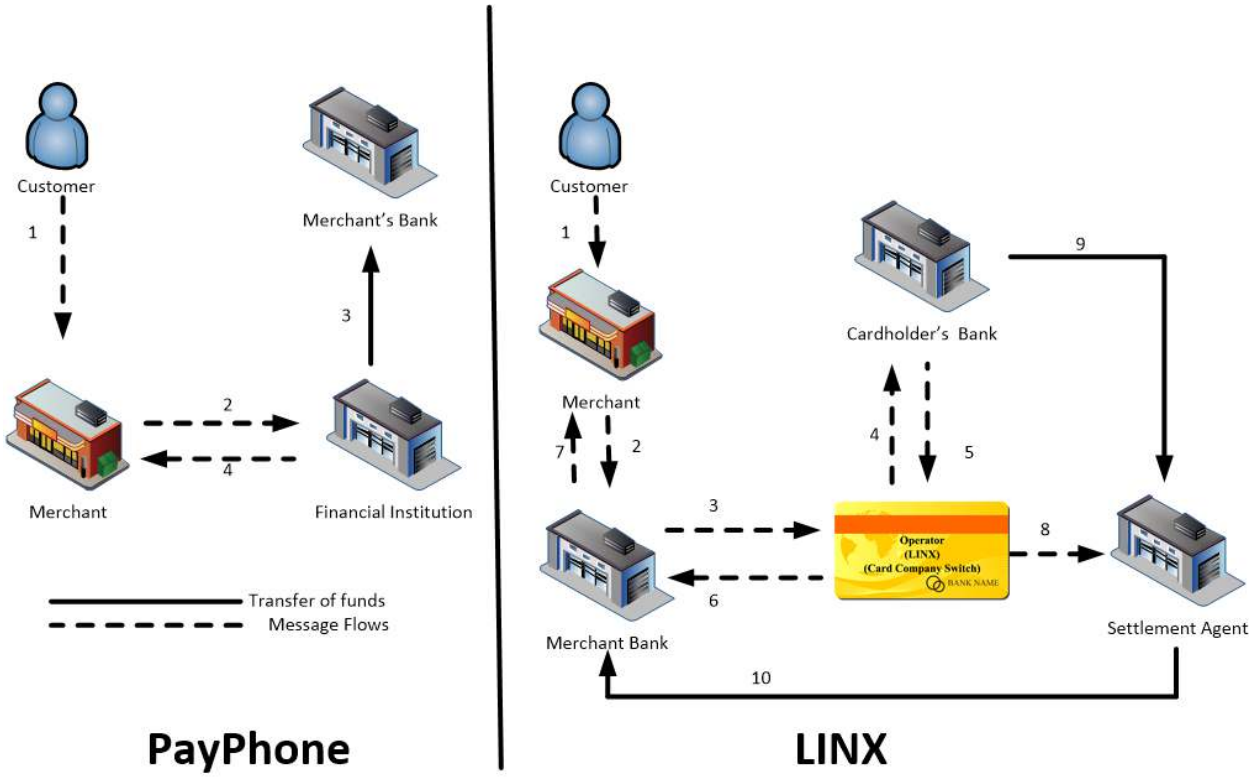


**Figure 2**: PayPhone Payment Clearance Process

The "Recent Transactions" screen of the user's smartphone is updated immediately once a transaction is completed to alert the user of its success or failure. The inherent security in NFC is attributed to the proximity requirement. The range necessary to complete the transaction is so small that it prevents any malicious user from attempting to intercept the communicated data.

As an additional security feature, users are required to tap their NFC-tag IDs before completing a transaction. These tag IDs are passive NFC tags embedded into everyday items. Passive NFC tags are small storage tags with radio chips attached to an antenna that are easily integrated into ordinary items such as posters, books and jewellery. They draw power from the reading device through magnetic induction, hence the term 'passive'. The NFC tag ID stores a unique auto-generated code associated with that customer. This means that, in order to complete the transaction, the customer must not only know their secure PIN code but must also present their NFC tag ID to confirm. The customer cannot change this code and only one code can be associated with a customer. The code can be written to any number of items at the customer's discretion and request. However, the safety of such items lay solely with the customer. This measure is a necessary step in the event that the smartphone is stolen or lost. The tag ID is disguised as any ordinary item that the user possesses. However, without it, the transaction cannot be completed and the user's smartphone cannot be used to conduct illegal transactions. Once all necessary steps are complete, the transaction is processed.

# 4. Implementation

The PayPhone system is comprised of a mobile component and a Back-end Management System seamlessly connected to ensure constant, uninterrupted communication. It was important to ensure that all these components work independently as they are further subdivided into a total of 4 components. The mobile component is comprised of the Android smartphone application and the NFC Terminal. The Back-end Management system has two separate components depending on the type of user. Consumers have access to the User Management and Administration System (UMAS) and merchants have access to the Merchant Management and Administration System (MMAS), both built using the Node.js server-side environment.

## 4.1 Android Application

The mobile application component is the main means of conducting transactions within the entire system. It is built for the Android Operating System since mobile phones that support this operating system are dominant and hold an 80% control of the global market (IDC Corporate USA, 2013). The application is built to support Android OS versions 4.0 and higher that account for more than 74% of the phones in circulation (Google, 2013). When a customer installs the application for the first time they are prompted to register for the service. Once the user registers they are given a unique Registration ID that is used to identify their mobile device. In order to use the application, users must activate their account by navigating to their email client and following the link attached from the registration-generated email. Once this is done, users are prompted to log in to the mobile application, which maintains the logged in state for the duration of their use.

The PayPhone Android application relies heavily on NFC to complete communications with merchants. Customers simply tap their phone against the NFC terminal to begin the transaction. The NFC terminal transmits an encrypted token unique to the merchant along with the payment amount to the Android application. The user can choose to confirm or deny in which case the transaction is ended. If the user confirms the transaction amount they enter their secret PIN and tap against their tag ID. The tag ID is compared with the customer's stored tag ID to confirm authenticity. This transaction data is sent to the PayPhone system.

The PayPhone system needs to maintain communication between both the merchants and customers. When a purchase is made, both the merchant and the customer need to be updated to confirm payment and receipt respectively. The PayPhone system achieves this by using two separate communication channels. Notifications to the Customer are sent via Google Cloud Messages and to the merchant via Socket.io messages. Google Cloud Messaging for Android (GCM) is a service provided by Google that allows servers to send data to Android-powered devices. These messages can be in the form of send-to-synch messages and messages with payload. PayPhone makes use of both. When the user registers for the PayPhone system, an auto-generated GCM registration ID is assigned to that user's device. This means that only that customer can use the registering device to complete transactions. Once a transaction is carried out, customers must always be notified of its status, whether it is successful or not. The server sends a send-to-synch message if the transaction is successful, prompting the device to update the current list of recent purchases to reflect the sale. If the purchase is not successful, a message with payload is sent, alerting the customer to the failure together with a reason code. Reasons

may include that the account is not active or that there are insufficient funds. GCM removes the overhead of maintaining connections to the mobile device from the PayPhone system.

The customer receives instant feedback on the status of his transaction. This is viewed in the *Recent Purchases* screen where transactions are sorted by most recent completion date and time. The customers see their ten most recent transactions and view their receipts from the transaction. The receipts generated contain the merchant, tax and service charges of the merchant and application. This gives customers immediate feedback on their transaction history whenever they need it. This sale also displays a receipt of the transaction that the customer also can access via the UMAS. The settings screen also allows users to update their secure password, their PIN code and Daily spending limits. Figure 3 shows the full payment procedure of application.

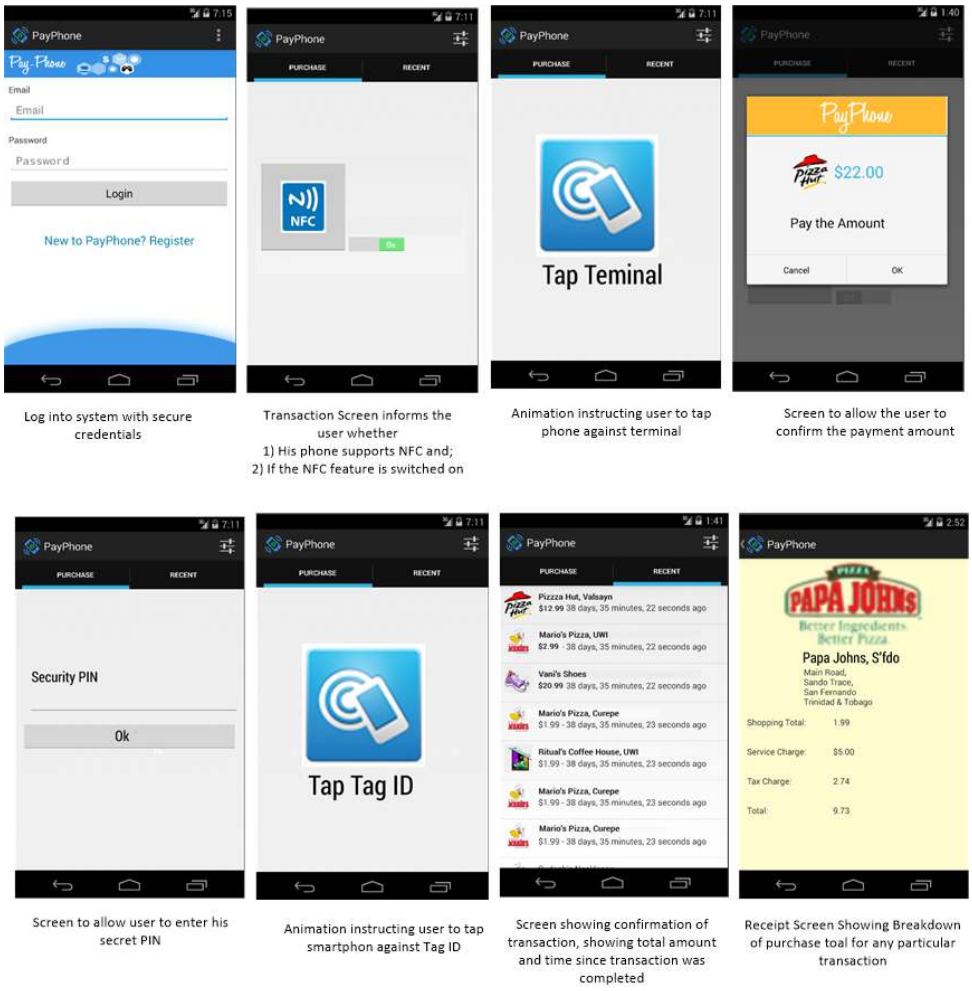


**Figure 3**: PayPhone Android Phone Application

## 4.2 NFC Terminal

The NFC terminal is not a novel technology. It is simply used to send transaction data to the customer's smartphone application. Once a merchant registers, their NFC terminal is programmed with their unique authentication token and other merchant details. The authentication token is sent along with the transaction amount to the customer's smartphone for

their confirmation. The NFC terminal is independent of any other components. Confirming or denying a transaction on the customer's part does not affect the functionality of the terminal.

## 4.3 Node.js

Node.js is a server-side JavaScript environment built on Google's V8 engine (Tilkov & Vinoski, 2010). It allows users to leverage the power of asynchronous programming to create complex but simple-to-manage, high performance network applications. Node.js uses Event-driven programming to handle I/O functionality. In contrast to most server-side implementations that make use of multi-threading techniques to handle multiple client connections, Node.js uses event-driven programming to handle multiple client connections and requests. One drawback of multi-threading is the risk of deadlocks and exploited shared resources. Node.js mitigates this by using event notifications to alert the application as to whether or not the event can be handled. The asynchronous implementation prevents blocking requests to the application. In the PayPhone system, where it is imperative that transactions are timely and efficient, there can be no room for deadlocks. The choice for the JavaScript based server-side environment was also made based on runtime comparisons with other common server-side implementations. Based on benchmark tests performed by Sopyło (2012), PHP applications perform slightly better than Node.js applications for a small number of requests (anywhere below ten thousand). However, once requests are drastically increased, Node.js outperforms PHP, handling more than 1 million requests in almost the same amount of time that PHP handles ten thousand.

The system takes full advantage of the Node.js asynchronous calls to load all the data related to a single customer and merchants in a timely fashion without blocking the server from other users. All requests are made to a MySQL database that stores user data. Node.js allows seamless integration with existing technologies such as No-SQL, relational and non-relational databases. Through the use of the sequelize.js, an Object-Relational Mapping (ORM) library, we use JavaScript to map MySQL database entries to objects and objects to database entries. This allows us to manipulate database entries as easily as we would objects within the Object-Oriented Programming (OOP) paradigm. Another benefit of the ORM comes from the execution of parameterized queries to aid in protection against malicious attacks such as SQL Injection. Input sent to ORM queries are sanitized for malicious code and executed safely or return errors.

### *4.1.1 Merchant Management & Administration System (MMAS)*

It is important to understand how the merchant is represented in the PayPhone system. A merchant is represented as a "Branch" of a "Retailer". When a merchant registers to use the PayPhone system, they do so as a Retailer and must register at least one Branch with which customers are to conduct business. Branches have no control over their setup and solely receive payments. This is important as it separates the transaction processing side of a merchant from the managerial side. In large companies that have many branches, the benefits are obvious; the main branch or corporate head does not deal directly with the customers but rather manage the accounts and other duties of the entire company. This model was adopted within the PayPhone system. Payments are made to the branches but the branches do not store any information on the overall business. They can merely access a list of transactions carried out. However, the main branch, or retailer, can see every branch, whether there is one or many, and view all transactions done by each singularly or totally. This design lends itself to implementations where branches do not store the vault keys on-site but at a remote location, usually the corporate head.

When a transaction is carried out at a merchant site (i.e. the branch) the data is sent to the PayPhone system. The necessary data is extracted to credit the *retailer* with the transaction amount and record the branch identification. The branches need to be in constant communication with the server so as to be updated of the completion of a transaction. If a transaction is not successful the branch is alerted to the failure and the reason. Again reasons may include insufficient funds in the customer's account. Once there is no error the branch and customer are simultaneously updated, with the branch receiving notifications through the use of Socket.io. Socket.io is a JavaScript library that provides an object interface for creating and using secure web sockets for broadcasting messages to one or more clients. Following the successful completion of a transaction, the MMAS is sent a notification prompting an addition to the current screen seen at the branch terminal. The socket.io was used mainly to allow seamless UI (User Interface) update without merchants having to ever refresh the page. A page refresh would simply load all successful transactions up to the point of the request which would include all those transactions sent by the socket.io. Figure 4 shows a system overview of how each component within the PayPhone system communicates.

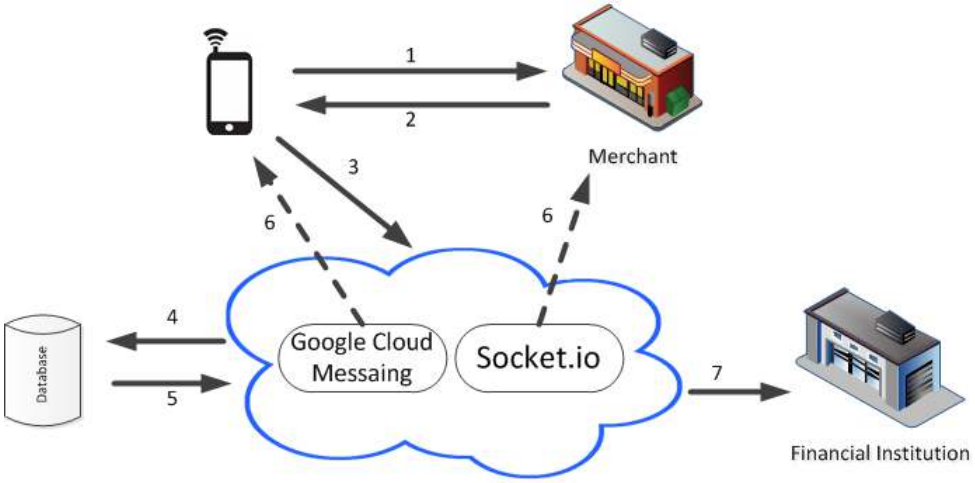


**Figure 4**: PayPhone System Overview

### *4.1.2 User Management & Administration System (UMAS)*

The UMAS allows users to monitor their transaction history, shutdown the application and other managerial tasks. The dashboard portion of the back-end system displays the user's transactions on a monthly basis. It also displays the percentage of money spent in relation to their set daily limit. There are several groupings that are configured for the user, namely their *Most Frequent Purchase Locations*, *Most Recent Purchases* and *Total Spent* at different merchants. These options allow the user to know which merchants are frequented the most, the purchases most recently made and the total amount spent at each specific merchant, respectively. A full history of their transactions is available for the user to keep track of their spending habits. The user can also manage their password, PIN and daily limit settings in a similar fashion as done on the mobile phone application. In the event that a customer's smartphone is lost or stolen, the backend component also provides an emergency button that allows the user to shut down their account to prevent unauthorized purchases.

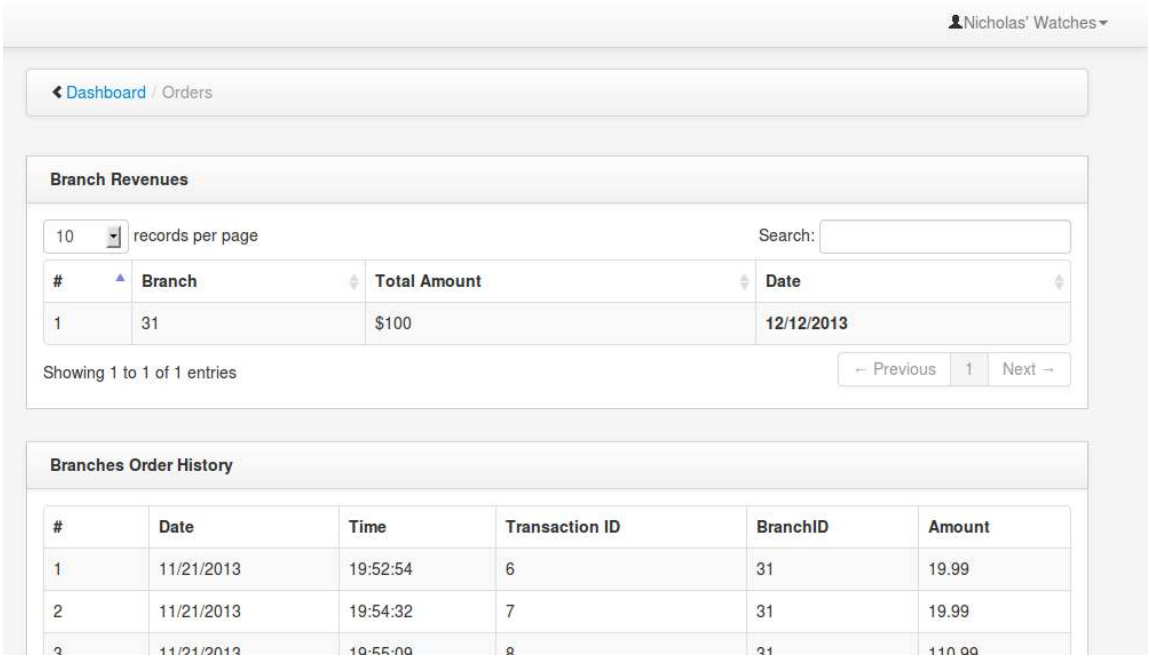


**Figure 5a**: PayPhone System Overview

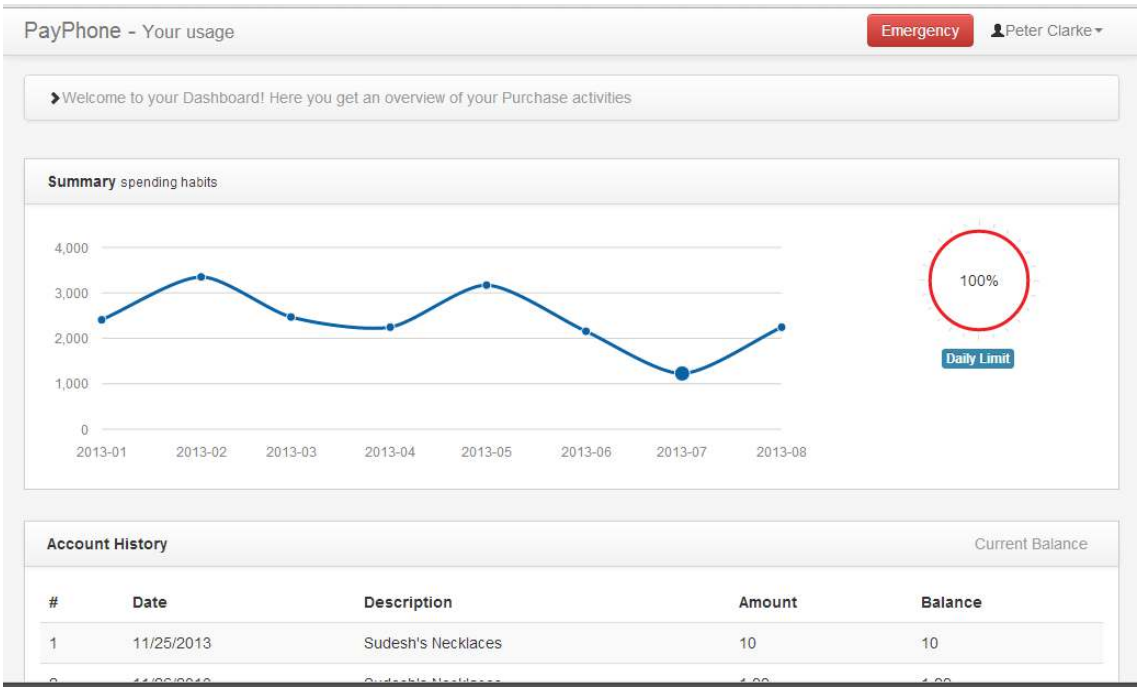


**Figure 5b**: PayPhone System Overview

Figure 5 shows both the UMAS and MMAS in operation. Figure 5a shows the UMAS part of the system. It shows the welcome screen that customers see upon logging in. This screen represents their account history for the month graphically and shows the remaining allowance if they set a Daily Limit restriction. The other parts of the system display a customer's transaction history and their user profile allowing them to reset their password and change address information and daily

limit as well as to deactivate their account. Figure 5b shows the MMAS part of the PayPhone system. It shows the retailer screen where the merchant has an overview of its branch activities: the amount of funds each branch has brought in for the day and the total amount since their creation. The other parts of the MMAS system allow the retailer to manage their branches. When branches log in all transactions carried out at this branch, sorted by date, are displayed.

# 5. Comparison between LINX, PayPhone and other systems

The LINX system is the only regionally operated debit-card based system in the Caribbean. The PayPhone system can provide faster transaction processing than LINX machines through the use of Wi-Fi and 4G customer data plans. The LINX system uses a dial-up connection to complete transactions between merchants and their banking institution as illustrated in Figure 3. To complete a transaction, the system must complete 7 different steps using an antiquated dial-up process. The PayPhone uses 4 steps with a much faster connection. Dial-up connections, even on dedicated lines still run at 56 kbps, as compared to 4G connections, which can range between 7-15 Mbps. A major fault with the LINX system is that most merchants do not have access to a separate dedicated line and so a transaction cannot be carried out while the line is in use. Based on 30 trials, it was found that the average time taken for a LINX transaction was 2.5 minutes.

Moreover, the PayPhone system is a truly low cost M-Commerce system. A truly low-cost system is inexpensive on both sides of a transaction, namely the merchant and the customer. It should not be costly for the merchant since such costs will be passed on to the consumer. The LINX system requires a monthly rental charge to be paid by the merchants and customers pay a fixed fee every time they swipe their card. The NFC terminal needed by the PayPhone system is inexpensive and is a one-time purchase. It does not need expensive rental fees. Customers also need not pay high swipe fees to complete a transaction, reducing the cost on both ends. Other systems (e.g., Google Wallet and ISIS) similar to PayPhone exist in developed countries. However, these systems have the financial backing and resources that are lacking in developed countries. The PayPhone system requires little start-up and maintenance costs.

# 6. Conclusion

Many developing countries are yet to realize the significant monetary gains obtainable through M-Commerce and micro-payment systems. The statistics presented by the ITU (2012) show an average mobile penetration rate of 123% across the Caribbean. This realization can speak volumes to the way in which the Caribbean conducts business. The current climate may not be conducive to the quick integration with current banking institutions. However, like Kenya with their M-Pesa payment system, PayPhone can provide a low cost alternative payment system for the Caribbean countries. This system makes full use of the NFC capabilities on smartphones to allow users to "tap-and-go" to make purchases thus removing the need for customers to keep wallets on hand. The PayPhone system can offer Caribbean nationals, and, in the future other developing countries, a truly low-cost cashless experience.

# *References*

Balan, R. K., Ramasubbu, N., Parakobphol, K., Christin, N. and Hong, J. (2009) "mFerio: the design and evaluation of a peer-to-peer mobile payment system*", Proceedings of the 7th International Conference on Mobile Systems, Applications and Services*, pp. 291-304

Central Bank of Trinidad & Tobago (2009) "The Payment System in Trinidad & Tobago", *Public Education Pamphlet Series*, October 2009

Eijman, F., Kendal, J. and Mas, I. (2010) "Bridges to Cash: The Retail End of M-Pesa", *Saving & Development*, (34) 2

Haselsteiner, E. and Breitfuss, K. (2006) "Security in Near Field Communication (NFC)", *Workshop on RFID Security*

IDC Corporate USA (2013), "Android Pushes Past 80% Market Share While Windows Phone Shipments Leap 156% Year Over Year in the Third Quarter", Retrieved from http://www.idc.com/getdoc.jsp?containerId=prUS24442013

InfoLinks Services Limited (2014), "About Us", from http://www.infolink.co.tt/aboutus.html

Jiajun C. and Adams, C. (2004) "Short-range Wireless Technologies with Mobile Payment Systems", *Proceedings of the 6th International Conference on Electronic Commerce*, pp. 649-656

Madlmayr, G., Kantner, C. and Grechenig, T. (2014) "Near Field Communication", *Secure Smart Embedded Devices, Platforms and Applications*, pp.351-367

Mbiti, I. and Weil, D. N. (2011) "Mobile Banking: The impact of M-Pesa in Kenya", *NBER Working Paper No. W17129*

Mulliner, C. (2009) "Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones", *International Conference on Availability, Reliability and Security*, pp. 695-700

National Entrepreneurship Development Company Limited (NEDCO) (2012), "General Information", Retrieved from http://www.nedco.gov.tt

Panjwani, S. and Cutrell, E. (2010) "Usably secure, low-cost authentication for mobile banking", *Proceedings of the Sixth Symposium on Usable Privacy and Security*

Schlöglhofer, R. and Sametinger, J. (2012) "Secure and Usable Authentication on Mobile Devices", *Processings of the Tenth International Conference on Advances in Mobile Computing & Multimedia*, pp.257-262

Tikov, S. and Vinoski, S. (2010) "Node.js: Using JavaScript to Build High-Performance Network Programs", *Internet Computing, IEEE*, (14)6, pp.80-83

Warman, M. (2013), "Mobile spending to double" *The Telegraph*, March 25. Retrieved December 17, 2013, from http://www.telegraph.co.uk/technology/news/9949610/Mobile-spending-to-double.html