IT SECURITY RELATED ISSUES AND CHALLENGES IN ELECTRONIC PAYMENT SYSTEM IN NEPAL: A STUDY FROM CUSTOMER'S PERSPECTIVE

Sandeep Dangol[1] and Dr. Sandeep Kautish[2]
[1] PG Scholar, Lord Buddha Education Foundation, Kathmandu, Nepal
[2] Dean (Academics), Lord Buddha Education Foundation, Kathmandu, Nepal

ABSTRACT

As the number of internet users grows exponentially, not only in developed countries but also in developing countries like Nepal, it has been adopted and used for multiple applications like e-government, e-learning as well as e-commerce. Many prior studies already found that e-commerce provides bunch of benefits such as flexibility and efficiency. However, along with the advantages, problems like frauds remains a serious threat. Recent reports and news are constantly reporting cases of fraud incidents with increasing victims and losses. These reports are likely to affect the trust of parties which are involved in e-commerce systems, particularly customers. Therefore, this study attempts to address this problem by investigating the presence of customer's trust, their perception towards vulnerability while using an e-payment system.

The study was undertaken in Nepal by surveying customers' perspectives of e-commerce transactions. Questionnaires were distributed through an online portal and total of 113 people responded which were later analyzed in SPSS. The result of this analysis showed age group, gender, education qualification makes a significant difference in performing the electronic payment. Moreover, the results also indicated the customer's perception towards the vulnerable are negatively influenced by the lack of enough security protocols. Consequently, the more information on or the more experience with cyber-fraud incidents customers have, the more likely they will not commit transactions in e-commerce.

Keywords

Internet, e-government, e-learning, e-commerce, frauds e-payment system, SPSS, security protocols, cyber-fraud.

1. INRODUCTION

The concept of commencing business electronically via online method is a very fast spreading field. It makes easier for purchasing and beneficial. The customer does not need to be physically present on the store, rather stay at home and buy goods from almost all over the world. This also facilitates various merchants around the globe to sell their products (Raziq, et al., 2011). The appearance of this advancement in global business platform triggered almost every business house to convert to electronic payment from physical cash, known as e-payment system. This electronic system can be used for buying products or services and paying via internet (Roy & Sinha, 2014) (Kabir, et al., 2015).

Payment industry refers to the medium for the payment through which transactional payment is done, nationally as well as internationally. The idea of exchanging products though payment was introduced since the dawn of the evolution. Money has various shapes, exchanging goods with goods, from paper money to plastic, from bank accounts to electronic accounts. These payment methods have evolved from various shapes and size, varying from traditional exchange system, to taken based, to bank accounts and deposit to cashless payment like plastic money (credit or debit cards, electronic wallets, etc.) (gomedici.com, 2018).

In this ever-growing world of technology, everything is changing. So is payment gateway industry. People are starting to pay via their cards more often than before which results in the growth of new

providers, new platforms and new payment tools. Most of the companies usually adopt the on-site datacenter which results in poor service in compare to the data center in cloud.

An e-payment system (EPS) is the process of paying for goods and services through an electronic medium, without the use of physical checks or cash. In other words, paying electronically is consider as an electronic payment system or online payment system.
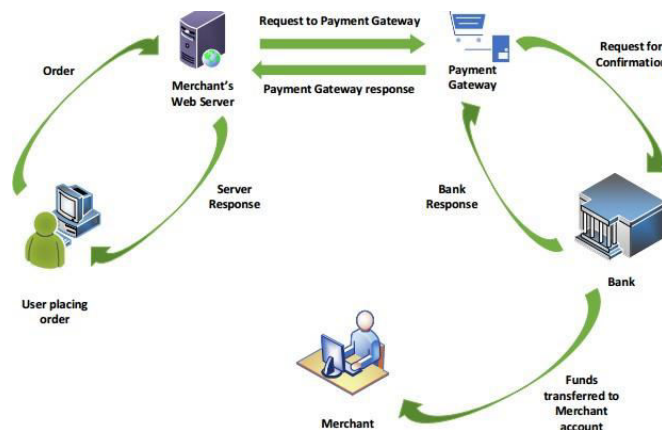

Figure 1. Workflow of existing standard online Payment Gateway (source: (Khan, et al., 2017))

The issue bank has customer's card details, such as account balance, name, address and other details like card verification value, expiry date which are not visible to the payment network expect the issuer bank. In settle process, which is usually last step for the payment, the issuer bank deposits the transaction amount to the respective merchant's bank account. Since the transaction happens online, merchant will be completely unaware whether card is used or not. Hence, security is completely dependent on the customer using valid card data. The electronic payment system has grown gradually over the last decades due to the fast growing spread of internet-based banking application and shopping. Since shopping online is convenient, most users just browse the products and order and pay electronically. As the world advances more with technological development, we can see the rise of electronic payment systems and payment processing devices such as POS machines in different outlets, QR code to pay via mobile application, etc. The usage of physical cash can be somewhat low in compare to online payment, as it provides more secure transaction along with various benefits. Generally, when we think of electronic payment, we refer to as normal transaction commenced via internet. However, there is a lot more than that. Since the usage of electronic transaction is increasing, usage of physical cash and checks are gradually decreasing. As a result, users are more and more people are attracted towards the facility and convenience e payment provides (URS, 2015).

E-finance and e-commerce along with electronic payment is one of the major issues and challenges in the competitive and global economy. These technologies are considered one of the most important reasons for increasing the competitive advantage in the global economy. Organizations are thus seeking to increase information trading and electronic payment and to increase the means of transactions between exchange partners (suppliers and customers) (Camenisch, et al., 2015). Debit and credit cards can be easily considered as one of the most popularly used electronic based payment method. Alternate way to plastic money can be internet banking, mobile banking, electronic wallets (SecurionPay, 2018). In case of Nepal, third party application like Esewa and Khalti are also popular. In general, EPS can be classified into five which are listed below:

1. Electronic cash: Transactions are resolved through electronic currency exchange.

2. Pre-paid card: The card has a pre pain amount already loaded. Customers use this

card for a specified amount by making an entry. The amount is then decreased as the transaction progresses.

3. Credit cards: The payment system is responsible for maintaining the credit card transaction and sends a bulk transactional information at the end of the month to the bank. Bank then forwards the information to its customer. The customer is then mailed the overall expenses over the month after which the cardholder pays the balance to the bank.

4. Debit cards: Normal ATM card can also be used by swiping in the POS machines or registering into the online shopping. The amount decreased as the transaction progressed

5. Electronic checks: The payment gateway is responsible for settling the transactions between the buyer's bank, issuing bank and the sellers bank, acquirer bank in the form of an electronic check.

6. ATM: Physical cash is withdrawn from an automated teller machine electronically.

7. Point-of-Sales: Generally referred as POS devices, used to pay the bills by either swiping the magnetic striped cards or reading the EMV based cards.

8. Financial Switch: Considered as the main mediator between the Core Banking System (CBS) and payment mechanism.

In context of Nepal, as per the report of Nepal Rastra Bank (NRB), the Central bank of Nepal, on April 2018, there are, currently, 28 class A registered commercial banks, 33 class B registered development banks, 25 class C registered finances companies, and around 65 class D micro finance financial institutions. Among them, all the commercial as well as development banks are using a payment gateway for their customers to withdraw or pay the amount. It can include ATM transactions, POS payments, card-less transactions like online shopping, etc.

Banks like Nepal Investment Bank Ltd (NIBL), Nabil Bank, Standard Chartered, Everest Bank, SBI Nepal, etc. are using their own financial switch which enables them to control and operate overall transactions. NIBL's switch is named as National Payment Network (NPN), under which some of banks like Kumari Bank Ltd, Mega Bank Ltd, Sanima Bank Ltd. Tourism Dev. Bank ltd, etc. are performing their transactions. Other banks like NIC ASIA, Machhapuchhre Bank, Bank of Kathmandu, Citizens International, etc. are using a third-party switch operator called Nepal Electronic Payment Systems Ltd. (NEPS), which are powered by those commercial banks. NEPS is responsible for ATM, POS, Card-less transaction for those banks which are using its service. Furthermore, the NPN network as well as NEPS should be PCI DSS (Payment Card Industry Data Security Standard) in order to fully utilize its system and be secure. Moreover, the banks like Everest and SBI Nepal which operates with a joint venture with Indian Banks, directly operates and are maintain from India as well. The payment gateway is responsible for all the transaction back and forth from any banks, along with the participation in VISA or Mastercard or UnionPay International (UPI) for interbank transactions on both ATM and POS.

The Rastra Bank of Nepal is taking a strategic approach to reforming Nepal's payment system. Overall financial infrastructure along with individual projects of various banks are also affected if proper payment system regulation is not formed. As a result, national economy could also be affected. The future of Nepal's electronic payment system could be jeopardized if National Payments System (NPS) strategy is not formed and deployed by the central bank. The country's payment industry could provide uncertain results (NRB, 2016).

1.1. Problem Context

The flexibility provided by online purchasing and e-payment has various unseen authentication and authorization problems that lingers in each transaction. Despite various security standards, sending customer's payment information to a payment gateway via merchant in an unprotected line is one of the main reasons for customer data theft and breaches. When performing the transaction through a merchant, customers are required to enter their name, card number, expiry date, CVV value, issuer bank name. Even if the data are encrypted, merchant can decrypt the data.

1.2. Research Questions

- What are the factors associated with the perception of the customer?

- What are the possible factors causing threats to EPS in Nepal?

- What are the vulnerabilities in electronic payment system?

- How much secure the customer thinks about paying electronically?

1.3. Purpose of the Study

The main purpose of this study is to find what the users of electronic payment thinks about the security and usefulness of payment via electronic methods. Moreover, this research is more focused on customers perception, challenges on security vulnerabilities and adopting as well as accepting the e payment.

1.4. Scope and Significance of the Study

The scope of this research is to ensure the awareness of various types of transaction and their weaknesses and how to overcome those weaknesses by adapting suitable protocols. Appropriate solutions can include use of a One-time password, proper encryption algorithm, use of virtual private networks, etc.

2. THE LITERATURE REVIEW

Literature review provides an insight to a particular field of study through the work of past researchers on the same field. The term "electronic payment" is referred as convenient methods for payment by electronic means such as card, the Internet, or Electronic Fund Transfer. Electronic payment gives consumers an alternate way of paying. The main purpose of implementing electronic payment system is to promote the cashless payment process. Since developing countries like Nepal is still climbing in the technology enhancement, technology and its new innovative capability has put forward the important tools to electronic payments and settlement system (Giri, 2013).

Currently, the fund transfer mechanism needs to be efficiently maintained in order to cover larger network of rural people and their old way of transaction. Since the capital and financial market is growing, payment system's utmost priority should be given. To go hand in hand with the country's increasing financial center, strong and stable payment system need to be built. The current payment system does not have much security standards in compare to what it needs. People's data and money are at stake and vulnerable in every transaction. That is why, Nepal needs to develop an efficient and secure payment system to regulate and smooth out all the electronic payment mechanism in the country and help mitigate the issues concerned with the payment system by both small businesses and consumers in the economy (Giri, 2013).

A safe, reliable, secure and efficient payment system will enhance the economic growth along with boosting growth of small and medium enterprises. Strengthening the legal and regulatory framework is, therefore, the key medium in order to support introduction and adoption of innovative payment products in both urban and rural markets. Mobile banking on the other hand, plays much less role in the e payment in the context of Nepal as 70% of Nepalese households are unbanked. Due to people still relying on traditional banking system, survey questions like the status of Nepalese customers with mobile banking will be extremely helpful to know the popularity of mobile banking services along with the ratio of Nepalese people getting along with the modern technologies in sense of financial activities (Sherpa, 2015).

According to Hitesh Malviya, a security researcher and evangelist from India, has stated, one of the reasons for vulnerabilities and problems in the web based payment transaction is the fact that web application developers are often not very well familiar with techniques to secure the web application (Malviya, 2017).
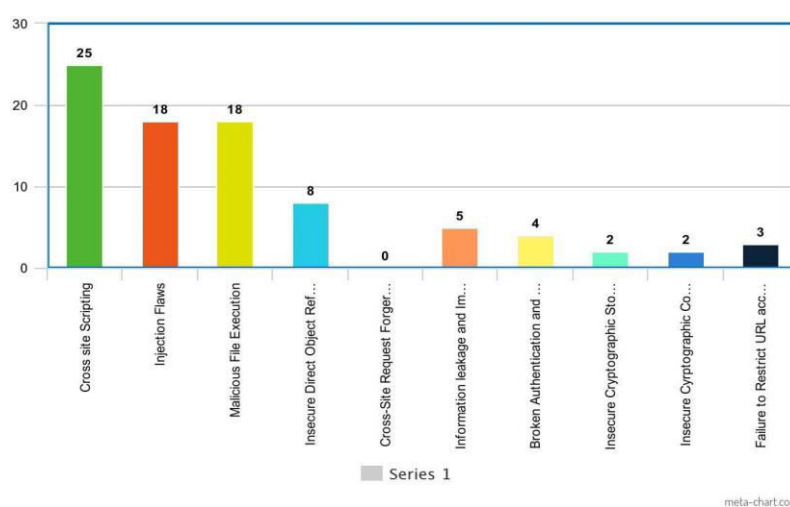

Figure 2. Ratio of Vulnerabilities (source ((Malviya, 2017))

In the online shopping sites, SQL injection, where a query is inserted with the user input so that the user will run the query in the back end without user's consent. Once the site's vulnerable-ness and loopholes are identified, attackers send a single quote (') character in order for the query to be executed (Malviya, 2017). Most executed vulnerable on an online site be cross-site scripting. Generally, known as XSS, it is a common type of vulnerability found in web application. The attacker can easily gain access on the cookies and cache data on the web site. These data can be analyzed which can extract information like login information of the users. It is a client-side attack where an attacker can add his own contents in the web page by forcing the vulnerabilities from the client side. Followed by the execution of malicious file by the users without any knowledge whatsoever. The attacker sends file in such a way where users are prompted and are manipulated to click on the link or open an attachment.

Payment delivery channels such as ATM, internet banking, mobile banking is subject to monetary loss and have increased the risk of financial loss and electronic frauds (Kautish et al, 2008, 2012, 2013, 2020) along with other banking risks. Not only technology risk is concerned with operation risk of the bank, other banking risks like credit risk, reputation risk, compliance risk, market risk, strategic risk are also increased due to it (NRB, 2016).

Moreover, Nepal Rastra Bank (NRB) has formed and issued certain set of Information Security rules regarding the usage of an electronic payment systems by Banks and their roles in the customer's awareness. Strong information flow along with information processing capability is crucial to

achieve business goals and for managing risk prudently in banks. For the information to be securely stored, accuracy, integrity, consistency, completeness, validity, timeliness, accessibility, usability and auditability should be properly maintained. To achieve these qualities of data, banks should develop and maintain comprehensive information security program (NRB, 2012).

- Banks must conduct annual asset risk assessment. This includes the update of devices that meets the End of Life period. This could affect the confidentiality, integrity and accountability of the information of the bank.
- The system activities should be properly monitored and logged. Any access grant permission should be approved by higher information authority.
- Proper installation of high-end firewalls should be installed in both outgoing and incoming sites. Employee with privilege access such as system administrator, security officer or officer of other critical system should be monitored with additional screening process such as background check, credit check etc. should be done.
- Payment Gateway used by respective bank should be PCI DSS complaint. The POS terminals should also be replaced with non-PIN based terminals for extra security.
- Two factor authentications should be enabled in each transaction to the customers and be notified with email or SMS or calls.

Customers has the easiness to conduct banking without physically being presented in the bank with the introduction of electronic delivery channels. However, this easiness has intensified the challenges and issues regarding data theft and breaches. Authentication and authorization of valid data from the customers. The security concerns regarding the electronic payment systems are constantly changing, as the security threats are evolving. Viruses and trojan are always trying to invade the system via mails or downloaded file which can disrupt the communication channels.

3. Methodology

The Quantitative Research Methodology will be implemented in this research. The Quantitative Research Methodology is the research method which deals with number and anything that is measurable by their research process.

3.1. Aims and Objectives

The aim of this study is to find what the users of electronic payment thinks about the security and usefulness of payment via electronic methods. Moreover, this research is more focused on customers perception, challenges on security vulnerabilities and adopting as well as accepting the e payment.

The objective of this research is:

- To investigate the vulnerabilities, present in the E payment system.
- To determine the factors associated with the perception of individuals in E payment system.
- To evaluate the aspects causing threats to EPS in Nepal.

3.2. Scope of Research

This study attempts to collect the data on an e payments user's perception and the security flaws they felt while doing the transactions. Transactions from consumers, business houses, bankers, etc. are included in the statistics gathered. Data has been gathered in the area of Electronic payment options used by buyers of goods and services, including point-of-sale, ATM, online payment as well as mobile banking.

3.3. Sampling

All the respondents selected for the study were e payment individuals and processors. Since the study is on IT security issues and challenges (Kautish et al, 2016, 2018, 2019) based on consumers' perception and their experience while performing transaction, the data collection was only limited on the consumers. As mentioned in the literature review and introduction, there are about 28 commercial banks in Nepal. And all the banks provide e payment facility to its customers.

3.4. Research approach

During the research tenure, characteristics of topic, its objectives, research questions, time located should be considered. The IT security issues and challenges in electronic payment in context of Nepal is a complex topic, since e payment is just blooming in the country. Lots of security flaws are presented, due to which cyber threats and hacks can be easily performed.

The study mostly based on primary sources conducted via questionnaire and partially based on secondary sources. Primary data included questionnaires. Secondary data source included journals, internet reports, etc. This research originates from the mail question, to what extent the customer feels about the security concern to use electronic payment. To address this question, a set of questionnaires were developed to answer the research questions and meet the objectives. Data are collected from the respondents through online survey. SPSS (Statistical Package for the Social Sciences) tool was applied to analyze and test the model. The application is mainly used for analyzing all sorts of data.

To find the frequency and total usage of e payment method by the customers, frequencies from descriptive statistics has been applied which provides total percent among the respondents. Since the data contained variables like gender, profession, education qualification, age group, various descriptive statistics frequencies have been applied along with pie chart for diagrammatic presentation of data. For the data comparison of perception between various age groups, profession, education qualification, one-way ANOVA has been applied. Since the variables in the questions were more than two independent(unrelated) groups. For the mean difference between the perception of the users and age group, profession and educational qualification, the ANOVA one-way test is used. However, the data for the gender is only in two variables. Since the population means will probably differ a little bit but not too much. Thus, for comparing the mean significance between perception and gender, independent sample T test is applied.

3.5. Data Collection Method

As the main objective of this research were to collect the data from the users themselves, certain set of questionnaires were made and distributed. The questions circled on the difficulties the user faced and any sort of vulnerabilities presented in the electronic paying process. A set of Likert as well as other questions were prepared from the customer's perception. It was mainly focused on the users who are consistently involved in the e payment process. Conclusions and recommendation are finalized from the data collected from the questionnaire after interpreting. Based on the current electronic payment system in the country, a revised framework has been suggested to reduce the threats and vulnerabilities.

4. DATA ANALYSIS AND REQUIREMENT VALIDATION

4.1. Frequency of usage of Payment Method

The table shows that, out of all the questionnaire asked, every respondent one used electronic payment. The questions were set and distributed to a set of both male and female respondents, where everyone was using some sort of electronic payment method alternate to cash. Those payment could include ATM machines, POS machines, mobile banking, internet banking or online purchase.
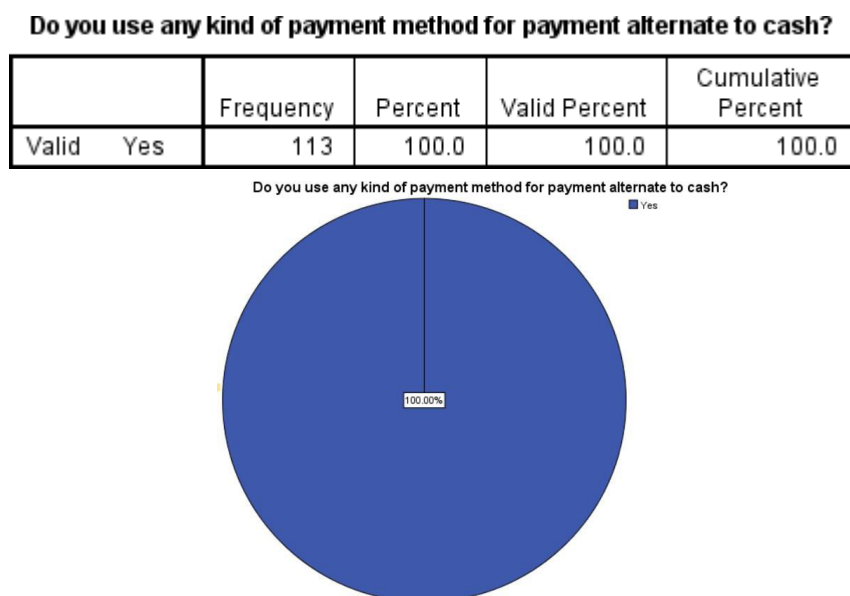
Do you use any kind of payment method for payment alternate to cash?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	113	100.0	100.0	100.0

Figure 3. Usage of E payment method

4.2. Frequency of usage of ATM

ATM or Automated Teller Machine is one of the convenient ways to get money, without using any kind of paper-based withdrawal process. Out of total 113 respondents, majority of people, 86, to be precise, uses ATM facility. While the other 27 respondents do not u se ATM.
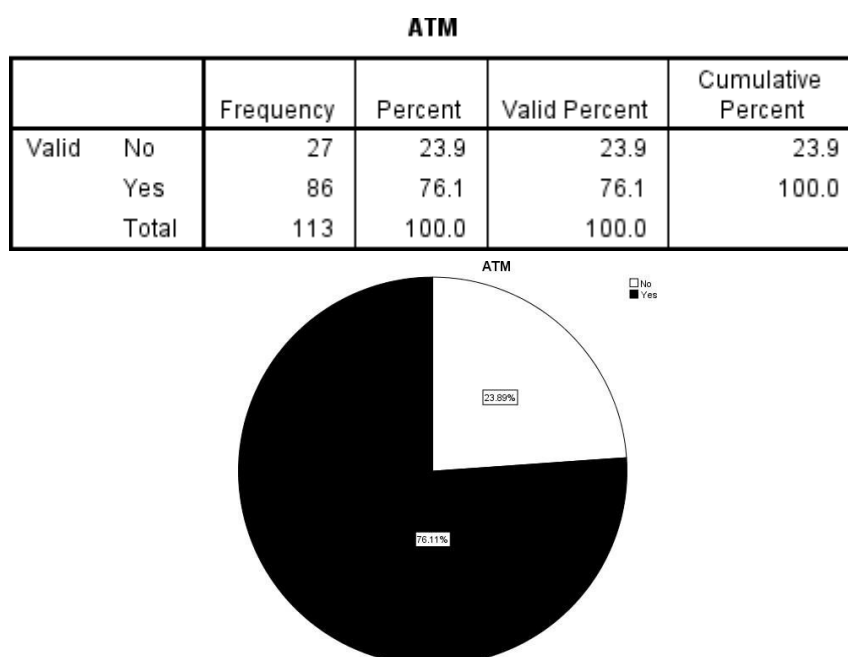
ATM

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	27	23.9	23.9	23.9
	Yes	86	76.1	76.1	100.0
	Total	113	100.0	100.0	

Figure 2. Usage of ATM

4.3. Frequency of usage of Mobile Banking

Mobile Banking application can also be used for various transaction. User just have to use the application of respective bank. These applications nowadays provide various features like mobile top up, Q pay etc. Out of 113 respondents, majority of the people, 67 to be precise, used mobile banking application for their transactions.
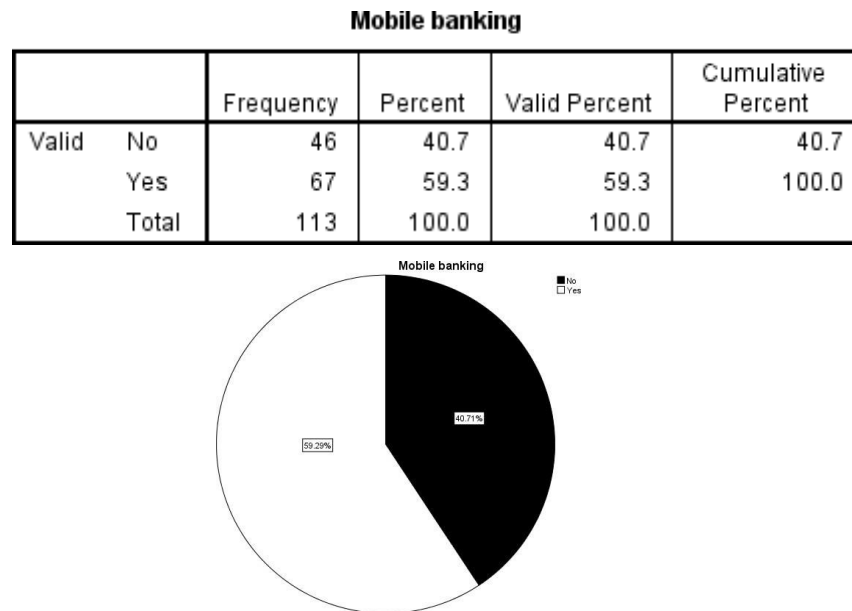
Mobile banking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	46	40.7	40.7	40.7
	Yes	67	59.3	59.3	100.0
	Total	113	100.0	100.0	

Figure 5. Usage of Mobile Banking

4.4. Frequency of usage of Internet Banking

Alternate to mobile banking, Internet banking also acts like a similar kind of online platform where one can perform transactions. It can be used to transfer funds, calculate interests, mobile top up, etc. Out of 113 respondents, 49% of respondents uses internet banking, while other 64% of respondents do not use it.
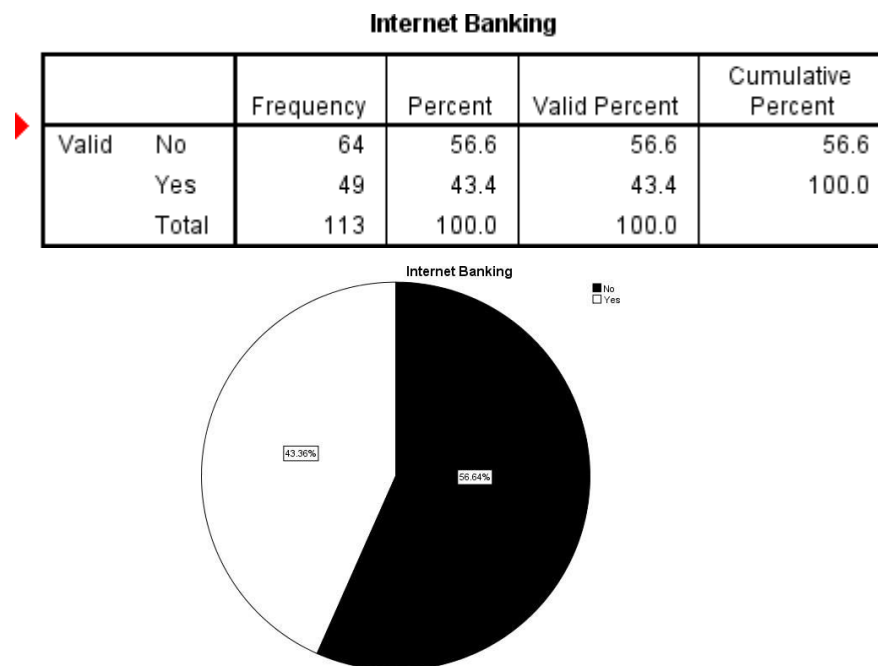
Internet Banking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	64	56.6	56.6	56.6
	Yes	49	43.4	43.4	100.0
	Total	113	100.0	100.0	

Figure 6. Usage of Internet Banking

4.5. Frequency of usage of Point of Sales (POS)

The chart shows the number of respondents that uses POS (Point of Sales) devices. It is an alternate method to for paying in restaurant or shopping. The number of people who uses POS device are about 34 out of total respondents while other 79 does not.

Point of Sales

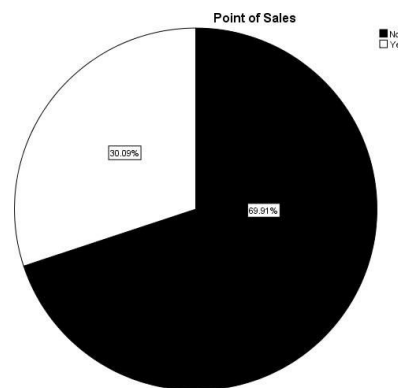|		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	79	69.9	69.9	69.9
	Yes	34	30.1	30.1	100.0
	Total	113	100.0	100.0	

Figure 7. Usage of POS Machine

4.6. Frequency of Vulnerability Distribution I

Among all the respondents, majority of the e payment users didn't faced difficulties, while other did. The difficulties can also be considered as a kind of vulnerabilities, since the users found suspicious transaction types while performing or after the transaction.

Have you face any kind of difficulties while performing any transactions?

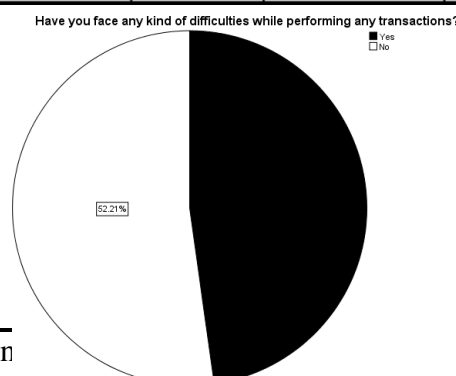|		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	54	47.8	47.8	47.8
	No	59	52.2	52.2	100.0
	Total	113	100.0	100.0	

Figure 8. Ratio for Difficulties while Performing Transaction

4.7. Frequency of Vulnerability Distribution II

One of the suspicious attempts while performing transaction can be considered as sudden PIN change prompt. About a quarter of the respondents faced this problem. This problem can be faced while performing transaction at the ATM. Fraudulent attempt could be launch by the hackers, and critical information like Personal Identifiable Number or PIN number along with personal information and money could easily be lost.

Sudden PIN change prompt

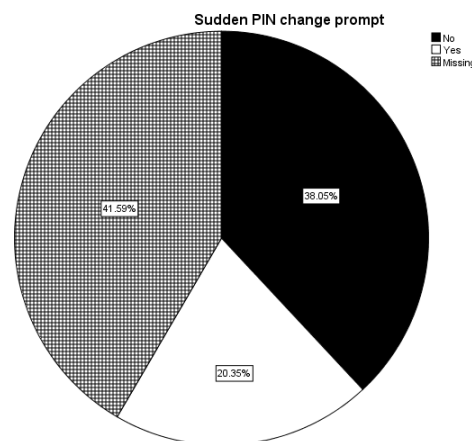|		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	43	38.1	65.2	65.2
	Yes	23	20.4	34.8	100.0
	Total	66	58.4	100.0	
Missing	System	47	41.6		
Total		113	100.0		

Figure 9. Ratio for Sudden PIN change Prompt

4.8. Frequency of Vulnerability Distribution III

This could be treated as a malicious web content that pops up frequently, mainly stating to enter the card number to win exciting prizes. These kinds of advertisements are considered as fake and do not contain genuine information. This is a pop up rather than a problem. When surfing through an online shopping portal, some of the users faced a pop-up stating, 'You have just won a lottery, enter your credit card number'. It's a phishing technique and could cause people to lose their information including money. Among the respondents, only a handful has faced that kind of pop up. Majority of people has not faced the pop.

Pop up stating 'enter your card number to win lottery'

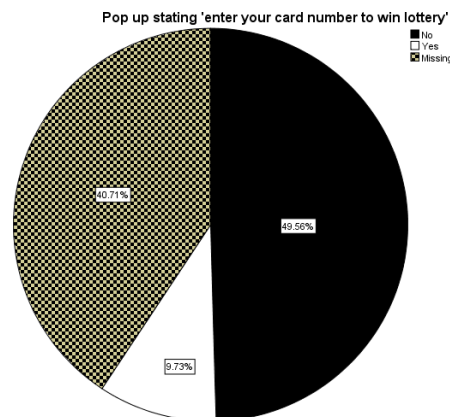|		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	56	49.6	83.6	83.6
	Yes	11	9.7	16.4	100.0
	Total	67	59.3	100.0	
Missing	System	46	40.7		
Total		113	100.0		

Figure 10. Ratio for Pop up

5. DISCUSSION AND CONCLUSION

5.1. Demographic Analysis

In this study, the number of male respondents is more than females. In addition, the fewer number of female participants than males may reflect actual e-commerce users. In online usage and purchases, or usage of cards, males dominate. In relation to age group, young ages dominate respondents of this survey. The study shows that younger people are more likely to respond to online surveys. Moreover, the people within age group of 20-40 are actively participating in e payment transaction. This may also reflect the degree of e-commerce engagement.

Besides, a typical electronic payment user being male, they have the following characteristics:

- Aged between 20-40 years old
- With a college degree
- Engage in a profession

When asked about the insecurity and vulnerabilities, majority of the respondents felt the insufficient security, user unawareness, etc. are the main factors causing the data and information loss.

5.2. Challenges and Issues on E Payment System

Poor and inadequate legal and regulatory framework for the e payment system is one of the main problems and challenges for the adoption of e payment system and to run smoothly. Poor infrastructure and lack of user awareness on the other hand also plays vital role for the e payment threats and vulnerabilities. Moreover, majority of respondents also felt lack of security and poor precautionary advice is another reason for the problems in e payment system. Being one of the underdeveloped countries in the globe with only handful of ICT experts and its development being the slowest, its components in the field of electronic and online payment are also not satisfactory. In

such environment, security and privacy issues are always a concern regarding the risks of criminal attacks and monetary loss (Lim Choon Seng, 2014).

Some threats or problems includes:

- Low customer awareness about the procedures of electronic money.

- Lack of proper legal provision regulating the electronic payment system

- Lack of proper privacy concerns.

- Proper validation of e-signatures.

5.2.1. General Legal Issue

No proper regulation and efficient law have been formed to overcome the legal part and problem of electronic payments in Nepal. As the problem persist, central bank of Nepal is pressurized and placed it as high priority in its recent monetary policy published paper. Moreover, a legal framework has also been stated to be formed and applied soon to streamline the modes of electronic and online payment in Nepal (NRB, 2016).

5.2.2. Relevant Security Issue

The Nepal Rastra Bank and its Bank Supervision Department and Financial Institutions Supervision Department does not have any kind of security regulation for evaluating the appropriateness of current security features of electronic payments. For any kind of security related issues and challenges, the central bank should be able to tackle and have counter measures. Due to insufficient security regulation and framework, banks and financial institutions often procure the solutions on their own from suppliers. Most ATMs are run by third party service providers like NEPS or SCT, or the bank itself in some cases. Since the bank must be dependent on the service provider, they should be properly compliance and secure.

5.2.3. Lack of Usability

For the users to use electronic payment modes, they should also be familiar with the process, its UI, or the they could abandon the transaction. Most of the information is generated from the end users. So, if it is difficult for the users, then, there is no point of the payment method. For example, paying via credit card from a website could be difficult, since the system needs large amount of valid data to be entered. Thus, the users must be given as simple interface as possible for them to use efficiently. From the questionnaire, it can be said that majority of the respondents could feel the difficulty they face while performing transaction. One of the examples can be that they are redirected to several pages before checking out, which could lead them to discard the card and abandon the purchase.

5.2.4. Provider Issue

The issue regarding the provider of ICT solution in banking and financial sector should be properly addressed. They should be properly compliance for the vulnerability to be minimized. In current case of Nepal, third party service providers like SCT and NEPS are providing the service as a payment gateway. If these providers are not functioning properly or are not compliance, then the service receiver is automatically vulnerable since their Core Banking System (CBS) is the one the provider communicates. So, majority of the respondents felt lack of compliance, lack of proper precautionary advice is extremely necessary in order to properly secure the payment system. The operation of e payment system in Nepal, as of date is based on confidence in the system provider (Lim Choon Seng, 2014).

5.2.5. Lack of Security

Since online payment requires substantial amount of information from the user, it can be an easy target for staling that information along with monetary subject. Customers must provide detail information about credit card and payment account and other personal information online. Such kind of data, if transferred in an insecure line, could be easily hacked and misinterpret. Maximum number of respondents are concern about the security procedure included in the payment eco system. From the time the data is entered, to the time data is stored, is the most vulnerable, since the data is flowing from one server to another server. At that time, if enough security protocol and encryption is not used, the data can get intercept, as a result, customer's crucial information such as bank account information, their monetary information, etc. can be easily revealed. Due to lack of proper security, users faced various difficulties like suspicious transaction and phishing sites, cash deduction without withdrawing, etc. About 67 % felt the same.

5.2.6. Payment System Issue

The concept of electronic money is just starting to bloom in the context of Nepal. Only credit and debit card were used as a form of plastic money. The Nepal Rastra Bank should develop a mechanism to address the development of a payment system in electronic mode and inter-operability of various cards in use for making payments. The payment system industry consists of such system which needs to be regularly monitored and up to date. The PCI DSS compliance also contains system hardening, which provides the benchmark for the system to be secure at some point. So, for the system to run smoothly, compliance like PCI DSS and continuous monitoring should be done.

5.3. Factors causing problems on customer's perception

According to (Abrazhevich, 2001) , consumers' perception of electronic payment is highly dependent on user's attitudes and therefore has a significant impact on their acceptance. Further, he also confirmed that consumers will adopt new services only if it has identifiable impact as they had the same experience before. Customer's attitude towards the e payment system is assess in this study in terms of perception as it is more efficient than traditional payment systems, can be easily used, and is more secure and trusted.

5.3.1. Technical & transaction procedures in E-Payment

According to (Hwang, et al., 2007), technical and transaction procedures are the special mechanisms employed by EPS to successfully fulfill an electronic transaction. The procedures should ensure proper security and privacy of user information and actions, in order to promote customers' perceived trust. In this category, we consider factors related to technical protections such as integrity, privacy and stability.

This can include user awareness for them to use the e payment properly. They should be able to understand the technical ways to use them. If they suspect anything suspicious, then they should be able to identify, whether it is technical or not. They should be familiar with the procedures.

5.3.2. Security guidelines in E-Payment

The security plays the most vital role in the perception of the user. They should feel secure while performing the transaction. The data they sent should be protected and encrypted which results in safe transaction. The security concerns and guidelines for the user's dos and don'ts are among the critical factors that influence customers to use electronic payment (Mukherjee & Nath, 2003).

By making people aware and understand the security factors and measures, electronic payment systems can take a leap towards gaining customer's trust (Lim, 2008).

Maximum number of respondents are concern about the security procedure included in the payment eco system. From the time the data is entered, to the time data is stored, is the most vulnerable, since the data is flowing from one server to another server. At that time, if enough security protocol and encryption is not used, the data can get intercept, as a result, customer's crucial information such as bank account information, their monetary information, etc. can be easily revealed. Due to lack of proper security, users faced various difficulties like suspicious transaction and phishing sites, cash deduction without withdrawing, etc. About 67 % of the respondents felt lack of proper security is one of the main reasons for data and information breach and theft.

5.3.3. Usability in EPS

Adaptation of an e payment system relies (Rani and Kautish, 2018) (Kaur and & Kautish, 2019) heavily on the perception of the users, their abilities to understand the application, skills, etc. Since lots of users still lack professional understanding of the payment system, and various usage and services, they can be reluctant to perform transaction electronically, which results in decreased level of trust and security. According to (Mashayeshi & Mashayeki, 2016) complexity of the processes in EPS as perceived by the customers, can negatively affect the trust of customers to these systems. (Ankara, 2002) states that, the some of the psychological factors from the perspectives of customer can also control the level of trust including usability, reliability, availability, confidentiality and safety. Perceived ease of use has a positive influence on intentions to transact (Sanayei & Noroozi, 2009).

The customers must understand and be familiar with the ease of use of technology for them to use it (Curran & Meuter, 2005). Furthermore, experience will lead to faster adoption and consumption of new technologies. If the users have prior experience with same kind of technology, they are more likely to get more comfortable using similar but new technology. Since previous experience helps in building trust but is negatively related with the concerns regarding the security of e payment. As a result, customers with prior experience in these systems will trust and perceive them as a secure way of completing transactions.

5.4.   Research Questions

5.4.1. Research Question 1

What are the factors associated with the perception of the customer?
One of the main factors associated with the customer's perception includes their trust. It is the main factor that drives the e payment system. Likewise, the experience is also drive by trust. The system's trustworthiness is directly related to the consumer decision. It is as (Kniberg, 2002) stated, the users and merchants are more likely to use an insecure payment system from a trusted provider, than a secure system from untrusted company. For the adoption of e payment, trust and risk plays significant role. As e payment is carried out via internet, human interaction is almost zero which results to having lack of trust and high risk of fraudulent attempts.

Moreover, (Kim & Prabhakar, 2004) also states trust is extremely essential to mitigate the uncertainty of financial transactions to induce the customer to use it.

Likewise, the concern for security, useableness, technical procedures are also important factors that influence the perception of customers towards the E payment system. The perception of customers towards the usage of e payment can differ. From most users being at age group between 20 to 40. Profession does not vary the usage whereas the education qualification and gender played a significant role in the e payment method usage.

5.4.2. Research Question 2

What are the possible factors causing threats to EPS in Nepal?

The first and foremost factor causing threats, according to the users is insufficient security. Security can be classified into three areas: system, legal, and transaction. For this reason, e-payment can only be deemed as confidential when all phases of the transaction process are able to satisfy users' needs. This could also affect adoption of e payment in the future.

Similarly, user unawareness could also pose serious threats to the e payment. If the users are not familiar with the do's and don'ts, it can be serious issue. Among all the 113 respondents, majority of people thinks user awareness can be considered as possible factors causing threat to e payment. Moreover, the proper compliance such as PCI DSS (Pin Card Industry Data Security Standard) must be compliance. The compliance includes security benchmark, which should be fulfilled in order to smoothly run the system. Customer's trust will also increase if the system is compliance. Majority of the respondents, 69% to be precise, also felt that lack of proper compliance can also cause problems in the e payment system. The lack of security precautionary advice can also lead to problems like security breaches and data theft.

5.4.3. Research Question 3

What are the vulnerabilities in electronic payment system?

The major vulnerabilities in the e payment system are originated from the threats and problems and issues like lack of proper advice to the users, lack of awareness training, etc. The major breaches and hacks are originated from the users themselves. Due to unawareness and lack of precautionary advice, they might as well be hypnotized by the fake advertises. Due to these, major problems like hack and data breaches occur.

5.4.4. Research Question 4

How much secure the customer thinks about paying electronically?

The system should be secure enough for the data that customer transfer from the merchant to appropriate payment gateway. Majority of customer does not feel safe in the online payment world as there are too much problems and news related to data theft and breaches. In such case, the payment gateway should secure their system and gain trust of their customer's by implementing flawless system.

5.5.   Research Objectives

5.5.1. Research Objective 1

To investigate the vulnerabilities, present in the E payment system.

From the questionnaire distributed, majority of respondents, about 52%, had faced some kinds of difficulties. Suspicious problems like sudden PIN change prompt in the middle of transaction can be quite troublesome for the customers. Likewise, pop ups while online shopping could also irritate the user's which requests for the card number. It can even result in abandoning the shopping. Moreover, the customers can get suspicious if their money gets deducted without withdrawing. About 33% respondents faced the problem.

5.5.2. Research objective 2

To investigate the factors associated with the perception of individuals in E payment system.

The perception of everyone differs from one another. In the study, variable perception has been grouped into and then compared to the different components. Male ratio counted higher than female. Moreover, perception with gender group showed significance value being lower than 0.05

which resulted in significant difference between mean of perception between male and female. From the profession perception, there was no significant difference between the perception and profession since the significance value is 0.056 which is more than 0.05. This means, e payment is used by all individuals engaged in any kind of profession.

Similarly, in the age group, there was high level of significance, value being 0.000. Since majority of people fall between 20-40 age group. People between the age of 20 and 40 are the most active one to use e payment technology. Followed by the people between 40 to 60. Lastly, the factor education level also seemed to be highly significant, as most of the users hold bachelor's degree. Being most people of bachelor's degree, it can be concluded that, education level also differs the perception of people towards e payment usage.

5.5.3. Research objective 3

To evaluate the aspects causing threats to EPS in Nepal

Factors causing threats involve the lack of security in the system. Majority of respondents responded the same along with the user unawareness, proper compliance, lack of security precautionary advice. On top of that, the contents available online could be fake and might try to steal critical information from the users. So, only genuine contents with valid evidence of identity of the owner should be trusted. Majority of responded felt that no evidence of identity of owner is also one of the main reasons and threat to consumer online.

5.6.   Conclusion and Recommendation

Along with the rapid evolution and development of electronic based commerce, the need for appropriate and secure electronic payment channel to support the payment procedure is extremely necessary. It could be also treated as a challenge for the electronic based payment systems to meet the user's expectations, requirement, preferences and needs in order to design and exploit the payment systems. Failure to meet them can results in low usability, insecurity, and inefficiency of payment systems and eventually abandoning of customers to use such systems.

This study has investigated the issues and vulnerabilities of the electronic payment system and what the users think about when they are performing transaction. The study also assessed the level of possible threats to the electronic payment system. Despite the benefits that electronic payment system brings to the nation, banks as well as an individual, it has its own challenges and issues. The challenges and issues discussed in the questionnaire can be categorized as security, awareness, legal and regulatory issues.   Nepal's payment system development has come a long way. With the central bank's proactive role, the Nepalese payments system is currently taking new shape. With the payment gateway industry like Nepal Electronic Payment System Ltd. (NEPS) and Smart Card Technologies (SCT), the e payment system is growing. However, the electronic and internet world contains much vulnerabilities and is far from being secure for banks, merchants and card holders.

Almost about 70% of the respondents thinks the threats and vulnerability is due to user unawareness. It won't eradicate the vulnerabilities but will reduce it since the user are the one who are affected. Moreover, the compliance like PCI DSS should also be completed and verified for the threats and vulnerabilities to mitigate. Counter measures for the data breaches should also be consider. The banks must also be educated to promote the benefits of e payments, training programs for its customers. Also, the user should also be cautious every moment they are on the internet. They must be able to check the originality of the contents and be able to trace back to its owner. However, even if the breach occurred, proper investigation procedure must be conducted to find its root cause. The users must be aware of not entering their personal data into the internet until there is proper validation and identification of the owner.

References

Abrazhevich, D., 2001. Electronic payment systems: issues of user acceptance. In B. Stanford-Smith and E. Chiozza (Eds.), E-work and E-commerce.

Ankara, T. W., 2002. Adaption Internet of Banks customers on Internet Banking services. ABAC Jornal, 22(3).

Curran, J. & Meuter, M., 2005. Self-service technology adoption: comparing three technologies. The Journal of Services Marketing, 19(2), pp. 103-114.

Giri, P., 2013. PAYMENT AND SETTLEMENT SYSTEM DEVELOPMENT IN NEPAL: HURDLES AND WAY OUT. Economic Journal of Development Issues, 15 & 16(1-2), pp. 116-127.

Gomedici.com, 2018. Overview of the Payment Industry. [Online] Available at: https://gomedici.com/overview-of-the-payments-industry/   [Accessed 11 February 2018].

Hwang, R., Shiau, S. & Jan, D., 2007. A new mobile payment scheme for roaming services. Electronic Commerce Research and Applications, 6(2), pp. 184-191.

Kabir, M., Saidin, S. & Ahmi, A., 2015. Adoption of e-payment systems: a review of literature. International Conference on E-Commerce, pp. 112-120.

Khan, B. U. I. et al., 2017. A Compendious Study of Online Payment Systems: Past Development, Present Development and Future Considerations. International Journal of Advanced Computer Science and Applications, 8(5), pp. 256-271.

Kim, K. & Prabhakar, B., 2004. Initial trust and the adoption of B2C e-commerce. The case of Internet banking, ACM sigmis database, 35(2), pp. 50-64.

Kaur, H. and Kautish, S., (2016). "An Implementation of Wireless Sensor Network Using Voronoi _ PSO (Particle Swarm Optimization)", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 4, Issue XI, November 2016, pp.361-368

Kautish,S. (2008), "Online Banking : A Paradigm Shift", E-Business, Vol. 8, No.10, pp. 5459.

Kautish S., Thapliyal M P, "Concept of Decision Support Systems in relation with Knowledge Management – Fundamentals, theories, frameworks and practices", International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 1, Issue 2, October 2012 ISSN 2319 – 4847

Kautish S. 2013. Knowledge sharing: A contemporary review of literature in context to information systems designing. Academia 3(1). The South Asian Academic Research Journal: 101-113.

Kautish, S., & Thapliyal, M. P. (2013). Design of new architecture for model management systems using knowledge sharing concept. International Journal of Computer Applications, 62(11), 27–30.

Kumar, A., Rajpurohit, V.S. and Kautish, S., 2020. A Study on Technology-LED Solutions for Fruit Grading to Address Post- Harvest Handling Issues of Horticultural Crops. In Modern Techniques for Agricultural Disease Management and Crop Yield Prediction (pp. 203-221). IGI Global.

Kaur, R., & Kautish, S. (2019). Multimodal Sentiment Analysis: A Survey and Comparison. International Journal of Service Science, Management, Engineering, and Technology (IJSSMET), 10(2), 38-58

Lim Choon Seng, V., 2014. THE DEVELOPMENT OF E-PAYMENTS AND CHALLENGES FOR CENTRAL BANKS IN THE SEACEN COUNTRIES, Kuala Lumpur: The South East Asian Central Banks (SEACEN) Research and Training Centre.

Lim, A., 2008. Inter-consortia battles in mobile payments standardisation. Electronic Commerce Research and Application, 7(2), pp. 202-213.

Malviya, H., 2017. Common Security Vulnerabilities in Online Payment Systems, s.l.: s.n.

Mashayeshi, H. & Mashayeki, Y., 2016. Factors influencing adoption of e-payment systems: an empirical study on Iranian customers. Information Systems and e-Business Management, pp. 1-26.

Mukherjee, A. & Nath, P., 2003. A model of trust in online relationship banking. International Journal of Bank Marketing, 21(1), pp. 5-15.

Niraula, P. and Kautish, S., Study of The Digital Transformation Adoption in The Insurance Sector of Nepal. LBEF Research Journal of Science, Technology and Management, 1(1), pp.43-60.

NRB, 2012. Nepal Rastra Bank Information Technology Guidelines, s.l.: Bank Supervision Department.

NRB, 2016. BANKS & FINANCIAL INSTITUTIONS REGULATION DEPARTMENT , s.l.: s.n.

Rani, S. and Kautish, S., 2018, June. Association Clustering and Time Series Based Data Mining in Continuous Data for Diabetes Prediction. In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1209-1214). IEEE.

Raziq, N., Khan, A. & Khayal, M. S. H., 2011. Certification in Electronic Payment Gateway. International Journal of Reviews in Computing, Volume 6, pp. 17-20.

Roy, S. & Sinha, I., 2014. Determinants of customers' acceptance of electronic payment system in Indian banking sector–a study. International Journal of Scientific and Engineering Research, 5(1), pp. 177-187.

Sanayei, A. & Noroozi, A., 2009.) Security of Internet banking services and its linkage with users' trust: A case study of Parsian bank of Iran and CIMB bank of Malaysia. International Conference on Information Management and Engineering, pp. 3-7.

Sherpa, P., 2015. Development and Impact of Mobile Banking in Nepal, s.l.: s.n.

URS, B.-A., 2015. SECURITY ISSUES AND SOLUTIONS IN E-PAYMENT. Volume 1, pp. 172-179.