Electronic Payment Security According to User's Perspective

Ahmad Tasnim Siddiqui

Department of Computer Science

Taif University, Taif

Saudi Arabia

Email: ahmad.tasnim@tu.edu.sa

Abstract— **This paper focuses at the user concerns when they are making electronic payment. The major concern is for the security of their payment and identity theft. Everyday people are transacting billions of dollars due to the business needs, shopping over Internet and from one person to another person. Now a day's end user is becoming more and smarter and they are very much concerned about their identity and security of payment. This paper includes the survey results which was conducted to get an idea what users are thinking while transacting online. The security and privacy according to the user.**

I. INTRODUCTION

In the early 1990s the business and consumer world encountered a new way of conducting trade business, which was named electronic commerce (e-commerce). Over the years electronic commerce has evolved into a popular and acknowledged way of conducting business. While researchers are still trying to understand it and gauge its importance and turnover, e-commerce is changing and growing incredibly quickly, producing such extraordinary results from both business and customer perspective that its phenomenon cannot be overlooked by anyone who has ever thought of conducting business, whether in online or offline environments. With many organizations and people laboring in the field of e-commerce it has become very clear that ecommerce is here to stay and organizations and customers are trying to get maximum benefit from it.

E-payment is a subset of e-governance which is the application of electronic means in the interaction between Government and Citizens and Government and Businesses. E-payment can be described as the method of effecting payments from one end to another end through the medium of the computer without manual intervention beyond inputting the payment data.

An electronic payment system is needed for compensation for information, goods and services provided through the Internet - such as access to copyrighted materials, database searches or consumption of system resources - or as a convenient form of payment for external goods and services - such as merchandise and services provided outside the Internet. It helps to automate sales activities, extends the potential number of customers and may reduce the amount of paperwork.

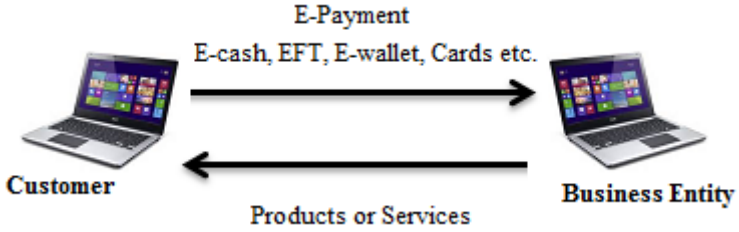


Figure 1: Electronic Payment Scheme

An electronic payment is any kind of non-cash payment that doesn't involve a paper check. Methods of electronic payments include credit cards, debit cards and the ACH (Automated Clearing House) network. The ACH system comprises direct deposit, direct debit and electronic checks (e-checks).

The main drawbacks to electronic payments are concerns over privacy and the possibility of identity theft. Fortunately, there are many safeguards available to protect your sensitive personal information from falling into the wrong hands.

II. WORKING OF ELECTRONIC PAYMENT

When it comes to payment options, nothing is more convenient than electronic payment. You don't have to write a check, swipe a credit card or handle any paper money; all you have to do is enter some information into your Web browser and click your mouse. It's no wonder that more and more people are turning to electronic payment - or e-payment - as an alternative to sending checks through the mail.

Basically there are three important parts when it comes to processing credit and debit card payments, whether online, via phone sales, or even in person. At one end you, the business owner or merchant. On the other end is customer. And in between is a lot of technology involved that connects two of you.

The merchant: In order to accept credit and debit card payments from online customers, you'll need to partner with some key players. As a business owner, it's likely you'll need a merchant bank (sometimes called an acquirer) that accepts payments on your behalf and deposits them into a merchant account they provide.

Customer: Similarly, in order for your customer to pay for your goods and services, she needs a credit or debit card. The bank that approves her for the card (and lends her the cash to pay you) is called the issuing bank.

The technology: In the middle are two technologies that enable you and your customer to transact. The first is the payment gateway, software that links your site's shopping cart to the processing network. The second is the payment processor (or merchant service), which does all the heavy lifting: moving the transaction through the processing network, sending you a billing statement, working with your bank, etc. Often, your merchant bank is also your payment processor, which helps simplify things.

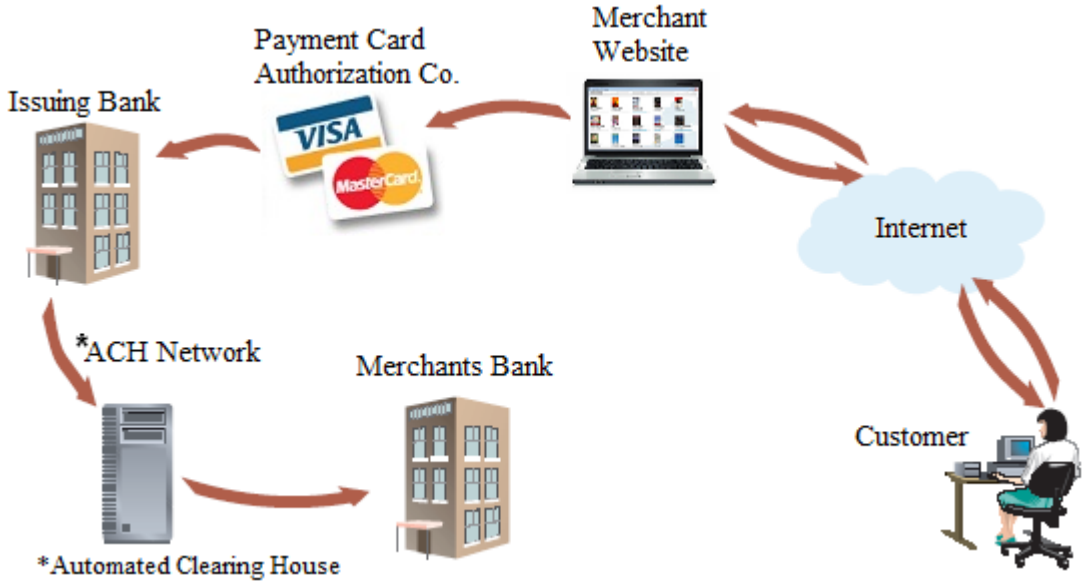


Figure 2: Payment Processing

III. SECURITY REQUIREMENTS OF ELECTRONIC PAYMENT SYSTEM

Secure electronic payment system is very crucial for electronic commerce. Apart from the strong password, secured internet connection, firewall and antivirus software we need some other important things to accomplish the security of electronic payments. In order to ensure the security and integrity of each transaction they utilize some or all of the following security technologies and measures such as Authentication, public key cryptography, certificate, certificate authorities, digital signatures, SSL, SHTTP and secure electronic transmission (SET) protocol.

Authentication: This is the process of verification of the authenticity of a person and or a transaction. There are many tools available to confirm the authenticity of a user. For instance, passwords and id numbers are used to allow a user to log onto a particular site.

Public Key Cryptography: Public key cryptography uses two keys, one public and one private, to encrypt and decrypt data, respectively. Cryptography is the process of protecting the integrity and accuracy of information

by encrypting data into an unreadable format, called cipher text. Public key cryptography uses a pair of keys, one private and one public. In contrast, private key cryptography uses only one key for encryption. The advantage of the dual-key technique is that it allows the businesses to give away their public key to anyone who wants to send a message. The private key is not publicly known.

Digital Signature: Rather than written signature that can be used by an individual to authenticate the identity of the sender of a message or the document; a digital signature is an electronic one. E-cheque technology also allows digital signature to be applied to document blocks, rather than to the entire document. This lets part of a document to be separated from the original, without compromising the integrity of the digital signature. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering. This technology would also be very useful for business contracts and other legal documents transferred over the web.

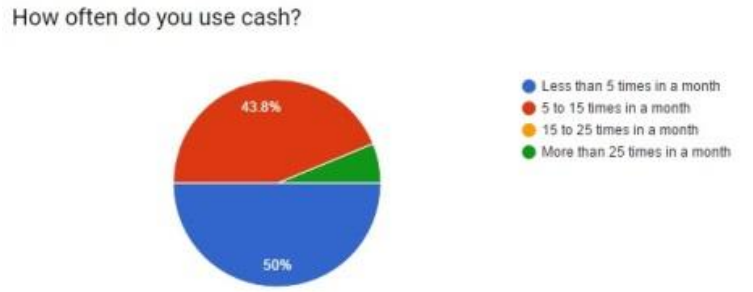
Certificate Authorities: Certificate authorities are similar to a notary public, a commonly trusted third party. In the e-commerce world, certificate authorities are the corresponding of passport offices in the government that concern digital certificate and validate the holder's identity and authority.

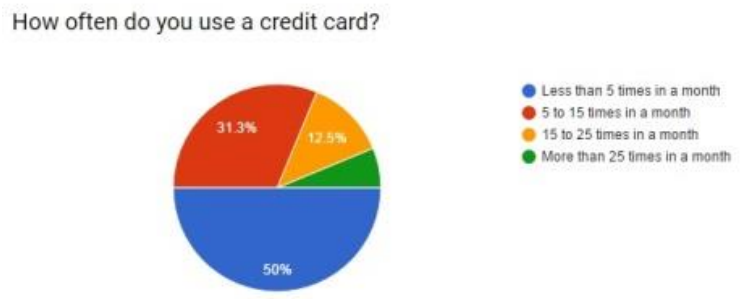
SSL (Secure Socket Layer): SSL is a protocol developed by Netscape Corporation. SSL provides a relatively secure method to encrypt data that are transmitted over a public network such as the internet, also offers security for all web transaction, including file transfer protocol and telnet-based transactions. It provides an electronic wrapping around the transaction that go through the internet. Authentication begins when a client requests a connection to an SSL server. The client sends its public key to the server, which in turn generates a random message from the server and sends its back.

SHTTP (Secure Hyper Text Transfer Protocol): Another protocol for transmitting data securely over the World Wide Web is secure whereas SSL creates a secure connection between a client and a server, over any amount of data can be sent securely, SHTTP is designed to transmit individual messages securely. SSL, SHTTP, therefore, can be seen as complementary rather than competing technologies.

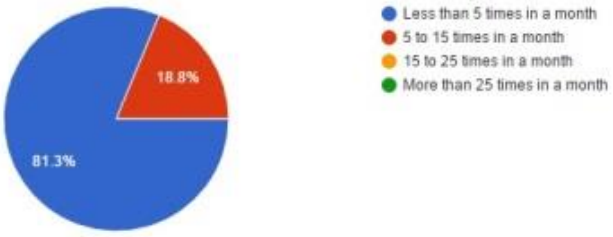
IV. SURVEY QUESTIONNAIRE AND RESULTS

A survey was conducted to get the response from the end users. The purpose of this survey was to get the idea of users what they are thinking when it comes to electronic payment or online payment. What they are using while shopping a credit card, debit card, cash or some other payment options. What according to them are secured way of payment method? And many more questions which are given below along with the responses:

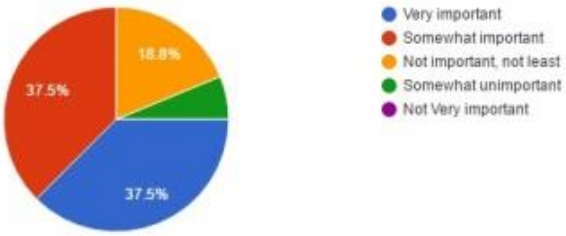




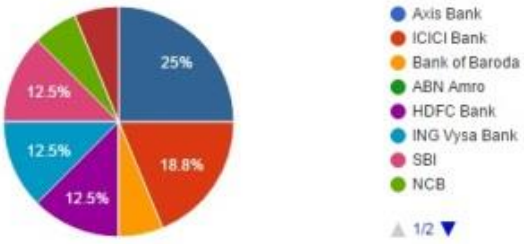
How often do you use an e-cheque?



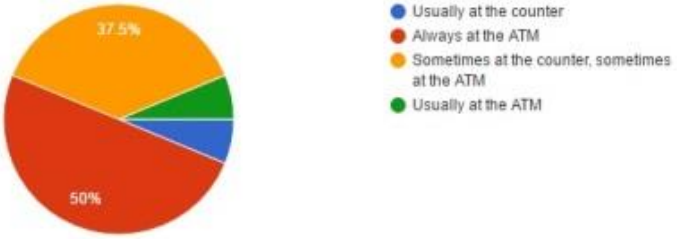
Do you think it is important that you have a currency in most places you pay?



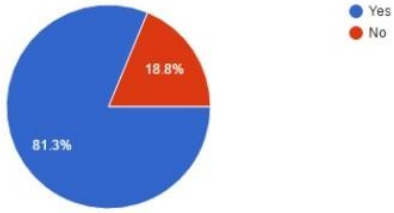
Which bank is your main checking account?



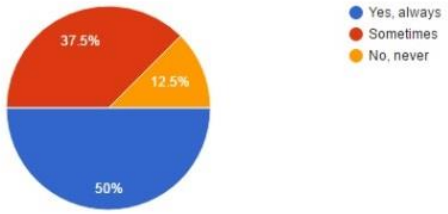
How do you usually cash in on the counter or at the ATM?



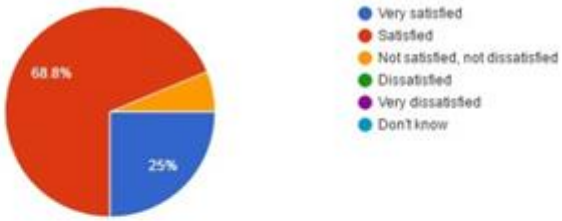
Did you know that banks and stores keep track of your payments if you use a credit card or other electronic means of payment?



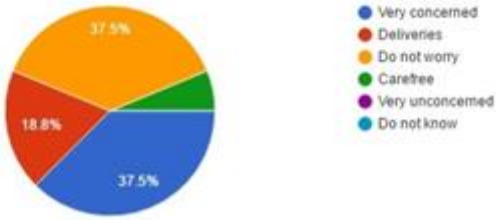
If you use your electronic payment is sometimes known by the identity store. Restrain you to make use of an electronic payment?



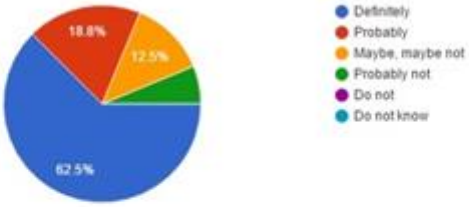
Are you satisfied with the extent to which a bank card offers you privacy?



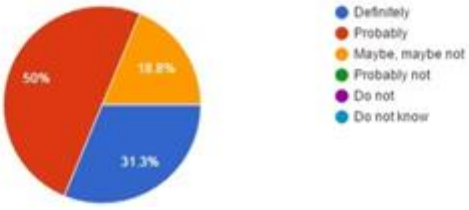
Are you worried about the fact that a store knows what you buy if you pay electronically using a credit or debit card?



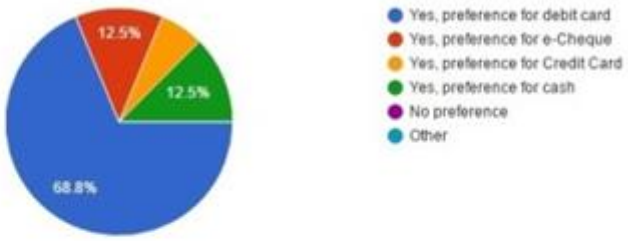
Banks and shops can make mistakes with your money. Would you like to register your purchases in order to demonstrate these errors, such as wrong amounts?



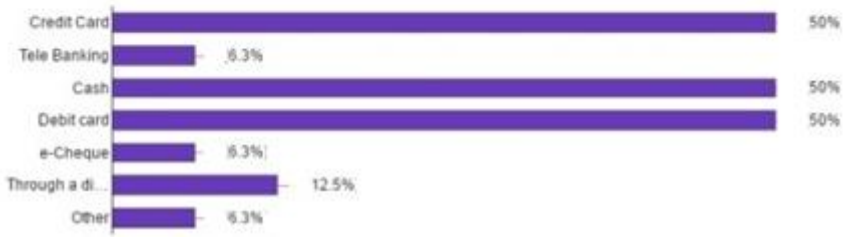
Do you think that stored information about your payment can use to improve their services?



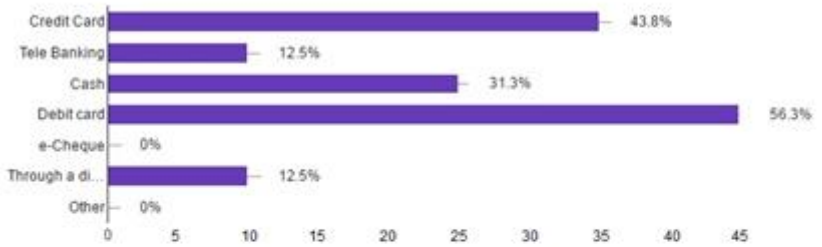
Do you have a preference for a particular payment because it's easy to use?



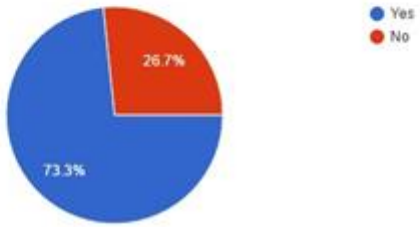
If you ever ordered over the Internet, how often you pay?



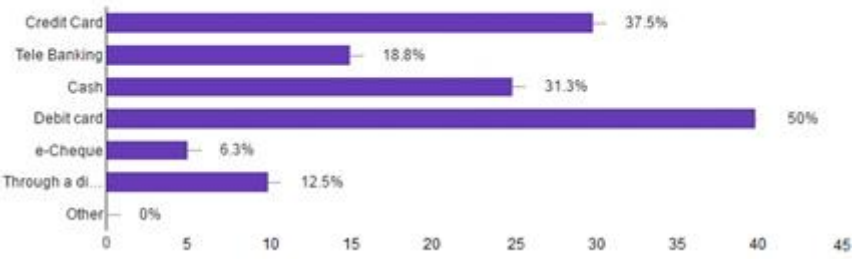
What method of payment for Internet purchases is generally preferred?



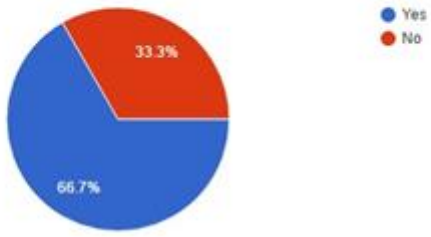
Are you concerned when you pay via internet, that abuse can be made of your data?



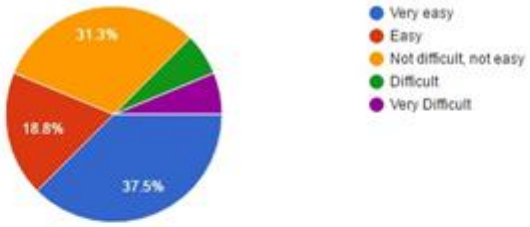
What do you think is the most secure payment method for payments through the Internet?



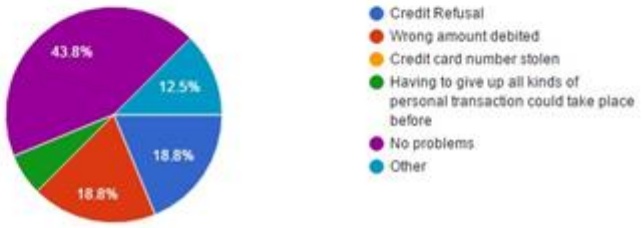
Have you ever used a credit card to pay on the Internet?



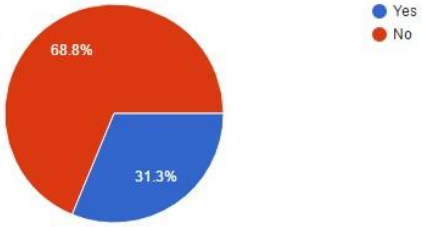
How easy was it to the Internet with a credit card?



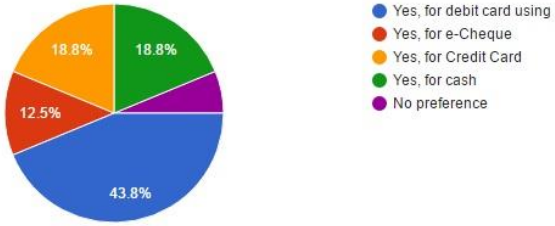
What are the main problems you have experienced credit card payments over the Internet?



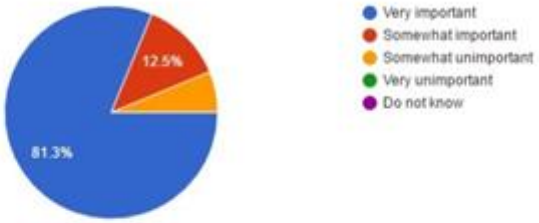
Have you ever lost money due to security vulnerability in the Internet?



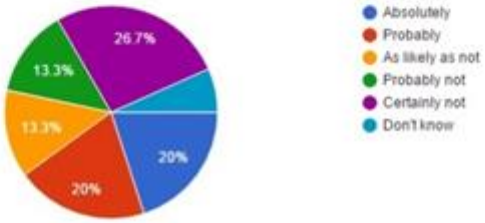
Do you have a preference for a particular payment because it is reliable?



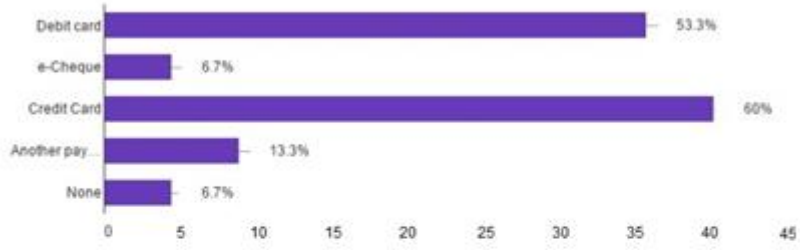
The security of payments is important for you if you use an electronic payment?



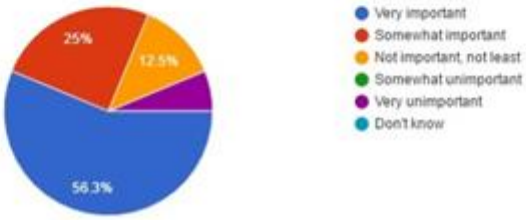
Keep on using a payment when you hear that there are security problems?



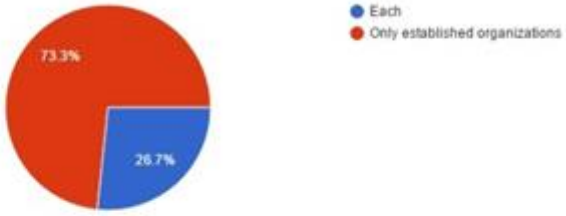
Which of the said electronic payment because you avoid the security of mistrust? (multiple answers possible).



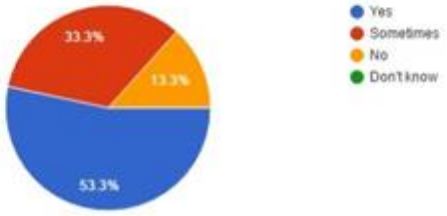
Is it important to you that no traces of your electronic payments such as your name, account number or address?



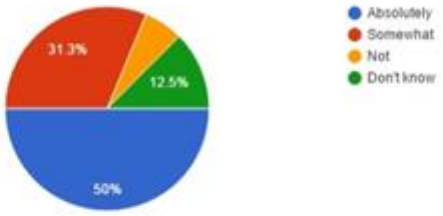
If a new system is introduced, then you trust any organization, or just based organizations such as banks?



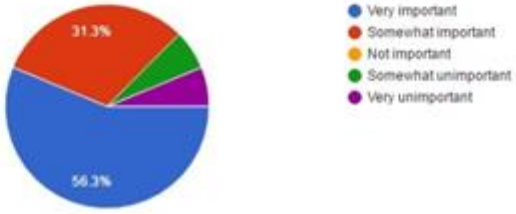
Do you think a shop should offer you the choice to pay with the currency of your choice?



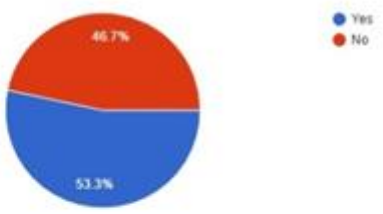
Do you feel more at ease in payments that you are using something tangible (eg a bank card)?



Is it important to you that at any moment you can see how much money you have?

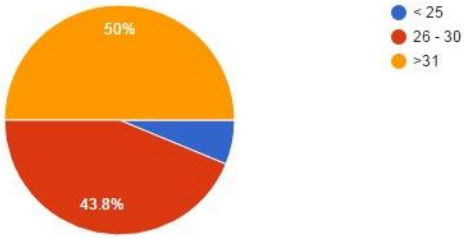


Do you professionally to deal with payment systems, such as bank employee, investigator or as a software developer?

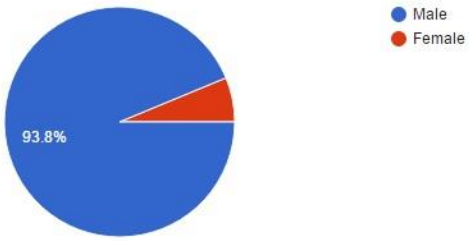


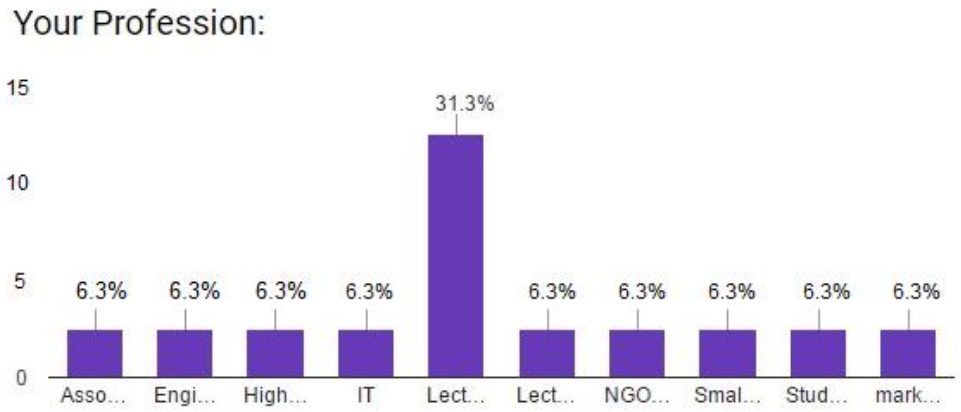
What industry do you work?

Age:



Your Gender:





V. CONCLUSION

To make any electronic payment secure first of all we should follow the basic instructions to make our computers secure. After that Authorization, SSL, Cryptography, SSH, Digital Signature, Certificate Authority (CA) and other things comes into the picture. According to the survey result 77.8% of users said that they prefer to use only established organizations or banks to make transactions. Up to 50% of users are satisfied with the security and privacy measures which are taken by their banks. 42.1% users think that the most secure payment method for payments through the Internet is credit card and debit card. 35% of users think that using debit card is reliable for shopping over Internet while 20% of users are thinking credit cards are more reliable. 84.2% of users are thinking that security of payment is very important while for 10.5% of users it is somewhat important. So, to conclude the security and privacy of electronic payment is very important for the users who are using electronic payment system.

REFERENCES

[1]. Bellis, M. 2003, "The History of Money and Credit Cards", http://inventors.about.com/library/inventors/blmoney.htm
[2]. Gulati, Ved Prakash. "The Empowered Internet Payment Gateway". Computer Society of India. Retrieved 22 May 2013.
[3]. https://www.ccavenue.com/
[4]. Awad, E., M., Electronic Commerce – From Vision to Fullfillment,
[5]. Electronic Commerce Gary P. Schneider. Course Technology, Cengage Learning.
[6]. Pandey, Dr. Vivekanand; Siddiqui, Ahmad Tasnim; "Computer Application in Management", Himalaya Publishing House Pvt. Ltd
[7]. http://webdevelopmentby.ifoundries.com/2009/01/advantage-and-disadvantage-of-ecommerce/
[8]. Siddiqui, Ahmad Tasnim; Singh, Arun Kumar. "Secure E-business Transactions by Securing Web Services", 2012 International Conference on Management of e-Commerce and e-Government. DOI 10.1109/ICMeCG.2012.11