A Step Towards a More Secure and Risk Free E Service System

Sehar Qayyum
Department of Computer Science Lahore College of Women University Lahore

Abstract

The technology has been going through a stage of evolution and it is rapidly changing day by day. The huge development in the field of computers and internet has given birth to the concept of E services which aims at providing services to customers online over the internet like shopping, banking etc. But every technology has its flaws, and so does E services. There have been many flaws and issues surrounding the concept of the E services like frauds, security issues, customer privacy issues, data security, etc. In this paper we are going to focus on the security issues and flaws that can be faced in E services. E services have become an integral part of any business and customer's life. In many countries people prefer to shop online or even access their bank accounts online via internet banking. It surely has reduced the time factor and made the delivery of services easy but it has given birth to a lot more security issues. Many customers are hesitant to provide their personal details and credit cards details online on websites because of the security issues. This proposal aims to address specifically the security issues faced in E services and how different researchers have tried to tackle them

Keywords: Data integrity and confidentiality, DDOS, E services, Privacy, Security, Security loopholes, Trust.

1. Introduction

Internet has been expanded to a very large extent in many countries over the past few years and has resulted in more and more services being provided online like banking, shopping etc which gave birth to the concept of E services. E services received a great acknowledgement from the businesses as well as customers because it is easy to access any service they want online and with less time consumed [1]. But as E services have been expanding worldwide, it has also been prone to cyber-attacks and there have been issues regarding security and privacy of the customer data. Most of the application forming E services includes long line of commands and programming which are prone to bugs and attackers around the world can easily exploit these bugs to gain access to the servers or systems hence creating a security problem [2].

It is also hard for the customers to trust completely on the E services because of lack of confidentiality and other security issues yet it remains the medium of providing services throughout developed countries and some of the developing countries. In some countries like Australia, E services has been given a legal status and has been passed through bills and acts to make it more authenticated and is supported by the government and users (customers) are encourages to use the E services [3]. E services are prone to all threats on the internet including cyber attackers; viruses etc and customers demand more of the system to be bug free and to provide ultimate security and privacy. Many cyber attackers pose threats by Denial of Service Attacks commonly known as DDOS to bring down the server due to which it stops responding and customers accessing the website cannot access it. It also helps the attackers to gain access to the security systems due to which all the data is vulnerable. The focus of the research is the authentication of the customers accessing the E services, Privacy issues, Trust, Data integrity and confidentiality [3]. In most cases the authentication is done via username and passwords to confirm the identity of user accessing the E services. Some common issues faced by the users in E services are discussed below

2. Characteristics of E Services

E Services has been defined in the above section as delivering of services or products online. There are some characteristics of E Services which makes it a broader rather than a narrower concept. Some of the characteristics of E Services are:

- E services are intangible which means they cannot be seen or touched but they do exist.
- E services are delivery of product and services through electronic means i.e. Computer networks etc.
- E service is the addition of technology to normal business processes.
- E services are separable which means that the services of every specific provider can be differentiated.
- E Services can be patented as a registered trademark but they can also be copy righted which is not present in normal services or goods.
- Most of the E Service businesses are homogenous which means that the nature of most of the E services businesses is same.
- E service is the desire of the providers to reduce operating costs and enhance the speed of the delivery.
- E services is the buying and selling of products or services online through internet or other online sources.
- E services are available all the time throughout the day and the whole week and month providing services every time.

- E services are evaluated on the basis of the provider's reputation [4].

3. E Service Model

The basic model of E-Service has three main categories that are users (client), e service providers system (server), and a network medium through which they are connected to each other. The figure below depicts the E Service model in an easy and understandable manner.

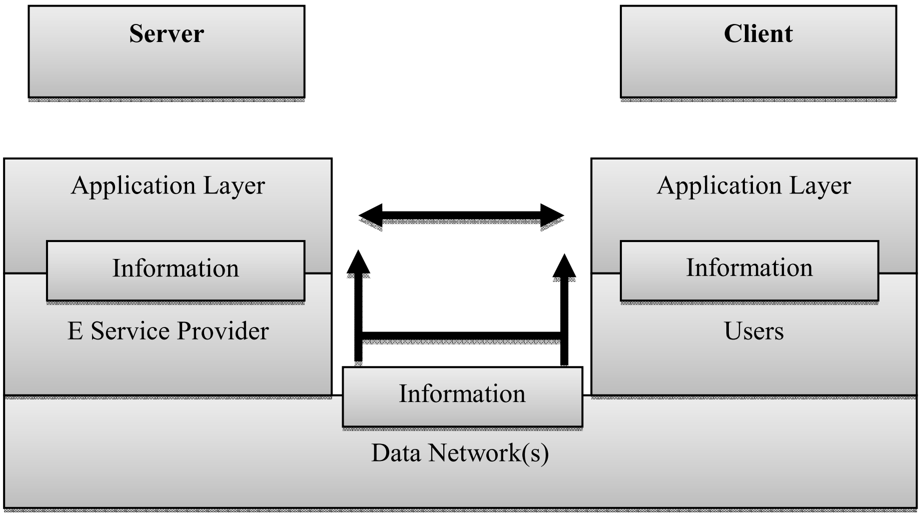

Fig.1. The client server model for E Services. The data is transferred by application layers through network and system layers [5].

In the above Fig.1 model, there are two service application systems on both client and server. There are three layers of protocols mentioned in this model that are application layer, network layer, and system layer. The data between the user and E service provider is transferred through application layer using the network and system layer. The messages are transferred the same way between both the server and client's end [5].

4. Security Issues in E Services

Security refers to the act of being safe from harm and hazardous things. Security in E services can be defined as the procedure for making sure that the confidentiality, availability, and integrity of the online data is protected and that it is not vulnerable to cyber attackers and other malicious activities. Security has been a major concern for most of the E service providers because they fear the loss of valuable information. Moreover the customers or users of the E Service system also fear the loss of their personal and private information including the financial data and bank information etc. The more the users face these security threats, the less will they avail the services provided by the E service providers

Security issues have long been existing in E Services and many solutions and suggestions have been made to improve the security issues but still they are ongoing problems which can be reduced but cannot be eliminated completely because of the involvement of human factors both in managing of E Service system as well as development of software's. A proper security technology will never solve the security issues unless the organization has a proper software engineering management that means how the software will be managed and brought to use in the organization. Organizations also need to have clear policies regarding the risk management, job specialization, and human involvement in the E Service Security system [6]. Some of the common security issues that a user can face while avail E services are mentioned below.

4.1. Privacy

Every person has the right to privacy in every aspect of his life be it his personal life or professional life. No author has yet come up with a perfect definition of privacy which makes it more interesting. Privacy is basically based on the perception of a user's view about how he views privacy as so it keep varying from person to person which means it cannot be defined precisely. But according to Schoeman privacy is the amount of right that a person has in controlling personal data and information regarding him [6]. The development of new technology has undoubtedly given more level of privacy to an individual but at the same time it has also caused threats to the privacy of the same individual. The concept of privacy with technology is not new. In fact it was first identified 115 years back when photographs were used in newspapers without people's consent. Privacy came out as a major issue in E services when users tried to communicate and avail web services. The problem can arise from user end as well as server end. Users having low security on their personal computers make them a hot target for cyber attackers and it can happen from E service system in form of information leaked by an employee or low level of security systems. Very few countries have the rules and regulations in place for protecting the privacy of online users. Countries like UK, Sweden, and Australia where no one can have a hold onto personal information without the consent of the original owner. [6].

4.2. Trust:

Trust is another issue that can arise in E service system and this inter related with the concept of privacy. The more a user faces privacy issues in availing E services the more his trust keeps diminishing. A research's outcome showed that 68.5 % people have trust issues and they believe that their personal information is been sold out or leaked out to third parties for marketing purposes [7]. Users tend to have more trust when the E service provider has the right security measures and technologies in use, as well as he has clear law on protecting the personal information of the online users. A trust development process was produced which suggested that users of the E services tends to have more trust on the provider when they ensure that privacy risks are minimal, and that the provider has the right type of security system to protect their private information and secure transactions and to add that the provider has the right type of privacy policies implemented within the organization [7].

4.3. Security loopholes:

Security loopholes can be defined as the deficiencies of the software or programming that create some gap in the system which can be exploited by the third parties or cyber attackers. Security loopholes are bound to happen for the reason that all software's are developed by some programmer who is a human and these software's are prone to errors. As research suggests that there are no silver bullets to eliminate the essential problems of software. Brooks divides the software error into two categories accidental problems and essential problems. Accidental problems are those which effect the production of software (problems which we create ourselves and can be fixed) but are not inherent. Whereas essential are difficulties that are inherent in software like algorithms, flowcharts and data sets. Brooks analyzed that accidental problems have diminished and eliminated due to the latest developments in software's and high level languages but the essential problems still remain. So it clearly indicates that each and every software is not perfect rather is has some gap called security loopholes which can be taken advantage of and can be exploited by attackers [8]. The cyber attackers usually have a keen eye on such loopholes so that they can find a way inside the system and can steal private information like credit card numbers etc. They tend to do so by mostly using DDOS (Distributed Denial of Service) attacks on web space of specific E Service provider which makes it unreachable for the users and user cannot access that website for some time. The cyber attackers usually get into the security systems of the E service provide and steal much valuable information including private information of the user. It also denies the user access to that specific website which in turn can result in a financial loss too.

4.4. Data Integrity and Confidentiality:

Data integrity means that the data after being stored inside the databases is consistent accurate and up to date and its security cannot be compromised in any case whereas Data confidentiality means that data is kept safe and private and can be accessed by those people who are authorized to do so. It has been pointed out that a big problem in E services security issues is the data integrity and confidentiality [9]. Sometimes the personal not authorized to get hold of the private data gets into the system compromising its security and selling that information to third parties. E services providers need to have strict laws regarding this issue and they should make sure that information is available to only those people who are authorized to access it and to add to it, they should only hire people who are trust worthy and can be depended upon. Because if this problem keeps repeating, the users trust over the E service provider becomes threatened and they slowly tend to leave using E services.

5. Background Data On Security And Privacy Issues In E Services

The E services have no doubt been growing quite immensely but it has also been accompanied with problems throughout its evolution. Any problem in any aspect of the E services maybe it be authentication, security or any other malfunction will cause a problem for the customer. Parasuraman developed a scale named E S Qual scale. This scale had everything that covered the E services. The scale was divided into 4 dimensions and 22 statements. The four dimensions were system availability, privacy, efficiency, and fulfillment [9]. A research points out two possible privacy issues that customers would think over when they are availing E services. The first privacy issue would be the unauthorized access to the systems private data due security loopholes. The second is the re use of the users private data for other purposes without taking their consent [10].

Another research has suggested that to solve the privacy issue of E services, both law and technology has to be combined. Security problems will keep occurring despite the fact that more and more solutions has been designed to eliminate them as it has been discussed in a study which suggested that some E banking systems stores the password of users in Cookies which can easily be cracked and took over by hostile websites.

Schneier argues that each and every system has security loop holes and even updating the systems constantly and following all security protocols might still result in security breaches [10]. A study discovered the users of the E services are mostly concerned with three major issues system security loopholes, privacy, and scam companies running businesses online.

One study suggested the use of Public key infrastructure for the purpose of security. It includes two keys named as "public key" which former is used for the sole purpose of encrypting the data and is available to the world and "private key" which is used for decrypting the data. A research suggests that all the E services system should be operated using a firewall and all unnecessary services like email ftp etc should be removed from the website of the company. A survey found that most of the security issues surrounding E services are not from the merchant or the security loop holes in the system rather it is mostly due to the user using the computer and browser to authenticate them. Hackers can gain access to the user's pc and gain access to confidential data like passwords and credit card numbers etc [10]. The use of HTTP cookies can also be used as means to identify the user passwords but cookies where provides a good base for security but not yet as good as compared to the public key infrastructure. Another study concludes that organizations must have a proper process of allocation of duties and responsibilities for the purpose of security. He thinks that organizations must devise policies and rules for the security of the data so as to prevent the leakage of private information regarding the users as well saving the data from getting corrupted [10].

Most of the payments for the E services are SSL protected and that most users or customers consider privacy as a legal right and they won't indulge in using or availing E services until and unless they are fully satisfied that their data will be kept private [10].

6. Security Concerns Regarding E Services

There has been a lot of chanting going around since the E services came into existence and there has been an extensive amount of research performed on each and every aspect of this topic ranging from Security issues up to the trust issues and its affectivity as well as its negativity. The main purpose of performing this research is to identify all the security issues that a user can face while availing E services and specifically focusing on issues like Privacy, Security loopholes, trust, data integrity and data confidentiality. An extensive amount of research has been and is being performed on the security issues of E services. In our research is simply based on the data from researches that are previously performed by various researchers in different countries on the same topic [11].We have taken a few researches on security issues in E services and have performed an extensive analysis of those researches, journals, and handbooks taken from different internet sources and we have analyzed the methods they used to tackle the security issues being faced in E services over time and at the end we have suggested some possible solutions to eliminate the security issues so as to give the user full confidence and trust over availing E services without any risk or fear. The sources used in this research are all secondary sources like previous researches, books, journals, handbooks and internet sources.

In order to achieve our main objective i.e. to reduce the privacy issues faced by the consumers in E services, this research aims to perform a sequence of steps like checking the existing researches, journals, articles, and internet sources on privacy issues in E services and understand how they can affect a user and the E service provider and what impact it can have as a whole. The next step would involve analyzing different solutions to reduce the privacy issues and finally selecting one best possible solution and selecting it for implementation and then evaluating the final outcome. The result of this research can be generalized to every city in Pakistan and every country because most of the services provided by the provider of E services are almost the same despite the different countries so that enhances the chances of generalizing our findings to different contexts. The data taken from all the researches are those which are performed in a proper and scientific manner. According to a study, all of the high quality research always gets published in journals before getting published anywhere else [12].

7. Varying Viewpoints On E Service Security Issues

There are two main stakeholders involved in E Services that are users and E service providers. Both have different viewpoints about the delivery and security of E Services based on their perception. Both viewpoints are discussed below [13].

7.1. Users Viewpoints:

The user's viewpoints on Security and privacy of E services are:

- Services are available all the time which literally means the whole day and the whole week.
- The navigation on website is easy to use and has a sitemap to further make the accessibility easy.
- The login method is authenticated and highly secure.
- Their private data and information is secured and is not available to anyone without their consent and will.

- The government has a working policy or law which protects the privacy of the users.
- The E Service provider has appropriate security measures in practice.
- The E Service provider has a functional organizational law or procedure regarding protection of the privacy of online customers and users.

7.2. E Service providers Viewpoints:

The E service provider's viewpoint on security and privacy issues and making them better are:

- Dealing with DDOS (Distributed Denial of service attacks) by adopting software which has less or no security loopholes.
- Making the security of internal and external networks more efficient by using latest encryption and decryption techniques.
- Hiring employees who are trust worthy and dependable that they would not leak out the private information of users.
- Creating organization policies regarding the protection of the privacy of online users and publishing these rules and policies online.
- Constantly reviewing the security systems for any deficiencies on regular basis [13].

8. Improving The Security Of E Services

After reviewing various researches and journals on the E services security we have analyzed that with the abundance of E services, the security seems to be more at risk though latest development in hardware and software has brought it down to the minimal but still it exists and it is very hard to completely eliminate these problems but there are solutions to reduce the security and privacy risks.

8.1. Public Key Infrastructure (PKI):

The public key infrastructure can be one solution to all the E services security issues. The PKI i.e. public key infrastructure uses the concept of encrypting and decrypting the data which is also known as secret key cryptography. The concept was first introduced in 1976 by Whitfield diffie. This concept has two keys as opposed to the concept of using one key for both users. Now both users have two keys on their hand a public key which is made public to the world where as a private key which is kept safe by the user. The public key encrypts the data sent from one end and this data can only be decrypted at the other end with the private key of the user [14]

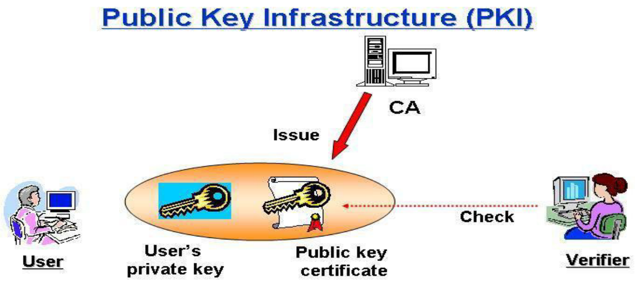

Fig.2. Public Key Infrastructure [15]

In the above Fig.2, using this method the chances of the E services security problems can be brought down to minimal. As the data is encrypted so if there are any security loop holes in the E service system, the cyber attackers cannot get hold of user's private information. The users need to keep their private key very safe out of the reach of any one so that no one can access and no one can take a hold of private information that is passing in between the network as encrypted. The public key and private key both are inter related with each other so there are minimal chances of security issues because of a cyber attacker guesses the way a users private key is derived from public key would make the whole security system fall down but those chances are very less [16].

8.2. Secure Socket Layer (SSL):

Another common technique that can be used is SSL i.e. Secure Socket Layer. SSL is a step ahead of the TCP/IP and HTTP layers. It is more secure to use in terms of E services because it authenticated through the use of the certificates. An SSL connection can only be established if the server and client are both SSL enabled. If the server is running in the SSL mode, it can interact with the client only through SSL [17].

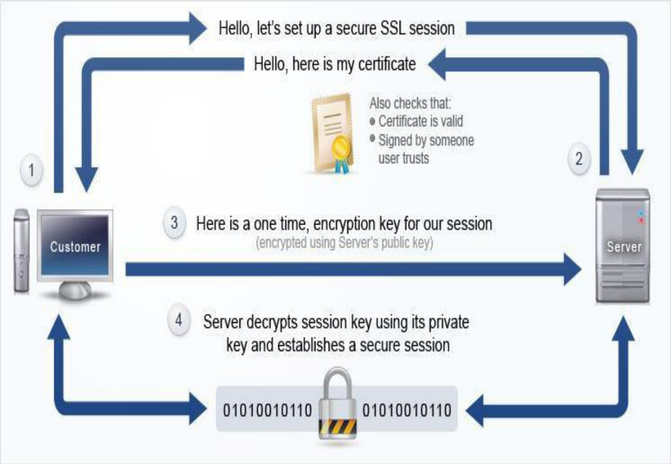
Hello, let's set up a secure SSL session
Hello, here is my certificate
Also checks that:
• Certificate is valid
• Signed by someone user trusts
1
2
Customer
Server
3 Here is a one time, encryption key for our session
(encrypted using Server's public key)
4 Server decrypts session key using its private key and establishes a secure session
01010010110
01010010110

Fig. 3: Secure Socket Layer [18]

In the above Fig.3, an SSL interface is basically set up between a user and server when the user sends the request to connect to a secure server, the server in response sends a signed certificate to the client or user and user then compares the certificate to identify if it is legal or not. If he is satisfied with it, he continues to use a cipher code which the server sends to him and hence they generate a session using a session key which is authenticated by the server's public key [19]. The server decrypts the key encrypted key with a private key same as in PKI and hence they starts sending data using both the keys in encrypted and decrypted form which provides an additional layer of security while communicating with an E service system which reduces the chances of fraudulent activities and helps protect from cyber attackers as well as it ensures the privacy of the clients data is kept intact.

8.3. SMS Authentication:

Another solution to all the security problems of E services could be the use of SMS authentication. When the user is going to sign up for a web service account, he will be asked to enter her cell number so a computer generated code can be sent to him each time he logins to his account. Besides using a user name and password to sign into a web service, an SMS authentication code would be sent to the user or customer each time he tries to log in to an E service system and he will be redirected to a page where he has to enter the code he has received on his cell phone [20].

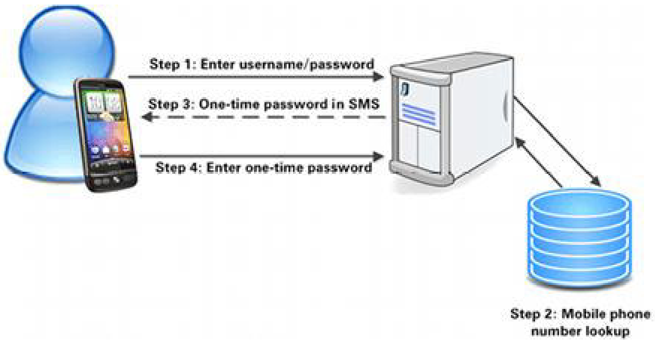
Step 1: Enter username/password
Step 3: One-time password in SMS
Step 4: Enter one-time password
Step 2: Mobile phone number lookup

Fig.4. SMS Authentication [21]

In the above Fig.4, this method will provide an additional security layer to protect the privacy and security risks that a customer can face while using an E service system. It will be prone to fewer issues because every time the user signs in he will receive a different code each time hence it would be hard for the cyber attackers to get hold of the code even if they crack the user name and password of the user. And it will provide an additional layer of security alongside the username and password which will make it more convenient and trustworthy for the user to avail E services [22].

The organization providing E services should also have clear rules and procedures on the security of E services. They should formulate strategies to help secure the user's data more efficiently and should hire that staffs that are honest and worth trust and deploy them on the E service system. This will lead to more secure E services because a survey suggested that most of the private data that is leaked to the third parties and other companies are through the employees working on the data security of E service system. Government should also take certain steps to formulate rules laws and regulations regarding the security and privacy of E service system because most of the developed countries like Australia and New Zealand are already ahead in this prospect. Added to that, a government rule regarding E services will also remove doubts in the mind of customers and they will avail these services with a more risk free attitude [22].

9. Identifying The Threats To E Services Security

There many reasons due to which the E Services security and privacy issues takes place and some of them have already been discussed above in various sections of this report. The main objective of the E Services provider would be to identify these threats and how they operate so as to resolve these issues more effectively and efficiently. Some of the threats are mentioned in the table below and how they can be identified.

Table.1 shows some of the threats that a user can face while interacting with E service system and the possible reasons for the threats are given. Threats can be happen from both internal and external sources i.e. employee involvement or cyber attackers. The attacks can put user's financial and personal data on risk as well E Service provider's financial data too. The attack might be intentional by some cyber attacker or it can be an accidental one too if the users have malicious software's installed on their personal computers.

The users are vulnerable to attack when they are on their own systems but they might also be vulnerable when they are interacting with provider's system or on their network. The main objective of the provider is to secure the user's private data as well as their own private and financial data [23].

10. Conclusion

E services are the next step in evolution of businesses. Many businesses and users are adopting E services due to the fact that it consumes less time in using these services from the customers point of view where as it helps the businesses to attract and cover a large area of target customers and provide services to them through one medium. E services has been expanding quite largely with the enhancement in the field of IT and internet and more people are availing them despite that they have some security issues which is a risk. Though that risk and issues have been diminishing over the last few years through latest developments in hardware and software technologies but still Security and privacy are ongoing problem in E services and will keep arising one way or the other. Many researchers have suggested many solutions to these problems but still the security or privacy issues could not be eliminated completely. This research covers all the aspects of E services issues within the domain of Security and Privacy and has suggested a few solutions with which these problems can be reduced to a minimal level [24]. In the findings section we have suggested a few solutions including Public Key Infrastructure which comprises of two keys namely "public key" which is used for the purpose of encrypting the data on network and "private key" which is used to decrypt the data on the other end. Without having a private key, the data cannot be decrypted and will remain in the encrypted form hence giving more security to the users and E service providers [24]. The second solution suggested in this research is Secure Socket Layer commonly known as SSL. The SSL requires both user and server to be SSL enabled. It provided a bit higher security then the usual HTTP protocol. The SSL session is verified through a certificate issued by CA i.e. Certificate

Authority and after that a onetime encryption key is issued from the user side and the server verifies that key and decrypts it using its private key and establishes a secure connection. It is one layer beyond the basic TCP/IP and HTTP layers hence provides more security and prevents hackers from getting hold on to the private information and data [25].

The third solution suggested is the use of an SMS authentication code. The mobile number of the user will be saved in the Server database and when a user signs in to his account he will request for an SMS authentication code. The server will check for the number in its database against the user name and password and will issue an SMS including an authentication code to the user. The user will enter that code and will be authorized to use his account. This is commonly known as two factor authentication and it provides an extra layer of security apart from the user name and password [26]. The users are recommended to use an updated antivirus and firewall system to prevent the cyber attackers from stealing personal data from their personal computers. The companies are also recommended to take action against its own employees who leaks the personal information of the users to third parties and to adopt the latest hardware and software technology which may reduce the security and privacy issues in E services. They should have a clear law or regulation to protect the privacy of the users. This will help reduce the privacy risks in the mind of customers and they will adopt E services more and with a risk and carefree attitude. Government is also recommended to create laws and regulations regarding the protection of the privacy of online users hence giving them a more sense of security [26].

11. Suggestions For Future Research

For researchers who wants to further study or research on this topic i.e. Security and Privacy issues in E services, few suggestions and recommendations are given below which will help them in conducting their research more efficiently and effectively. The future researchers should first of all pay attention to the limitations of this research and should try to eliminate these limitations in their research.

- There is no primary data or primary sources used in this study because this study is based on the analyzing and interpretation of previous studies so future researchers are recommended that they use primary sources in their studies and collect data from primary sources through the use of questionnaires and interviews.

- The result of this study is generalized to the context of Pakistan so future researchers should keep this in mind that this study may or may not be applicable in their country of research so they are advised to apply the solutions first to check if they generalize to their country or not.
- This study includes a suggestion that government should formulate laws and regulations to protect online user's privacy. This is suggested because there is no such law or regulation in Pakistan. Future researchers must first of all analyze this point in their own country if their government has any specific law regarding to protection of privacy of online users.
- Future researchers should also keep in mind the hardware and software developments that are evolving with time and maybe there is a better technology in future that can eliminate the privacy and security issues in E services completely.
- Future researchers should also focus on the fact that while analyzing the privacy risks using the primary sources the results may vary because of the fact that already discussed above, privacy is based on the perception and thinking of a person and it varies from individual to individual. So every user might have their own meaning and understanding of the concept privacy and it might make the result vary. It is more of a qualitative thing rather than a quantitative one.

Acknowledgement

First of all, thanks and all praises to Almighty Allah who gave me the courage, patience, and motivation to carry out my work successfully. I owe my gratitude to my colleagues for their help and support in producing this report. I would also like to thank my advisor Dr. Muhammad Mohsin Nazir Associate professor, Department of Computer Science, Lahore College for Women University, Lahore for his constant help and ideas. Without his attention and required help, I would have never been able to complete my work.

Finally I would like to thanks my parents for their patience and constant support throughout my work. They have been an inspiration for me and I am thankful for what they have done and what they keep doing for me and without their support and prayers I wouldn't have been here.

References

M. Mehta, S. Singh, Y. Lee, "Security in E-Services and Applications", Wiley[Imprint] Inc, 2000, ISBN 0-471-XXXXX-X, p. 1-2.

V. Cristea, F. POP, "E-service Security", The publishing house of Romanian Academy, 2012, Vol. 13.

M. A. Nasir, "Legal Issues Involved in E-Commerce", ACM, 2004, p. 3.

M. Shah, S. Clarke, "E-Banking management: Issues, Solutions, and Strategies", IGI Global, 2009, ISBN 9781605662527, pp. 18-19.

R. Boutaba, B. Ishibashi, B. Shihada, "A network management viewpoint on security in e-services", Springer, 2003, pp. 4-5.

R. Smith, J. Shao, "Privacy and e-commerce: a consumer-centric perspective", Springer Science+Business Media, LLC, 2007, pp. 3-5.

A. D. Miyazaki, M. S. Featherman, D. E. Sprott, "Reducing online privacy risk to facilitate e-service adoption", Emerald Group Publishing Limited, 2010, Vol. 24, pp. 6-7. ISSN 0887-6045.

F. P. Brooks, "No Silver Bullet: Essence and Accidents of Software Engineering", IEEE, 1987, Vol. 20, Edition 4 pp. 10-19.

N. O. Canarslan, "A Comparison of Customers Responses to E-Service Quality Statements", IEEE, 2013, Vol. 4, edition 11.

M. S. Ackerman, D. T .Davis, "Privacy and Security Issues in E-Commerce, New Economy Handbook", [Press], 2003, p. 1, Available: http://econ.ucsb.edu/~doug/245a/Papers/ECommerce%20Privacy.pdf

P. Subsorn, S. Limwiriyakul, "A comparative analysis of the security of E Banking", presented at International Cyber Resilience Conference Online, 2011, p. 71.

D. Arduini, A. Zanfei, "An overview of scholarly research on public e-services", ACM, 2014, p. 2

R. C. Marchany, J. G. Tront, "E-Commerce Security Issues", IEEE, 2002, pp. 1-9.

L. I. Peixian, "Issues of Security and Privacy in Electronic Commerce", ACM, 1997, pp. 6-8.

S. Koga, K. Sakurai, "Decentralization Methods of Certification Authority Using the Digital Signature Schemes", 2nd Annual PKI Research Workshop, 2003, ACM, pp.54-64.

Security and Authentication Issues in the Delivery of Electronic Services to Taxpayers, Forum on Tax Administration: Tax payer subgroup: OECD standard 11718, 2012.

S. Seltszam, S. Borzonsyi, A. Kemper, "Security for Distributed E-Service Composition", Passau, Springer, 2001, p. 6.

J. Davies, "Implementing SSL/TLS Using cryptography and PKI", Wiley Imprints, 2010, ISBN: 978-0-470-

92041-1, p. 122.

T. Dierks, C. Allen, "The Transport Layer Security Protocol", ACM, 1999, p. 7.

P. Subsorn, S. Limwiriyaku, "A comparative analysis of the security of internet banking in Australia: A customer perspective", ICRC, 2011, p. 5.

F. Aloul, S. Zahidi, W. E. Hajj, "Two Factor Authentication Using Mobile Phones", IEEE, 2009, pp. 641-644.

C. K. Dimitriadis, "Analyzing the Security of Internet Banking Authentication Mechanisms", ISACA, 2007, pp. 1-8.

R. Boutaba, B. Ishibashi, B. Shihada, "A network management viewpoint on security in e-services", Springer, 2003, p. 10.

M. Jordan, D. Belmonte, G. Bonin, J. Wagner, "Paving the way for the next generation of eservices", Price water house coopers LLP, 2013, p. 3.

R. Roland, K. N. Lemon, “E-Service and the Consumer”, International
Journal of Electronic Commerce", Springer, 2001, pp. 85-102.

K. Ghosh, T. M. Swaminatha, "Software Security and Privacy Risks in Mobile E Commerce", ACM, 2001, pp. 51–57.

Kristian Angelo, a, Mary Jovy Anne, V., Azie Trina, M., & Jonathan, C. (2014). Privacy Awareness in E-Commerce. International Journal of Education and Research, 2(1).

Huong, T., Ho, L., & Chen, Y. (2013). Vietnamese Consumers’ Intention to Online Shopping Adoption: A Qualitative Approach, 2(3), 431–442

Zhou, L., Long, F., & Yang, W. (2011). Research on customer perceived risks in internet group buying. International Conference on Management and Service Science, MASS 2011, 1–4. http://doi.org/10.1109/ICMSS.2011.5998990

Zuroni, M. J., & Goh, H. L. (2012). Factors Influencing Consumers’ Attitude Towards E-Commerce Purchases Through Online Shopping. International Journal of Humanities and Social Science, 2(4), 223–230.

Table 1. Identifying Threats To E Service Security

S. No	Identifying threats to E Service Security		
	Factors	*Description*	*Threats*
1.	Source	Who might attack the E Service system?	• Inside Organization • Outside Attacker • Malicious Customer
2.	Location of attack	Where does the threat come from?	• Internal Threat • External Threat
3.	Vulnerability	Where is the user more vulnerable to attack?	• On network • At his own PC • At providers computer
4.	Attack variety	How is the E service system affected from the attack?	• Assertive • Unassertive
5.	Intentions	Is the attack caused intentionally?	• Accidentally • Intentionally
6.	Risks	What risk does user have to bear?	Risk of privacy and security as well as confidentiality.
7.	Objectives	Which objectives need to be protected?	Users and provider’s personal data as well as financial data.