LITERATURE REVIEW

Bhaveshkumar R. Javani, APRIL 2012

This paper tells us about the security related existing pervasive computing based web services architecture and then proposes a middleware secure and scalable architecture. With open source protocols a lot of solutions have been proposed in the literature for implementing the security in pervasive environment. Most of them rely on the intermediate servers for securely transfer of data and communication between end user. This might be suitable for certain development but the broad range of users is not comfortable to accept and deploy such solutions. End-to-end secure communication between the users is a key for the communication protocol to be considered for deployment by broad range of users. The paper presents prototype architecture for pervasive computing based web service using open standards to implement a secure and scalable architecture.

Zachary B. Omariba, Nelson B. Masese and Dr. G. Wanyembi, July 2012

The e-banking system addresses several emerging trends: customer’s demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. The challenges that oppose electronic banking are concerns of security and privacy of information. This paper will first discuss the drivers of electronic banking; secondly, it will talk about the concerns about e-banking from various perspectives. Thirdly, the security and privacy issues will also be discussed, and fourthly the attacks of electronic banking with their solutions are discussed.

G. Jai Arul Jose and C. Sajeev2, Aug 2011

The cloud computing uses the internet as the communication media. The vendor has to provide some assurance for security of data in the cloud computing. Organizations use cloud computing as a service infrastructure; critically like to examine the security and confidentiality issues for their business critical insensitive applications. Yet, guaranteeing the security of corporate data in the "cloud" is difficult, if not impossible, as they provide different services like Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). Each service has its own security issues. Data Protection Application Security Privacy is important security issues that have to be included in cloud computing. This paper propose model system in which cloud computing system is combined with Cluster Load balancing, ssl over aes and secure session In this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.

Preeti Dhankar, May 2012

Nowadays electronic commerce services have risen to become more ... The handling of the payment may involve many ways, such as online banking. Computer network technology is developing fairly rapidly. With the Internet, Hacker and Virus overflows, such as the growing threat of cybercrime, network security management tasks will become increasingly difficult and complex, good grasp of network security issues on protection of network information security. Development of electronic
commerce exists in today’s security threats and the corresponding technical solutions. Therefore, the article on e-commerce payment security issues of network analysis.

Dr. Manju Gupta, July 2012

Despite this progressive growth the security of transaction which involves money over the World Wide Web has been a major point of uneasiness for many to join this modernized way of buying and selling. It is very true that electronic commerce will revolutionize businesses, and customers will be offered new product and exciting services. As e-commerce businesses are expanding, more and more secure technologies are being developed and improved every day. There are various types of algorithms for encryptions are available, but the most commonly used for security of e-commerce transaction, such as Cryptography - Public and Private keys cryptography, DES, RSA, S/MIME, SET, SSL, and Digital Signature which will be discussed.

Karun Madan, May 2011

In the recent years, the number of online banking users has increased swiftly. This has led many developers to investigate extra convenient methods for customers to perform mobile banking transactions. Mobile banking is a new system for customers to perform transactions, and is predicted to increase more rapidly in future also. At the moment most of the banks provide mobile banking through these two channels: First, through the Wireless Application Protocol over the General Packet Radio Service and Short Message Service by means of Wireless Internet Gateway. Mobile banking is appealing as it is a convenient approach to perform banking transactions, but there are security shortfalls in current mobile banking implementations. This paper discusses some of the security deficits.

Alaa Hussein Al-hamami, Fadi Ali Oqla Najadad and Mohammed Saad Abdul Wahhab, March 2012

Information security science started to play a vital role in our life and became an important issue used for judging on any system about either its success or failure. E-banking applications for transferring money are considered as one of the most important applications that banks nowadays are taking care about; maintaining its process validity and accuracy as a necessity for the health of the transferring process to transfer the correct amount into the right receiver.

This paper proposes a solution to the “Silent Banker” problem through blocking possible security vulnerabilities that Silent Banker can penetrate the security system through. The necessary tests were held through this thesis to prove the validity of the proposed solutions.

Three main phases are presented which are: phase (0): Lock the browser, phase (1): Encryption and phase (2): Decryption; all are combined in order to introduce the best results in preventing the Silent Banker attacks. Results showed that the banking side presents major role in the detection process as
checking whether the transfer process was successful so to successfully transfer the amount and without any error through, or to inquire both bank and client sides about the failures if not.


In the Internet world, data centers or network servers are anticipated to be the bottleneck in hosting network-based services, even though the network bandwidth continues to increase faster than the server capacity. Most of the research is going on to minimize the response time of a Web server one of the most popular protocol is Secure Sockets Layer (SSL). This is to provide a secure channel between a client and a cluster-based network server, its high overhead degrades the server performance considerably and, thus, affects the server scalability. Therefore, improving the performance of SSL-enabled network servers is critical for designing scalable and high-performance data centers. In this paper, we examine the impact of SSL offering and SSL-session-aware distribution in cluster-based network servers. In a back-end forwarding scheme, called ssl_with_bf, that employs a low-overhead user-level communication mechanism like Virtual Interface Architecture (VIA) to achieve a good load balance among server nodes. The experimental results with 16-node and 32-node cluster configurations show that, although the session reuse of ssl_with_session is critical to improve the performance of application servers the ssl_with_bf scheme can minimize the average latency by about 40 percent and improve throughput across a variety of workloads.

Meenu, Prabhat Kumar Pankaj and Tarkeshwar Nath, September 2011

This paper addresses the issue network security. The entire bank provides 128 bit ssl encryption in two way communication between client and server. This paper gives the mechanism behind 256 ssl encryption. By which two way communications is much secure (i.e.: using of secure socket layer 3.0)
This paper about the development of pervasive computing has put the light on a challenging problem: how to dynamically compose services in heterogeneous and highly changing environments? This paper proposes a survey that defines the service composition as a sequence of four steps: the translation, the generation, the evaluation, and finally the execution. With this powerful and simple model we describe the major service composition middleware.

Because of the speed, flexibility, and efficiency that it offers, the Internet has become the means for conducting growing numbers of transactions between suppliers and large international corporations. In this way, the Internet has opened new markets to the world and has accelerated the diffusion of knowledge. The meaning of Internet markets or online business has been widely used in these days. The success of the business depends on its flexibility, availability and security. Since that the web-based systems should have a special way to design the system and implement it. Nowadays, the Internet Banking System widely used and the banks looking to provide the best quality system with highly available, fast response, secure and safe to use. The Unified Modeling Language (UML) is the uniquely language which is used to analyze and design any system. In this paper, the UML diagrams has been proposed to illustrate the design phase for any banking system and presented two types of architecture which is used for the Internet Banking System.
Jean-Michel Sahut 2008

The paper provides objective explanations of the success factors of Internet payment systems, and the domination of SSL card payment in the market (Turban and Alii, 2006). Moreover, unsuccessful experiences show that it is necessary to consider network effects (Shapiro and Varian, 1998; Shy, 2001) and which business models to implement in order to avoid killing a new Internet payment system before it is launched. This article investigates also the stakes for the banking environment of the Internet payment systems and the problem of money creation.

Zachary B. Omariba, Nelson B. Masese and Dr. G. Wanyembi July 2012

This paper will first discuss the drivers of electronic banking; secondly, it will talk about the concerns about e-banking from various perspectives. Thirdly, the security and privacy issues will also be discussed, and fourthly the attacks of electronic banking with their solutions are discussed.