International Conference on Innovative Research in Science, Technology and Management
Modi Institute of Management & Technology, Dadabari, Kota, Rajasthan (ICIRSTM-17)
22nd-23rd January 2017 , www.conferenceworld.in ISBN: 978-93-86171-20-7

CLOUD SECURITY CONCERNS IN THE EMERGING CASHLESS ENVIRONMENT

Khurram Zaman

Research Scholar, Department of computer science and Technology,
Career Point University, Kota, Rajasthan

ABSTRACT

Cloud computing plays a pivotal role in the emerging cashless environment. In view of the prevailing scenario of E-commerce and trade, this paper explains about various applications of cloud computing system. It further highlights the cloud security concerns pertaining to cashless transactions and concludes with some solutions and recommendations.

Keywords- Application, Cloud, Computing, Cashless, Security.

I. INTRODUCTION

Advances in ICT have tremendously changed the way of using internet from simple network to more sophisticated and scalable data centre with huge storage capacity and processing capability. These data centres are integrated to provide services on-demand like hardware, software and data resources to the users. ICT has thus largely touched almost every aspect of our life and made our life inescapably dependent.

Cloud computing system provides on-demand services on internet such as **SaaS** (Software as a service - mostly being adopted by large organizations wherein users rent or borrow online software instead of purchasing and installing it on their own computers; **PaaS** (Platform as a service **-** mainly used by research organization and institutions, user can work on any Operating System of his choice on rent,); and **IaaS** (Infrastructure as service – used by small or medium business organizations with small funds for establishing their resource infrastructure, they use on demand scalable cloud hardware resources as service on certain rent).

In this era of competition, every organization is trying to have an edge over its competitor by moving fast towards on-demand and scalable cloud environment so that better options could be provided to users. The e-commerce organisations endeavour to place their web applications and services on private clouds and installing data-centre for cost advantages and up-scaling. With growing awareness among the internet users and advancement in e-commerce, nearly half of the global business is being done cashless via payment gateways, which are cloud based web services and act like interface between vendors' e-business and online customers. The beginning for cashless economy since the demonetization spree, the payment gateways gained huge popularity for making digital money transactions so easy. There are various modes of cashless environment which, among others, include Debit, Credit ATM Cards, Internet banking, Mobile banking etc. In spite of advantages of scalability and cost effectiveness of cashless transactions, e-business on cloud has alarmed of

certain security concerns. Therefore, in this context, the present paper highlights some cloud security risks and recommends solution for secured and trusted cashless transaction.

II. CASHLESS TRANSACTIONS IN CLOUD COMPUTING ENVIRONMENT

Although, we are moving slowly and steadily towards a cashless transaction environment but cash will continue to remain the mode of transaction in the foreseeable future. Cloud computing environment plays a pivot role in the fundamental shift the way that consumers and businesses make and receive payments today with a major emphasis on speed and transparency. More and more businesses are adopting **SaaS** technology platforms to streamline outdated processes, but when it comes to the movement of money, change has come slowly. Integration of cloud based Saas APIs in ecommerce is trying to bridge the gap between cloud technology and finance, and giving aging companies a new lease on life in the process. **Payments-as-a-Service** platform is being increasingly adopted in the larger enterprises, where its fixed-cost SaaS model can dramatically cut the fees and overhead currently associated with B2B payments.

Businesses in cashless transaction require increasingly "open" infrastructures that can integrate with internal systems such as accounting and procurement platforms. Cloud-based technology platform allows companies to fully outsource their international payments, while linked to the global banking network, and automates all the processes around it with transparency of delivery of payment and cost. By plugging into APIs, businesses can escape the heavy payments for infrastructure in order to focus on their core business. Companies using cloud environment for digital money transactions include banks, payment service providers, large e-commerce businesses, FX brokers, remittance firms, card processors, prepaid card companies and business payment firms.

III. MODES OF CASHLESS TRANSACTIONS

Technological advancements have changed the face of trade and commerce to e-commerce by means of digital/cashless transactions. For the purpose of study, cashless transaction modes can be understood as card-based or software based product services.

3.1. Card-based Mode of Cashless Transactions

The Card-based transactions are issued by banks such as Visa and MasterCard are networks that process payments between banks and merchants for purchases made with the cards. Payment networks offer cardholders added perks such as rental car insurance, fraud security and payment protection.

3.2. Card-less Mode of Cashless Transactions

A payment gateway is a merchant service provided by an e-commerce application service provider that authorizes credit card or direct payments processing for e-businesses. The payment gateway may be provided by a bank to its customers, but can be provided by a specialised financial service provider as a separate service.

A payment gateway facilitates a payment transaction by the transfer of information between a payment portal (such as a website, mobile phone or interactive voice response service) and the front end processor or acquiring bank.

3.3. Wire Transfer

A wire transfer sends money electronically through wire networks. To receive a wire transfer**,** the receiver needs to have an account number and a wire transfer routing number**.** International wires require a SWIFT code instead of the wire transfer routing number. Sending a wire transfer takes place at the sender's bank, over an internet banking website, or with companies that process wire transfers, like Western Union.

3.4. The 'Online Banking'

The 'Online Banking' allows a user to execute financial transactions via internet. Online banking is also known as "internet banking" or "web banking". An online bank offers customers just about every service traditionally available through a local branch, including deposits, which is done online or through the mail, and online bill payment.

3.5. Cashless Economy, Replaces Cash on Delivery by Simple UPI Apps

The Prime Minister Nadenra Modi proclaimed the vision of his Government of a cashless economy, by which, two technologies come to our mind - Unified Payments Interface (UPI) and Payment Wallets. Let us understand as to how UPI can replace the existing CoD (Cash on delivery) payment.

The UPI is a payment system that allows users to transfer money without giving bank details like card number, IFCI code etc. All that needed is a virtual identity number, like an ADHAR number for banking transaction, it can be any like .... (abhay123@icicibank). However, in India, cash on delivery (CoD) is one of the most preferred methods of payment and according to business insider, nearly 83% of consumers prefer it for online purchase. As contrary to CoD, with UPI, customers can make payment to e-commerce companies by using only a missed call and sms reply. It does not need any app or internet connection on mobile phone.

IV. ADVANTAGES OF CASHLESS TRANSACTIONS

In spite of many odds, the cashless transaction system has several advantages such as it:

- *Reduces chances of errors:* by escaping from entering transaction amounts at both the cash register and processing terminals
- *Creates transaction database:* transaction information in the database for a long time is stored
- Increases accountability: it is easy to confirm whether you have received the proper amount of credit for each transaction
- *Minimizes frauds:* by using Address Verification (AVS) the chance of shipping to someone using a stolen credit card are eliminated
- *Saves time:* allows users to do multiple transactions as a batch and reduces authorization time
- *Saves money:* multiple registers can share a single modem and phone line
- *Lowers transaction costs*: electronic processing is faster and less expensive than paper processing
- *Expedites billing process:* it is easy to schedule transactions to be processed according to the specific billing requirements.

V. SECURITY CONCERNS

The transaction model (SaaS) of Cloud based business applications is perhaps the most sensitive model as regards the security concerned. Since a lot of commercial information is made available and transmitted through internet, data security becomes a critical issue.

In *Software as a Service (SaaS) model*, the client remains dependent on the service provider for proper security measures of the system. The service provider must ensure that their multiple users do not get to see each other‘s private data. Thus, it becomes important to the user to get ensured that the right security measures are in place and need to have the assurance that the application will be available when needed. Cloud computing providers need to provide some solution to resolve the common security challenges that traditional communication systems often faces. At the same time, they also have to deal with other issues inherently introduced by the cloud computing paradigm itself. The following security concerns are to be taken into consideration while undertaking cashless transactions:

5.1. Authentication and authorization

The authorization and authentication of applications used in enterprise environments need to be changed so that they can work with a safe cloud environment. Forensics tasks will become much difficult for investigators to access the system hardware physically.

5.2. Data confidentiality

Confidentiality may refer to the prevention of unintentional or intentional unauthorized disclosure or distribution of secured private information. Confidentiality is closely related to the areas of encryption, intellectual property rights, traffic analysis, covert channels and inference in cloud system. Whenever a business, a government agency, an individual or any other entity wants to share information over cloud, confidentiality or privacy is needed to be asked.

5.3. Availability

The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The availability is one of the big concerns of cloud service providers. If the cloud service is disrupted or compromised in any way, it affects large number of customers than in the traditional model.

5.4. Information Security

In the SaaS model, the data of enterprise is stored outside the enterprise boundary, which is at the SaaS vendor premises. Consequently, these SaaS vendors need to adopt additional security features to ensure data security and prevent breaches in the wake of vulnerability of security. This will need the use of very strong encryption techniques for data security and highly competent authorization to control access the private data.

5.5. Data Access

Data access issue is mainly related to security policies provided to the users while accessing the data. Organizations have their own security policies based on which each employee can have access to a particular set of data. These security policies must be adhered to by the cloud to avoid intrusion of data by unauthorized users. The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization.

5.6. Network Security

In a SaaS deployment model, highly sensitive information is obtained from various enterprises, then processed by the SaaS application and stored at the SaaS vendor‘s premises. All data flow over the network has to be secured in order to prevent leakage of sensitive information.

5.7. Data breaches

Since data from various users and business organizations lie together in a cloud environment, it remains in vulnerability as the clouds are always the potential target.

5.8. Identity management and sign-on process

Identity management (IdM) or ID management is an area that deals with identifying individuals in a system and controlling the access to the resources by placing restrictions on the established identities. Area of IdM is considered as one of the biggest challenges in information security. When a SaaS provider wants to know how to control who has access to what systems within the enterprise, it becomes a lot more challenging task.

VI. SECURITY THREATS

A cloud SaaS model is a platform for the cloud based APIs and application used by B2B and B2C merchants to implement these application services in e-commerce (cashless). Nearly all payment gateways, banks and ecommerce business websites place their mobile application on public SaaS model of cloud environment like Google play for android and iCloud for iOS mobile devices for users. Technically Cloud environment works on virtualization of resources (software or hardware). Virtualization is a key enabling technology for evolution of Cloud computing into its current form. In particular, virtualization has enabled IaaS and SaaS providers to efficiently use the available hardware and software resources in order to provide computing and storage services to their clients. Virtualization helps IT organizations in optimizing their application performance in a cost-effective manner but poses its application delivery challenges that cause security concerns in the Cloud computing environment. Nevertheless current interest in virtualization mostly revolves around virtual servers/machines as it can result in significant cost savings. The virtual machine (VM), which refers to a software computer like a physical computer, runs an operating system and applications. In the hypervisor, all users see their systems as self-contained computers isolated from other users, even though every user is served by the same machine. In this context, a Virtual Machine is an operating system that is managed by an underlying control program.

6.1. Virtual machine level attacks:

Potential vulnerabilities are the hypervisor or Virtual machine technology used by cloud vendors are a potential problem in multi-tenant architecture. These technologies involve "virtual Machines" remote versions of traditional on-site computer systems, including the hardware and operating system. The number of these virtual Machines can be expanded or contracted on the fly to meet demand, creating tremendous efficiencies.

6.2. Cloud provider vulnerabilities:

These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability that exist in cloud service layer which cause insecure environment.

6.3. Expanded network attack surface:

The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases.

6.4. Authentication and Authorization:

The enterprise authentication and authorization framework does not naturally extend into the cloud. Enterprises have to merge cloud security policies with their own security metrics and policies.

6.5. Lock-in:

It seems to be a lot of angst about lock-in in cloud computing. The cloud provider can encrypt user data in particular format and if user decides to migrate to another vendor or something like.

6.6. Data control in cloud:

For midsize businesses used to having complete visibility and control over their entire IT portfolio, moving even some components into the Cloud can create operational "blind spots", with little advance warning of degraded or interrupted service.

6.7. Communication in virtualization level:

Virtual machines have to communicate and also share data with each other. If these communications didn't meet significant security parameters then they have potential of becoming attacks target.

Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DoS attacks against cloud itself or arranging another user in the cloud. For example an attacker knew that his victim is using cloud vendor with name X, now attacker by using similar cloud provider can sketch an attack against his victim(s). This situation is similar to this scenario that both attacker and victim are in same network but with this difference that they use virtual machines instead of physical network

VII. SOLUTIONS AND RECOMMENDATIONS

In view of the above risks and threats, this paper provides some features to virtualization architecture in order to improve the security for cloud environment which is shown in the Fig.1

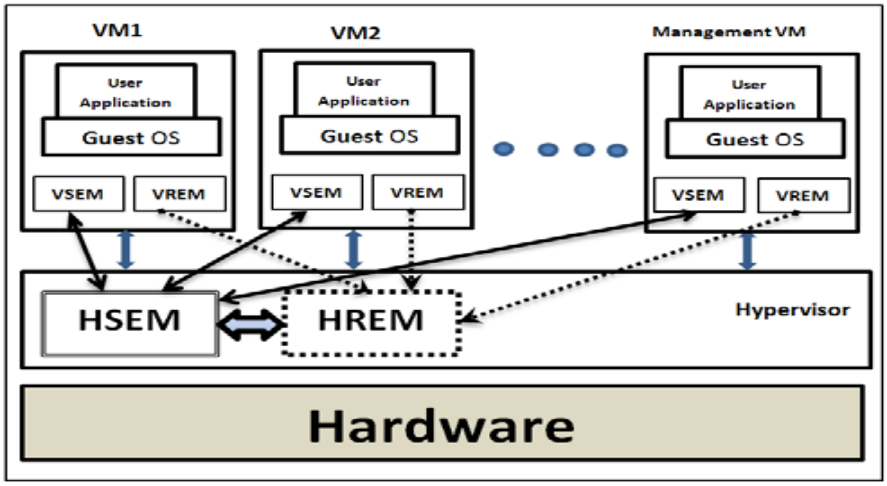

Fig.1

7.1. VM Security Monitor (VSEM)

There is a VSEM within every virtual machine (VM) that runs in a virtual environment. These monitors act as sensors, but are different from sensors. In fact, VSEM is a two-level controller and behaviour recorder in the cloud system that helps HSEM (hypervisor security monitor) identify attacks and malicious behaviour with less processing. VSEM monitors the security-related behaviours of VMs and reports them to HSEM. As there are a large number of transmissions in cloud and sending all of them to HSEM consumes a lot of bandwidth and processing resources, which can affect general hypervisor activity, some tasks were done by VSEMs in VMs such as collecting information that is asked by HSEM. Moreover, because the users do not want to consume

their resources, which they paid for, VSEMs have two levels of monitoring that consume more resource only when it is necessary. Actually, each level of VSEM is monitored almost the same events but at different levels.

Level 1: the VSEMs monitor their own VMs. In this level VSEM collects the source and destination addresses which are in head of data, number of unsuccessful and successful tries in sending data, and number of requests that were sent to the hypervisor. At this level, VSEM, according to the brief history of the VM which provided by HSEM, looks for anomaly behavior (HSEM has had history of VMs in more details). For instance, the system identifies the VM as a potential attacker or victim if the number of service requests from the hypervisor is higher than average based on the history of requests of the VM. If abnormal behavior is detected, or the type of sending data and unsuccessful tries increase above that threshold (according to history of theVM), then VSEM switches to *Level 2* and also notify HSEM about this switching in order to HSEM investigates the VM for finding malicious activities.

Level 2: In this level, the VSEM monitors and captures the activity of the VM in more detail, such as VM's special request from the hypervisor, details of requested resources (e.g. the number of requests), and the destination transmitted packets (to recognize if it is in the same provider's environment or outside). In this mode, VSEM notifies HSEM about the level of monitoring in the VM. According to this notification, the hypervisor sets activity limits in types of activities until HSEM learns that the VM is not an attacker or victim. At this level, HSEM makes a request from VREM about the reliability status of the VM, including the workload status and number of times when the VM workload was close to the maximum capacity of the VM.

7.2. VM Reliability Monitor (VREM)

VREM monitors reliability-related parameters, such as workload, and notifies the load-balancer (within the hypervisor) about the parameter results. VREM is also used for security purposes. The VREM sends useful information such as workload status to HREM and requests the status of the VM from HSEM, and then it decides whether to give the VM more resources. Actually, if the VM requests as many resources as it can (that is different behavior according to its usage history), it may signify an overflow of attack on victim. Therefore, proposed HREM can detect overflow attacks and notify the HSEM about it.

7.3. Anti-fraud Recommendations

Many payment gateways also provide tools to automatically screen orders for fraud and calculate tax in real time prior to the authorization request sent to the processor. Similarly, there are many tools to detect fraud which include *geo-location*, velocity pattern analysis, OFAC list lookups, 'black-list' lookups, delivery address verification, computer finger printing technology, identity morphing detection, and Anti-fraud face-recognition technology (AVS checks)**.** It works by taking a face picture of the beneficiary or sender and comparing it with a huge database of other faces captured during past transactions. It identifies if that face has performed a transaction under a different name, which will indicate identity fraud.

VIII. CONCLUSION

We are living in the era of ICT and the technology is transforming from the simple one to scalable on-demand cloud computing environment. Global business has expanded many times within a decade due to having switched over from traditional modes of trades to e-commerce which is mainly attributed to versatility, cost

effectiveness, speed and wide scope of ICT. Internet is just not a simple network but a web of networks on public, private and hybrid clouds of huge storage capacity, processing capabilities, scalability to serve the users on demand. Because of these properties of SaaS cloud model and environment, various merchants, vendors, banks, payment gateways and payment processors are attached to it globally that helps in e-commerce and cashless transactions in the cloud computing environment. In spite of tremendous advantages and huge usefulness of cloud computing environment, there are still security concerns due to various threats to the growing cashless transactions which needs to be duly addressed as recommended in this paper to create a secured cashless environment.

REFERENCES

[1] Mohamad Halaweh, Christine Fidler - " Security Perception in Ecommerce: Conflict between Customer and Organizational Perspectives". Proceedings of the International Multi-conference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9-2008-IEEE;

[2] Yuanqiao Wen, Chunhui Zhou "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management;

[3] Rui Wang, Shuo Chen "How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores". IEEE S&P‘11 proceedings;

[4] V.SRIKANTH "ECOMMERCE ONLINE SECURITY AND TRUST MARKS". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July- September (2012);

[5] Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012;

[6] Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues "Proceedings of the 35th Hawaii International Conference on System Sciences – 2002;

[7] Rashad Yazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"International Conference on Information Communication and Management - IPCSITvol.16 (2011);

[8] Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International;Conference on Software and Computer Applications-IPCSIT vol.9 (2011);

[9] RAJU BARSKAR, ANJANA JAYANT DEEN" The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology"(IJCSIS)-Vol. 8, No. 1, April 2010;

[10] Dr. Nada M. A. Al-Slamy, "E-Commerce security" IJCSNS - VOL.8 No.5, May 2008;

[11] W. Jeberson, Prof. (Col.). Gurmit Singh. "Analysis of Security Measures Implemented on G2C Online Payment Systems in India" MIT; International Journal of Computer Science & Information Technology Vol. 1 No. 1 Jan. 2011;