January to March, 2016

Trinity Tech Review

Vol. 2, No. (1) (5)

Disclaimer: The views and opinions presented in the articles, case studies, research work and other contributions published in Trinity Tech Review (TTR) are solely attributable to the authors of respective contributions. If these are contradictory to any particular person or entity, TTR shall not be liable for the present opinions, inadequacy of the information, any mistakes or inaccuracies.

Trinity Institute of Professional Studies
An ISO 9001:2008 Certified Institution
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)

Sector-9, Dwarka, New Delhi-110075

Ph: 45636921/22/23/24, Telefax : 45636925
www.tips.edu.in, tips@tips.edu.in

TRINITY INSTITUTE OF PROFESSIONAL STUDIES
Sector-9, Dwarka Institutional Area, New Delhi-110075, Tel: 011-45636921/22/23/24
Certified as "A+" Grade Institution by SFRC, Govt. of NCT of Delhi
ISO – 9001:2008 Certified
Affiliated to GGSIP University

STATEMENT ABOUT OWNERSHIP AND OTHER DETAILS OF
TTR/TMR FORM 5 (RULE 8)

1.	Printer‟s Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
2.	Place of Publication	:	Delhi
3.	Periodicity of Publication	:	Quarterly
4.	Publisher‟s Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
5.	Editor‟s Name	:	Dr. J.P. Singh/ Dr. L.D. Mago
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
6.	Name and Address of the individual who owns the journal and partners or shareholders holding more than one per cent of the capital.	:	CHAIRMAN Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
7.	Hosted at (url)	:	www.tips.edu.in

I, Dr. R.K. Tandon, hereby declare that the particulars given above are true to the best of my knowledge and belief.

Dr. R.K. Tandon

Introduction

This issue of Trinity Tech Review has prime focus on Technological Security Mechanisms. The Issue encompasses articles that give a bird's eye view of what are the new threats that stand before us in our pursuit of technological advancements and betterment of quality of human life. We also bring to you the upcoming solutions to these threats and what answers does technology hold in quest for a more secure and safer internet experience. Readers will agree that we are constantly faced by more complex and obscure intrusions motivated by malicious intentions to hamper personal or organizational privacy, financial growth, brand image and overall functioning. Therefore, this issue of TTR becomes more relevant in the light of the threats we face, online or offline. However, don't lose hope! We offer options for remedial actions and latest advancements that promise mitigation of risk. Our first article, "A Robust Enterprise Architecture and is Security Issues", explains how a strategically placed and designed organizational network architecture can safeguard the dissemination of crucial and confidential information. In the second article, "A Study of Digital Signature: Its Easy for Anyone to Verify a Message in Information and Communication Technologies", elucidates how one can use his unique digitised "signature" to protect and validate a message over a network preventing unauthenticated access. In the article, "A Study of Potential Threats of Data Mining to Privacy in the Retail Sector" brings to light a long speculated danger: The invasion of consumer privacy to boost sales. Our next article, "Roadmap for Usability Evaluation Techniques" highlights what it takes to evaluate new software on the basis of usability, reliability and security. It also elaborates the tasks undertaken to ensure the quality of the software before it is released. The last article, "The Study of Cloud Security in Insurance Industry with respect to Indian Market" talks about the concerns of safeguarding information on the Cloud especially when it comes to health related financial expenses. We are sure you are going to enjoy the compilation thoroughly. Happy Reading!

A Robust Enterprise Security Architecture and Its Security Issues

Anil Sharma

Abstract

Enterprise security architecture is a very important framework for balancing business and Information Technology and for adding value to an organization. Security is also nowadays an essential dimension for enterprises. It can prevent confidential information from being leaked or stolen, lost succumbing to other serious disasters. Security architecture is a concept that aims to design an infrastructure of information systems to ensure that they provide enough security to organizations and businesses. Today, most businesses rely on IT more heavily than in the past. Carelessly designed security architecture has serious implications for a business, such as high risk of being unable to do daily business operations. This heavy reliance on information systems highlights the importance of developing efficient and effective security architecture within the entire enterprise.

Emphasizing security technology alone is not enough to produce effective and efficient security for an entire organization. Security technology itself is designed to resolve security issues without considering other factors, such as cost and business operating models. Businesses differ in terms of organizational scopes, sizes, capital capacities, business operating models and top management support. These factors affect the security needs and the security trust level. This study discusses security architecture framework as a basis for developing enterprise security architecture. With such a framework, developers can clearly understand the security needs of businesses and the priority of implementing security projects in a specific time period and in a specific manner.

Keywords: Enterprise Security, Security Architecture, Risk Management, Security Management, Threat Management, Data Management

Introduction

Security architecture is a cohesive security design, which addresses the requirements (e.g. authentication, authorization, etc.) and in particular the risks of a particular environment and specifies what security controls are to be applied where [1]. Security architecture is a concept that aims to design an infrastructure of information systems to ensure that they provide enough security to organizations and business. Security architecture is divided into three broad categories viz. Product Security Architecture, Enterprise Security Architecture, Application Security Architecture[2]. Enterprise Security Architecture needs to address applications, infrastructure, processes as well as security management and operations. The purpose of the security architecture is to bring focus to the key areas of concern for the enterprise, highlighting decision criteria and context for each domain.

Security Architecture Framework

The purpose of security architecture framework is to bring focus to the key areas of concern for the enterprise, highlight

decision criteria and context for each domain. Since security is a system property which should be focused at different system layers and its role in the system as a whole [2].

This framework provides a basis for understanding disparate design and process considerations; to organize architecture and actions towards improving enterprise security. The security architecture framework depicts an approach to map the system stockholder's conceptual goals to a logical view of security, which is set of security policy and standards, security architecture and risk management domains. The decisions in logical layer drive the security processes, defense in depth services and security matrices through design time to run time. Fig.2 shows the different components of security architecture framework as:

Stakeholders

The stakeholders business and risk goals drive the overall security architecture. The challenge for enterprise security groups is to identify stakeholders in the enterprise that

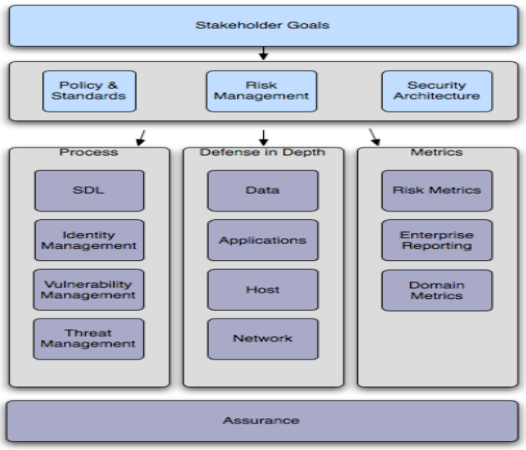


Fig. 1: Security Architecture Framework

have a stake in the system's security posture and to educate them about the actual risks and available countermeasures; finally giving the stakeholders' their own, custom metrics, tools and process they can bring to bear on the problem.

Risk management

Risk is comprised of assets, threats, vulnerabilities, and countermeasures.

$$\text{Risk} = \left(\frac{\text{Threats x Vulnerabilities}}{\text{Countermeasures}} \right) \text{x Assets}$$

Fig. 2: Risk Equation

A risk management centric approach allows for the security architecture to be agile in responding to business needs. Risk is a function of threats exploiting vulnerabilities against assets [3]. The threats and vulnerabilities may be mitigated by deploying countermeasures. The risk management process implements risk assessment to ensure the enterprise's risk exposure is in line with risk tolerance goals. The role of the security architecture is not to steer the business away from risk, but rather to educate their business partners about the risks they are taking and provide countermeasures that enable the business to take as much risk as suits their goals.

Security Policy and Standards

Organizational policies and standards that govern the system's design, deployment, and run time are termed as Security policy and Standards. The security policy describes both what is allowed as well as not allowed in the system. Security standards should be prescriptive guidance for people building and operating systems, and should be backed by reusable services wherever practical. Security policy and standards are

not end goals in themselves, they need to be backed by a governance model that ensures they are in use, and that it is practically possible to build, deploy, and operate systems based on their intent [2].

Security architecture

Security Architecture is the unifying framework and reusable services that implement policy, standards, and risk management decisions. The security architecture is a strategic framework that allows the development and operations staff to align efforts, in addition the security architecture can drive platform improvements which are not possible to make at a project level.

The security architecture delivers improved XML/ Web services security, a simplified programming model for developers, and saves development costs, because the wheel is not reinvented multiple times [2]. Risk management, security policy and standards, and security architecture govern the security processes and defense in depth architecture through design guidance, runtime support, and assurance services. Security metrics are used for decision support for risk management, security policy and standards, and security architecture.

Security processes

Security processes carry out the intent of the enterprise risk management, security policy and standards, and security architecture. They are broken into discrete domains because they solve very different problems, and require different staffing, support models, and success criteria.

SDL

Security functions as a collaborative design partner in the software development lifecycle (SDL), from requirements, architecture, design, coding, deployment and withdrawal from service [4]. Security adds value to the software development lifecycle through prescriptive and proscriptive guidance and expertise in building secure software. Security can play a role in all phases of the SDL, but an iterative, phased-based integration of security into the SDL is the wisest path, each additional security process improvement must fit with the overall SDL approach in the enterprise.

Identity management

Identity Management deals with the creation, communication, recognition and usage of identity in the enterprise. Identity management includes provisioning services, directories, multi-factor authentication, federation, and so on. All access control is predicated on identity, a central concern to security architecture, the quality of the system's authentication and authorization cannot be stronger than the identity management process. Identity management architecture is important to identify points of leverage across projects, because identity management components are often not able to support a business case individually [2, 4]. The net benefit is to improve the authentication, authorization, and auditing services for the system as a whole. The utility of the identity management architecture comes through mapping the subject request's claims (or assertions) to policy enforcement decision workflow; and the object's protection model, often in the form of group and/or role membership.

Threat Management

Management of threats to systems such as virus, trojans, worms, malicious hackers and

intentional or unintentional system misuse by insiders or outsiders is called Threat management. Threats differ from vulnerabilities in that threats are the actors that breach or attempt to breach security policies and mechanisms. The security gaps that are exploited by threats are called vulnerabilities [3]. Threat Management tools and processes include: Security Monitoring, Web Application Firewall, Security Incident Management Processes, Security Event Management System, Incident Response Planning Processes, cryptography, and Forensic Analysis Process and Tools.

The threat environment is inherently unpredictable and in large part out of control of the enterprise. Developers can assist the security team in understanding attack vectors and signatures to monitor for, but it is impossible to predict all threats, meaning that threat management has a large detection and response component. Monitoring systems and audit services at various levels in the system can identify threats that circumvent expected paths and controls.

Vulnerability management

The set of processes and technologies for discovering, reporting, and mitigating known vulnerabilities is known as vulnerability management [5]. The vulnerabilities may reside at any system layer – database, operating system, servers, and so on; specialized tools probe for known vulnerabilities. It is important to differentiate threat management and vulnerability management. The threat environment contains many unknown mysteries around attacker techniques and goals, attackers will identify currently unknown vulnerabilities (zero day attacks), but there are many known vulnerabilities that the security team can act on, while the threat landscape is inherently less predictable meaning security is reactive to threats and can be generally proactive towards dealing with known vulnerabilities.

Defense in depth

Defense in depth is predicated on the notion that every security control is vulnerable somehow, but that if one component fails another control at a separate layer still provides security services to mitigate the damage. Each level of the defense in depth stack has its own unique security capabilities and constraints. The core security services - authentication, authorization, and auditing apply at all levels of the defense in depth stack, for example audit logging occurs at network, host, application, and data access levels.

Network security

Network security mechanisms, such as network firewalls and network intrusion detection devices, are generally a convenient and scalable point to apply security controls and are an important locale for defining chokepoints and zones. Zones define logical and/or physical boundaries around a group of systems, for example the DMZ pattern in web applications [3]. Chokepoints define places to cross boundaries into and out of zones, where special security considerations apply.

Host security

It is concerned with access control on the servers and workstations. Host Intrusion Detection Systems identify host anomalies and security events [6]. Host Integrity Monitoring checks and protects the integrity of the critical files and programs on the host. Baseline Configuration Scanners provide assurance that the systems in use in the field meet the policy and standards at a granular

level. These scanners may be automated to support highly distributed and large scale environments.

Application security

It deals with two main concerns: 1) protecting the code and services running on the system, who is connecting to them, and what is output from the programs through a combination of secure coding practices, static analysis, threat modeling, participation in the SDL, application scanning, and fuzzing. 2) Delivering reusable application security services such as reusable authentication, authorization and auditing services enabling developers to build security into their system [7].

Data security

Deals with securing access to data and its use, this is a primary concern for the security architecture and works in concert with other domains. Vulnerability management tools conduct specialized scans against database hosts. The SDL defines secure patterns for database integration based on data classification defined in the policy. Database intrusion detection and monitoring provides ongoing intelligence as to the threats against the database. The value in performing detection and monitoring at this layer is that attackers may not traverse the expected path to get to the asset that the security system is trying to protect: data.

Metrics

Security metrics are a basis for assessing the security posture and trends of the systems. The security metrics data is fed forward to inform future assessments, risk management decisions, and overall security architecture, in an iterative fashion. Metrics provide a way to assess security through qualitative and quantitative analysis. The goal of security metrics is objective measurement that enables decision support regarding risk management for the business without requiring the business to be information security experts to make informed choices.

Risk metrics

It measure the overall assets, and their attendant countermeasures, threats, and vulnerabilities. Since risk metrics are focused on assets, they allow the security architecture to be measured in business terms [8]. Risk metrics inform stakeholders on security posture based on information that is harvested from the security processes, especially vulnerability management and threat management and the defense in depth stack.

Enterprise reporting

It is an enterprise view of security and risk. Enterprise reports show the states and rates of security, they can show which areas deserve additional focus and where the security services are increasing or decreasing the overall risk exposure. Enterprise reports are rolled up versions of domain metrics and risk metrics. The audience of the enterprise security metrics report will govern what areas are highlighted in the report. The importance of the enterprise security metrics report is in its objective and quantitative nature, which allows for ongoing assessment of security states and rates of change.

Domain specific metrics

Domain specific instrumentation of metrics for example vulnerabilities not remediate, provide granular view of security in a system. These can be aggregated into risk metrics and enterprise reporting formats.

Run time metrics, such as alerts and warnings can be used to understand the security events that are visible across a number of systems.

Assurance

Assurance is the set of activities that create higher confidence in the system's ability to carry out its design goals even in the face of malicious abuse. These activities are performed by, or on behalf of, an enterprise as tests of the security practices. Activities include penetration testing, code auditing and analysis, and security specific hardware and software controls. Assurance activities are applied to all of the core security services – protection, detection, and response [9]. The security architecture should identify areas where assurance services can be leveraged across the multiple projects. For example where multi-factor authentication is federated across domains or where an XML security gateway provides reusable input validation and authentication services for multiple web services.

Security architecture Lifecycle

Risk management process drives the security architecture and implementation of the overall enterprise security framework. The security architecture process is an iterative

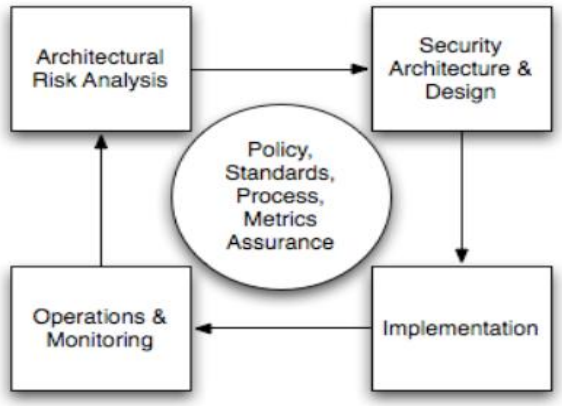


Fig. 3: Security Architecture Lifecycle

process that unifies the evolving business, technical, and security domains [10]. The four main phases in the process are: Architecture Risk Assessment, Security Architecture & Design, Implementation, and Operation & Monitoring.

Architecture Risk Assessment

It assesses the business impact to critical business assets, the probability and impact of security threats and vulnerabilities [11]. Since security is a system property, the architectural level is the proper level of abstraction to identify many of the most critical security flaws. The DHS Build Security In paper "Architectural Risk Analysis"6 defines a method for assessing the application's assets, threats, and vulnerabilities.

Security Architecture and Design

Architecture and design of security services that enable business risk exposure targets to be met. The policies and standards, and risk management decisions drive the security architecture and the design of the security processes and defense in depth stack [11].

Implementation:

Implementation security processes and services implemented, operational and managed. Assurance services are targeted at verifying that the Risk management, Security Policy and Standards, Security Architecture decisions are reflected in the actual runtime implementation.

Operations and Monitoring

Ongoing processes, such as vulnerability management and threat management that monitor and manage the operational state as well as the breadth and depth of systems security. Operational and monitoring processes should be instrumented with security metrics to better measure the runtime environment.

Conclusion

Security is important for all organizations especially for large enterprises. Inappropriate security management can allow critical events to threaten an organizations bottom line through the loss of reputation, customer's trust, fortune, confidential information and so on. Incorporating a security dimension to enterprise architecture framework allows development team to align business and IT security and to transform business needs into IT security business value.

Applying the framework discusses here can help organizations to pin point security strength, weakness and CSF (Critical Success Factors) with ease [11]. Gap analysis can help developer's priorities success factors and identify CSF for achieving security goals. Enterprise Security Architecture focuses on integrating the security dimension into Enterprise Architecture and is intended to serve as an Enterprise Security framework to assist an organization in successfully and effectively implementing security.

References

[1] Boh, W. F., & Yellin, D. (2006). Using Enterprise Architecture Standards in Managing Information Technology. Journal of Management Information Systems, 13(3), pages 163-207.

[2] Fumy, W., & Sauerbrey J. (2006). Enterprise Security: IT Security Solutions: Concepts, Practical Experiences, Technology. Berlin: Publics Corporate Publishing.

[3] Harris, S. (2005). All-In-One: CISSP Exam Guide. California: McGraw-Hill Companies.

[4] Jackson, C. M., Chow, S., & Leitch, R. A. (1997). Toward an understanding of the behavioral intention to use an information system. Decision Sciences, 28(2), pages 357-389.

[5] Kearns, G. S., & Sabherwal, R. (2006). Strategic alignment between business and information technology: a knowledge-based view of behaviors, outcome, and consequences. Journal of Management Information Systems. 23(3), pages 129-162.

[6] Lam, W. (2005) Investigating success factors in enterprise application integration: A case-driven analysis. European Journal of Information systems, 14(2), pages 175-187.

[7] Martin, N. L., Pearson, M., & Furumo, K. (2007). IS Project Management: Size, Practices and The Project Management Office1,2. The Journal of computer Information Systems, 47(4), 52-60.

[8] Metastorm (2008). Metastorm releases enhanced ProVision enterprise modeling suite.

[9] Ross, J. W. (2003). Creating a strategic IT architecture competency: learning in stages. MIS Quarterly Executive, 2(1), 31-43.

[10] Sherwood, J. (2005). Enterprise security architecture: a business-driven approach. San Francisco: CMP Books.

[11] Spewak, S. H. (1993). Enterprise Architecture Planning: Developing a Blueprint for Data, Applications, and Technology, Wiley, New York, NY.

A Study of Digital Signature: Its Easy for Anyone to Verify a Message In Information and Communication Technologies

Harjender Singh

Abstract

The concept of a signature has been with us for centuries as a means to establish the authenticity of documents. A digital signature is a way to ensure that an electronic document (i.e. e-mail, spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and it has not been altered in any way instead of that person created it, i.e. it is the process of verifying that information is coming from a trusted source. It also provides the confirmation that the contents of the message to which it is attached have not been tampered from the sender to the receiver. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. Digital signatures rely on certain types of encryption to ensure authentication.

Digital signatures assure on certain types of **encryption** to ensure authentication.

Encryption

Encryption is the process of encoding messages in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted.
There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

Authentication

It is the process of verifying that information is coming from a trusted source.
The aim of this paper is to ensure how digital signature is applied on the

document, how its work and what techniques should be considered to use digital signature.

Key words: Digital signature, Authentication, Encryption, Symmetric Encryption etc.

Introduction

A digital signature is an **electronic signature** that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. It also ensures that the document is really from the sender and not from someone else while at the same time it ensures that the message that reaches the recipient is sent without any alterations.

Private Key – Used for making digital signature

Public Key – Used to verify the digital signature

There are several ways to authenticate a person or information on a computer:

Password

User name and password provide the most common form of authentication. It checks the pair against a secure file to confirm. If either the name or password does not match, then you are not allowed to login the page or further access the page.

Checksum

Checksums is the oldest methods of ensuring that data is correct and provide a form of authentication. A checksum is a count of the number of bits in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message. A checksum is determined in one of two ways, Let's us say that the checksum of a packet is 1 byte long, it means that it can have a maximum value of 255. If the sum of the other bytes in the packet is 255 or less, then the checksum contains that exact value. However, if the sum of the other bytes is more than 255, then the checksum is the remainder of the total value after it has been divided by 256. Look at this example:

Byte 1 = 212

Byte 2 = 232

Byte 3 = 54

Byte 4 = 135

Byte 5 = 244

Byte 6 = 15

Byte 7 = 179

Byte 8 = 80

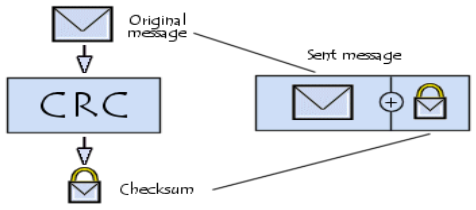
Total = 1151. 1151 divided by 256 equals 4.496 (round to 4).

Multiply 4 X 256 equals 1024.

So 1151-1024 **equals checksum of 127**

Cyclic Redundancy Check

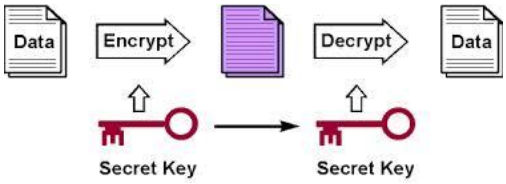
A cyclic redundancy check is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data i.e. it is a method of checking for errors in data that has been transmitted on a communications link. CRC, use polynomial division to determine the value of the CRC, which is usually 16 or 32 bits in length. CRC is very accurate and if a single bit is incorrect, the CRC value will not match up.



Private Key encryption

The private key is used to decrypt a message and transform it to a readable form i.e. each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to the other computer. Private Key encryption is essentially the same as a secret code that the two computers must each know in order to decode the information. The code would provide the key to decoding the message.

Eg : You create a coded message to send to a friend where each letter is substituted by the letter that is second from it. So "A" becomes "C" and "B" becomes "D". You have told a trusted friend that the code is Shift by 2". Your friend gets the message and decodes it.



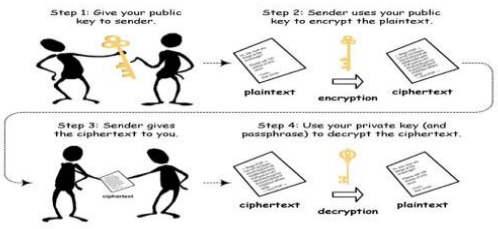
Public key encryption

Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use. It uses a combination of a private key and a public key. The key is based on a hash value. This is a value that is computed from a base input number using a hashing algorithm. Public key encryption is much more complex and required very large hash values for encrypting: 40-bit or even 128-bit numbers. A 128-bit number has a possible 2^{128} different combinations, i.e. it has many combinations as there are water molecules in 2.7 million Olympic size swimming pools.

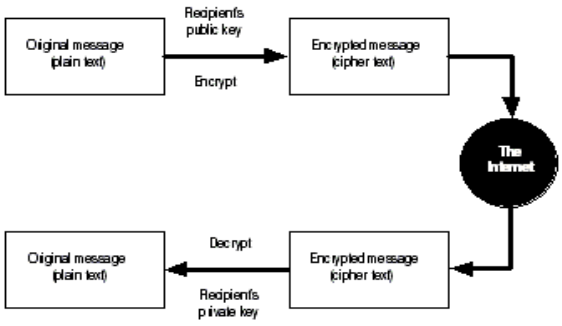
Input number 10667

Hashing Algorithm = Input # x 143

Hash Value = 1525381



Digital certificates: A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key used for encrypting messages and digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real.



Digital Signature: Today's Challenge

The concept of a signature has been with us for centuries to maintain the authenticity of documents. The paper documents are replaced by electronic documents and other digital assets such as messages, transactions, digital content, and software proliferate across every type of organization. Electronic versions of traditional signatures and watermarks provide some benefits but it provides lack of security. An organization used more secure platform to validate the authenticity and integrity of these electronic items and required that these items have not been changed maliciously or accidentally since they were created. When organization used digital transactions they need to establish a means of non-repudiation i.e. the ability to hold parties accountable for the transactions they execute. For this purpose most organization use digital signature.

Implement Digital Signature Technology: In customer-facing environments

Preparing your documents:

Document preparation support for creating reusable template documents and to locate and fix positions for signatures

Presenting the signer with the documents: This allows the signer to walk through the process of supplying signatures.

Document attachment: Additional documents such as a scanned passport, scanned driver's license or any other kind of document might be attached to the signed document.

Capturing the signer's intent to use an e-signature: It is recommended to capture the signature, and also to register the signer's intent and agreement to use digital signatures.

Comparison of signatures: Captured handwritten signatures may also be used for verification and authentication in critical processes.

Providing the signer with a copy of the signed document. Usually, the document is either printed out or sent via email to the signer.

Properties of a digital signature

Easy for the signer to sign a message

There is no point in having a digital signature scheme that involves the signer needing to use slow and complex operations to compute a digital signature.

Easy for anyone to verify a message

Similarly we would like the verification of a digital signature to be as efficient as possible.

Hard for anyone to forge a digital signature

It should be practically impossible for anyone who is not the legitimate signer to compute a digital signature on a message that appears to be valid.

How a Digital Signature Works

The use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature.

- **Digital signature creation** uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.

- **Digital signature verification** is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

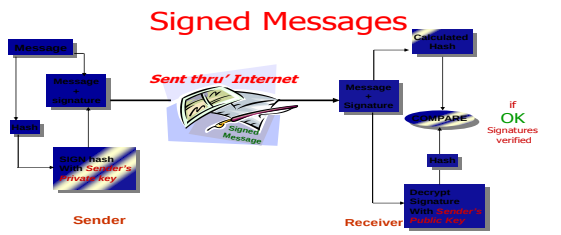
Example: Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

1. You copy-and-paste the contract (it's a short one!) into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.
2. Your lawyer then uses your public key to decrypt the message hash or summary.

3. If the hashes match, the received message is valid.



Security of digital signature

A signature scheme is secure (or unforgeable) if every feasible chosen message attack succeeds with at most negligible probability.
This digital signature scheme guarantees three information security properties:

Authentication

The signer is well identified by the private/public key relation.

Non-repudiation

The signing party cannot later on deny performing the action, since the private key was used for encryption process. Note that if a symmetric key cryptography was used, the non-repudiation properties could not be guaranteed.

Integrity

Since the signature itself is associated to the content to the message, any message alteration would make the signature invalid. This also implies that the signature cannot be copied from one message and applied to another.

Advantages

The following are the main benefits of using digital signatures.

Authenticity

An electronic document signed with a digital signature can stand up in court just as well as any other signed paper document.

Non-Repudiation

Signing an electronic document digitally identifies you as the signatory and that cannot be later denied.

Speed

Businesses no longer have to wait for paper documents to be sent by courier. Contracts are easily written, completed, and signed by all concerned parties in a little amount of time no matter how far the parties are geographically.

Time-Stamp

By time-stamping your digital signatures, you will clearly know when the document was signed.

Imposter prevention

No one else can forge your digital signature or submit an electronic document falsely claiming it was signed by you.

Tracking

A digitally signed document can easily be tracked and located in a short amount of time.

Costs

Using postal or courier services for paper documents is much more expensive compared to using digital signatures on electronic documents.

Security

The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed, or altered while in transit.

Disadvantages

Just like all other electronic products, digital signatures have some disadvantages that go with them.

Certificates

In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates at a cost from trusted certification authorities.

Compatibility

There are many different digital signature standards and most of them are incompatible with each other and this complicates the sharing of digitally signed documents

Expiry

Digital signatures, like all technological products, are highly dependent on the technology it is based on. In this era of fast technological advancements, many of these tech products have a short shelf life.

Law

In some states and countries, laws regarding cyber and technology-based issues are weak or even non-existent. Trading in such jurisdictions becomes very risky for those who use digitally signed electronic documents.

Conclusion

'Digital signature' under the Information Technology Act, 2000, that this is not only essential aspect for creating secure environment for electronic transactions, but it create a sense of authentication and non-repudiation. Digital signatures have different properties and offer different guarantees to hand-written signatures. The security of digital signatures critically relies on the security of the keys that are used to create and verify them.

References

[1] Leung, Karl R.P.H.; Hui, Lucas C.K. "Multiple Signature Handling in Workflow Systems". 2000.

[2] Information security/cryptography - how digital signature verification process works - Information Security Stack Exchange.htm

[3] Information security/ DigiStamp Digital Signatures - Why and How .htm

[4] Introduction to Cryptography and Security Mechanisms 2005

[5] XML Digital Signatures Reference - MSDN - Microsoft

[6] An Introduction to XML Digital Signatures - XML.com

A Study on Potential Threats of Data Mining to Privacy in Retail Sector

Ankita

Abstract

Data mining technology provides a user-oriented approach to novel and hidden patterns in the data. Data mining is a process which finds useful patterns from large amount of data. This technology has been successfully applied in Science, Engineering and Technology, Medical Diagnose Systems, Marketing and Finance to assist new sightings and strengthen markets. Some of the organizations have adapted this technology to progress their businesses and found outstanding results. In modern years, advances in hardware expertise have lead to an increase in the competence to store and record personal data about consumers and individuals. This has lead to concerns that the personal data may be misused for a variety of purposes. Because of data mining, even inexperienced users can connect data and make responsive associations. Therefore we must to implement the privacy of persons while working on practical data mining.

Privacy

According to Berry and Lineoff [1] privacy is a complex issue that, because of technology, is increasingly becoming a social issue. The Cambridge Advance Learner's Dictionary (2004), defines the word privacy as someone's right to keep their personal matters and relationships secret, Today, every form of commerce leaves an electronic trail, and acts that were once considered private or at least quickly forgotten, are stored for future reference.

It is an important issue to consider both as individuals and in the work we do that may intrude on the privacy of other.

Technology plays a role in defining privacy, protecting it, and intruding on privacy.

Data mining

Generally, data mining (sometimes called data or knowledge discovery) is the means of evaluating data from various viewpoints and compiling it into appropriate information - information that can be used to maximize revenue, minimize costs, or both. Data mining software is one of a number of analytical tools for evaluating data. It allows users to analyze data from

various different dimensions or angles, categorize it, and compiling the relationships identified. Technically, data mining is the process of determining correlations or patterns between dozens of fields in large relational databases.

Retail

Retailing can be defined as the promoting and selling of merchandise directly to consumers, augmented by advertising, store promotions, and personal contacts in the community where the retailer's outlet is located. Retailing is the selling of finished goods and services to the consumer for personal or family consumption.

Accounting for around 14-15 per cent of the gross domestic product (GDP), the Indian retail industry is likely to be worth around US$ 500 billion currently. Being one of the top retail markets in the world, India attempts tremendous extension to growth and opportunities in this area.

Importance of Data Mining in Today's Business World

Data and Information or Knowledge has an eloquent aspect on human activities. Data mining is the knowledge discovery process by evaluating abundant data from various panoramas and encapsulating it into fruitful information. Due to the importance of obtaining knowledge/information from the abundant data archives, data mining has transformed into an imperative element in various fields of human life.

Data Mining is by large used in several areas like understanding consumer research marketing, good analysis, demand and supply analysis, and e-commerce, investment trend in stocks & real estates, telecommunications and so on

Data Mining has great value in today's highly competing business environment. A new concept of Business Intelligence data mining has come into picture, which is mostly used by prominent corporate houses to stay ahead of their competitors. Business Intelligence (BI) can help in giving latest data and used for competition analysis, market research, economical trends, consume behavior, industry research, geographical information analysis and so on. Business Intelligence Data Mining assists in decision-making.

Famous data mining software programs are Connexor Machines, Free Text Software Technologies, Megaputer Text Analyst, SAS Text Miner, LexiQuest, WordStat, Lextek Profiling Engine.

Privacy Concerns

A recent article reported "Since the 1980s, computer scientists have been developing methods for designing privacy into new technologies and systems. One of their most important principles is data minimization. This means very carefully limiting the collection of personal data to that needed to provide a service – rather than storing everything that can be conveniently retrieved. Access to data should be limited within organizations, ideally held by the individuals it relates to, and restricted using encryption. And once

personal data is no longer needed, it should be deleted or anonymised." [2]

Applying data mining in retail

Data Mining has its great operation in Retail Industry as it gathers huge data from on sales, customer purchasing history, goods transportation, consumption and services. It is obvious that the amount of data gathered will continue to expand speedily because of increase in ease, availability and demand of web.

The Data Mining in Retail Industry helps in recognizing customer buying patterns and trends. This in turn improves quality of customer service and good customer holding and contentment.

Privacy concerns of data mining

In order to better recognize the impact of data mining on privacy, consider the following example of its potential application in the telecommunication industry. A cellular phone service provider has the technological ability to determine the location of any switched on cell phone in its coverage area. The cell phone service provider collects information about all its subscribers during the sale of a contract. Typical subscriber information that would be collected may include the following:

- Age
- Occupation
- Income
- Banking Details

The ability of the cell phone service provider to track the location of the cell phone, and therefore its owner, might yield the following information:

- The route typically traveled to and from work by the subscriber.
- Whether the subscriber travels during business hours, or spends most of the day in the office.

The cell phone service provider could make use of the gathered information to position its own advertising billboards more strategically, or to start its various branches at the appropriate shopping centers. At the same time however, the organization might decide to benefit from this knowledge by selling it off to other organizations. The information could for example be sold to other organizations who also want to be able to position their billboard more effectively, or a fast food chain could send out advertising messages to subscribers as soon as they come into close proximity of one of their outlets. One potential application of the above 5 information could be the use of the information by marketers selling billboard advertising on the side of the road. Knowing the age, income and occupation of the people who travel a specific route could improve the effectiveness of such marketing campaigns even further. This example highlights an interesting application of data mining, but it also shows the potential threats that data mining pose to privacy. [3]

It is up to the organization employing data mining to ensure that their actions result in

neither of the negative effects, namely, incurring legal liability or obtaining bas press as a result of privacy violations associated with their data mining effort (New 2004) [4]. Awareness project directed at implementing data mining to commercial databases for information on potential terrorists, due to inadequacy of consideration that was exhibited for privacy issues. The consumers might for instance be conscious of the fact that gathered information about them is used for billing purposes, but that they did not necessarily implicitly give consent to the organization to use the data in a data mining scenario, thereby overtaking the initial intent of the data collection. To this end it is important to pay particular attention to how the data used in data mining was obtained in the first place, and whether it's used could result in a violation of privacy.

Privacy Preserving Data Mining

Privacy preserving data mining is a unique research direction in data mining and statistical databases, where data mining algorithms are evaluated for the side - effects they incur in data privacy. The main objective of PPDM is to generate algorithms for changing the authentic data in some way, so that the private data and private knowledge remain private even after the mining process, (Verykios et al) [5]. In bottom line this means that the data to be mined would be derived of all information that could be used to determine a specific individual, and that the same would be done to the resulting knowledge achieved from the data mining effort. Privacy preserving data mining is still in its beginning, and whether it will be possible to remark all the privacy concerns in data mining is debatable. In the mean time, organizations should acknowledge the following in order to preserve themselves from legal accountability or bad press resulting from irresponsible data mining efforts:

- Inform customers about potential use of their data gathered from them for data mining purposes, and prior obtain their consent to release the same to other organizations.

One thing that IT experts and business professional must realize that following ethical proceedings and respecting the privacy of individuals leads to good business sense. The bad publicity accomplice with a single incident can damage an organization's reputation for years, even when the organization has followed the law and done everything that it perceives possible to ensure the privacy of those from who the data was collected. [6].

Conclusion

The interests related with data mining, for organization, individuals and society as a whole far beat its imperfections, but the huge issue facing organizations that want to employ data mining, is its cost. The other shortcomings of data mining relate to the threat that it poses to Privacy, and any data mining attempts must not only be done within the framework of the

appropriate laws, but must also be done in a principled manner.

References

[1] Berry MJA and Linoff GS. 2000. Mastering Data mining: The art and science of customer relationship management, Canada Wiley

[2] Ian Brown (2014, February 24). "Could even Facebook become a convert to privacy?" in TheGuardian

[3] Pradeep Kaur, Mukesh M Joshi, E-commerce in India: A review", IJCST Vol.3 Issue 1 Jan-March 2012

[4] New W. 2004. Pentagon failed to Study Privacy Issues in Data Mining Effort

[5] Verykios, VS; Bertino, E; Fovino, IN; Provenza, LP; Saygin, and Theodoridis, Y. 2004. State-of-the-art in Privacy Preserving Data Mining. SIGMOD Record. Volume 33, Issue 1:50-57

[6] Wang J. 2003. Data Mining Challenges and Opportunities. London, IRM Press

A Roadmap for Usability Evaluation Techniques

Sugandha Gupta Kalpna Sagar

Abstract

For any software, its evaluation is significant for managing, controlling so that we can improve a software development process. For such evaluation of software, many factors have been recognized in literature surveys. Quality is one of most important factor which cannot be measured easily, because of its dependency on various other factors. Usability is such important factor on which quality of software depends. Many techniques have so far been proposed for usability evaluation but they are not well integrated and fail to cover all the aspects of usability. The aim of this paper is to provide the roadmap for usability evaluation techniques and their application- a decade review from 1992 to 2015. The paper is also providing comparison between various existing usability evaluation techniques so as to highlight their respective advantages and disadvantages.

Key-Words: Software engineering, quality models, usability model, software quality, human computer interaction, hierarchical model, usability attributes, metrics.

Introduction

One important aspects of software development process is software quality. Usability is one of important quality factor. In recent years, research shows that lack in usability evaluation can

result into failure of software system. Research studies have also shown the benefits of incorporating usability evaluation in the process of software development. For this many usability evaluation techniques have been proposed by various research practitioners. They can be classified as inspection, testing and inquired techniques. Selection of one these evaluation techniques are based on number of parameters like available resources, abilities of evaluator, types of users and environment. The paper is providing the roadmap for usability evaluation techniques and applications-a decade review from 1992 to 2010.

Literature Review

A number of methods have been given by various researchers over the last few decades for evaluating the usability of software systems. These can be classified as belonging to one of the three main categories: Inspection, Testing and Inquiry.

Inspection Techniques

These techniques comprises of a set of methods that are all based on having evaluators inspect a user interface with respect to its conformance to a set of guidelines. Guidelines can range from highly specific prescriptions to broad principles

Cognitive Walkthrough

Cognitive walkthrough (Lewis et al., 1990; Wharton et al., 1992; Rieman, Franzke and sRedmiles, 1995) is a theoretically structured usability evaluation process that focuses on a user's cognitive activities, especially while performing a task. Cognitive walk through involves one or more evaluators exploring an interface,

prototype, or paper mock-up by going through a pre-determined set of tasks and measuring the understandability and easiness of learning for each task.

Heuristic Evaluation

Heuristic evaluation is the most informal inspection method [Nielsen and Mack 1994], mainly because it relies on a small set of usability criteria. In this technique, one or more evaluators independently evaluate an interface using a list of heuristics. The outcome of this evaluation is typically a list of possible usability problems.

Feature Inspection

The purpose of this evaluation method [Nielsen (1994)] is to inspect a feature set of a product and to analyze the availability, understandability, and other functionality aspects for each feature. Evaluators use a list of product features along with situations for such inspections.

Pluralistic Walkthrough

Pluralistic Walkthrough [Bias (1994)] is a variation of the cognitive walk through inspection method wherein representative users, evaluators, and developers inspect the interface as a group.

Perspective based Inspection

Perspective-based inspection [Zhang 1998] is a variation of heuristic evaluation. Interfaces are inspected from three diverse perspectives i.e. novice use, expert use and error handling; considering one perspective at a time.

Formal Usability Inspection

It is a six step procedure that combines heuristic evaluation and cognitive walkthrough. The steps include planning, kick-off meeting, review, logging meeting, rework and follow-up [Bell (1992)].

Consistency Inspection

Evaluators use this method to conclude a consistent interface appearance and functionality that they can then use to weigh the uniformity of interfaces across multiple products in a family. It gives a summary of the inconsistencies [Wixon et al. (1994)].

Standards Inspection

In this inspection method [Wixon et al. (1994)], an evaluator equates components of an interface to a list of industry standards to assess the interface's compliance with these standards. This inspection method is usually aimed at ensuring a product's market conformance.

Testing Techniques

These techniques are the best way to understand how real users experience particular software. During usability testing, participants use the system or a prototype to complete a pre-determined set of tasks while the tester or software records the results of the participants' work.

Remote Testing

In this method [Hartson et al. (1996)], the testers and participants are separated in space and/or time. It may be same time different place or different time different place, depending on the need.

Coaching Method

The coaching method [Nielsen (1993)] allows participants to ask any system related questions to an expert during usability testing. The main goal of this method is to define the information needs of users to deliver improved training and documentation in addition to probably redesigning the interface to eradicate the need for questions in the first place.

Performance Measurement

The goal of this testing method [Nielsen (1993)] is to capture quantitative data about participants' performance when they complete tasks. As such, there is typically no collaboration between the tester and participant during the test.

Co-Discovery Learning

During a co-discovery learning [Nielsen (1993)] session, two participants attempt to perform the tasks together while the tester observes their interaction.

Question Asking Protocol

This method [Dumas and Redish (1993)] is an extension of the thinking-aloud protocol wherein testers prompt participants by asking direct questions about the interface. The goal of such questioning is to enable the tester to get an even better understanding of the participant's mental model of the system.

Retrospective Testing

This method [Nielsen (1993)] is a follow-up to any other videotaped testing session wherein the tester and participant review the videotape together. During this review, the tester asks the participant questions regarding her behavior during the test. The goal of this review is to collect additional information from the usability test.

Teaching Method

For this method [Vora and Helander (1995)], the participant interacts with the system first to develop expertise to subsequently teach a novice user about the system. The novice user serves as a student and does not enthusiastically participate in problem solving. The participant does the problem solving, describes to the novice user how the system works, and shows a set of predetermined tasks.

Thinking Aloud Protocol

The Thinking-aloud protocol [Nielsen (1993)] requires participants to articulate their thoughts, feelings, and opinions during a usability test. One goal of this approach is to empower the tester to get a better understanding of the participant's mental model during interaction with the interface.

Shadowing Method

Shadowing is an alternative to the thinking-aloud protocol wherein an expert user sits next to the tester and explains the participant's behavior during the testing session. Evaluators use this method in situations where it is inappropriate for participants to think aloud or talk to the tester.

Inquiry Techniques

Inquiry methods entail feedback from users and are often employed during usability testing. However, the focus is not on studying specific tasks or measuring performance. Rather the goal of these methods is to collect subjective impressions about innumerable aspects of a UI.

Field Observation

Field observation (Hom, 2003) is a field research method that in which product develop team member visits the user at the user's work place, observe the user's work activities; accumulate artifacts or gather data about the physical traits that marks the work place by photographing, note taking, or sketches; and interview the user about their work.

Focus Groups

Focus group (Rosenbaum et al., 2002) originated as a market research method. A focus group is a meeting of about six to nine users wherein users discuss issues relating to the system. The evaluator plays the role of the moderator and accumulates the desirable information from the discussion.

Interviews

An interview [Nielsen (1993)] is essentially a discussion session between a single user and an interviewer. During an interview, an evaluator enquires a user a sequence of questions about system issues to guide the discussion.

Logging Actual Use

It comprises automatic collection of statistics by the computer about the detailed use of the system. Typically an interface log contains statistics about the frequency with which the user has used each feature and frequency of various events e.g. error messages, undo, redo, etc. [Nielsen (1993)].

Questionnaires

A questionnaire [Soken (1993)] is a measurement tool designed to assess a user's subjective contentment with an interface. It is a list of questions that are circulated to users for responses. Responses on a questionnaire are usually quantitative.

Surveys

Survey is a widespread method to send out inquires and collect data from a large population in a short period of time. During a survey, an evaluator asks a user pre-determined questions and records responses. They could be done over the telephone, in person, over the mail or email.

Conclusion

Many usability evaluation techniques have been developed so far. We have reviewed all these techniques. It was noticed that each usability evaluation technique has its own advantages and disadvantages. It was also found that many of these techniques may be chosen for evaluating usability of a software system depending on various factors e.g. qualitative and quantitative estimation, types of user, environment, available resources, abilities of evaluator etc.

References

[1] Bell B., Using programming walkthroughs to design a visual language. Technical Report, pages 581-92 (Ph.D. Thesis), University of Colorado, Boulder, CO., 1992.

[2] Bias R., "The Pluralistic Usability Walkthrough: Coordinated Empathies," in Nielsen, Jakob, and Mack, R. eds, Usability Inspection Methods. New York, NY: John Wiley and Sons, 1994.

[3] Blackmon, Polson M. H., Muneo P. G., Kitajima M. & Lewis C., Cognitive Walkthrough for the Web CHI 2002 vol.4 No.1, 2002

[4] Dumas J. S. and Redish J. C., A Practical Guide to Usability Testing, 1993.

[5] Holzinger A., Usability engineering methods for software developers. Communications of the ACM, 48(1), 71–74, January 2005

[6] Lewis C. H., Using the Thinking Aloud Method In Cognitive Interface Design (Technical report), IBM. RC-9265, 1982.

[7] Molich R. and Nielsen J., Improving a human-computer dialogue: What designers know about traditional interface design, 1990.

[8] Nielsen J. and Loranger H., Prioritizing web usability. Berkeley, CA: New Riders Press, 2006.

[9] Nielsen J., Usability Inspection Methods. New York, NY: John Wiley and Sons, 1994.

[10] Soken N., Reinhart B., Vora P., & Metz S., Methods for evaluating usability, 1993.

[11] Vora P. and Helander M., "A teaching method as an alternative to the concurrent think-aloud method for usablity testing", in Y. Anzai, K. Ogawa and H. Mori "Symbiosis of Human and Artifact", pp.375-380, 1995.

Dumas J. S. and Redish J. C., A Practical Guide to Usability Testing, 1993.

[5] Holzinger A., Usability engineering methods for software developers. Communications of the ACM, 48(1), 71–74, January 2005

[6] Lewis C. H., Using the Thinking Aloud Method In Cognitive Interface Design (Technical report), IBM. RC-9265, 1982.

[7] Molich R. and Nielsen J., Improving a human-computer dialogue: What designers know about traditional interface design, 1990.

[8] Nielsen J. and Loranger H., Prioritizing web usability. Berkeley, CA: New Riders Press, 2006.

[9] Nielsen J., Usability Inspection Methods. New York, NY: John Wiley and Sons, 1994.

[10] Soken N., Reinhart B., Vora P., & Metz S., Methods for evaluating usability, 1993.

[11] Vora P. and Helander M., "A teaching method as an alternative to the concurrent think-aloud method for usablity testing", in Y. Anzai, K. Ogawa and H. Mori "Symbiosis of Human and Artifact", pp.375-380, 1995.

[12] Wharton C., Rieman J., Lewis C. and Polson P., The cognitive walkthrough method: A practitioner's guide. In Nielsen, J., and Mack, R. (Eds.), Usability inspection methods. New York, NY: John Wiley & Sons, Inc, 1994

A Study of Cloud Security in Insurance Industry with respect to Indian Market

Dr. Kamal Gulati Alisha Gupta

Abstract This research paper presents a brief overview on cloud computing security in terms of Security Considerations, models, threats and precautions in Insurance Industry. This paper gives the brief view for Cloud Security in terms of Problems, Solutions and Challenges which are face in Indian Market with respect to different Insurance companies. Cloud computing is the use of highly scalable offsite Information Technology resources, assembled virtually, accessed over the internet, and used on demand in real-time or near real-time on a pay-per-use or subscription basis, where the workloads are shared among multiple customers. Cloud will also be increasingly important to support new insurer initiatives in social and mobile technology that are demanded by today's consumers in Insurance Industry. Organizations new to cloud say security is their number one concern. Indeed, many perceive it as a significant barrier to adoption. But those further along the cloud journey have a different perspective. While security is just as important for them, it is no longer a source of worry or apprehension. It has simply become another consideration in their Risk Management Strategies and Processes. This Paper also gives the standards, Measurements and Metrics for evaluations of threats need to be initially discussed carefully and then applied to the real applications.

Keywords: Cloud Security, Cloud Protection, Cloud Privacy, Cloud Security Models, Big Data, Data Mining.

Introduction

"By 2020, the people of India will be more numerous, better educated, healthier and more prosperous than any time in our long history"

Technology changes our life and expectations. Cloud computing is recent technology to provide new benefits to users, companies and institutions. This is also a new era of future computing. It is a macrostructure distributed computing instance with minimal effort and cost in highly available and dynamically scalable computing resources. Cloud computing allows customers to share data resources dynamically and charged based on usage. This technology raises concerns about security requirements that are interest to customers and needed for cloud providers such as data prevention, web security, location, identity and access management, recovery, data loss prevention, web and e-mail security, security assessments, regulatory compliance, violation management, event management, encryption, data segregation, business continuity and disaster recovery. The cloud computing model has three actors: cloud provider presents infrastructure to consumers, service provider uses infrastructure to present applications or

services to end users, service consumer uses services on the infrastructure.

History of Cloud Computing

Cloud computing traces its history back to 1950 after availability of mass-scale mainframes in corporations, which could be accessed by terminals/thin client systems, generally known as dumb terminals as they were used for communication purposes but didn't have self and internal computing capability. In order to make better use and management of expensive mainframes, a practice was undertaken whereby many users were allowed for sharing both the physical access to the computer from many terminals and to share the CPU timing as well. In era of 1990, telecom companies started offering VPN facility with comparable quality of service at considerably low costs. By switching traffic they were able to use overall network bandwidth more efficiently. They started to use cloud sign or symbol to signify the demarcation point between what the providers was liable for and what users were liable for. Cloud Computing extends this boundary to cover the servers & network infrastructure as well.

Cloud computing

Cloud computing refers to the use of highly scalable offsite IT resources, assembled virtually, accessed over the internet, and used on demand in real-time or near real-time on a pay-per-use or subscription basis, where the workloads are shared among multiple customers. In simple terms, cloud computing is a model that makes a set of services available through the web, which are provisioned and consumed outside of the enterprises' firewall.

Cloud computing allows companies to access IT-based services, including infrastructure, applications, platforms and business processes, via the Internet. Cloud technologies allow IT to better respond to the changing needs of the business, create new services and open new markets, thereby helping to achieve high performance. Although the term ―cloud computing‖ was coined relatively recently, many elements of the concept, such as timesharing and virtual machines, have been around for several decades.

Three Categories of Cloud Computing:

- Software as a service (SaaS): is software offered by a third-party provider, available on demand, usually via the internet configurable remotely. Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Google Docs, and so on).

- Platform as a service (PaaS): allows customers to develop new applications using APIs deployed and is configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine.

- Infrastructure as service (IaaS): provides

virtual machines and other abstracted hardware and operating systems that may be controlled through a service API. Examples include Amazon EC2 and S3, Windows Live SkyDrive and Rackspace Cloud.

Clouds may also be divided into:

Public: available publicly – any organization may subscribe.

Private: services built according to cloud computing principles, but accessible only within a private network.

Partner: cloud services offered by a provider to a limited and well-defined number of parties.

Moving up the hierarchy

At the infrastructure level, some companies have begun to source raw computing resources, processing power, network bandwidth and storage from the outside on an on-demand basis. Infrastructure cloud providers draw from a pool of shared resources and dynamically expand and contract to accommodate fluctuating demand from different user organizations. As a result, they provide far greater elasticity, economies of scale, and cost advantage compared to standalone data centers.

At the platform level, cloud-based environments provide application developers with similar functionalities to those available in traditional desktops including tools for development, testing, deployment, runtime libraries, and hosting. The emergence of cloud-based platforms enables independent software vendors (ISVs) and IT staff to develop and deploy online applications quickly using the third-party infrastructure.

At the application level, the first wave of cloud-based services, also known as software-as-a-service or SaaS, falls broadly into the areas of CRM, human capital and financial management. The second wave focuses on desktop productivity tools, including word processing, spreadsheets, e-mail and Web conferencing. We can also foresee a third wave, as core insurance applications become available as cloud solutions. Such offerings are currently being developed to handle core activities such as claims first notice of loss, billing, and extended distribution channels. Already, application clouds running on third-party infrastructure span all major enterprise solution areas, ranging from procurement to enterprise resource planning and content management. Organizations generally subscribe to these services based on the number of users or seats. Because these services are available via standard browsers, they support device independence and anywhere access.

At the business process level, cloud based solutions, also known as business process utilities or platform based business process outsourcing (BPO), offer an Internet-enabled, externally provisioned service for managing an entire business process, such as claims processing, expense management or procurement. Unlike traditional BPO, which

often requires the service provider

to take over an existing software installation, the process cloud uses a common, one-to-many platforms to automate highly standardized processes. It differs from application clouds in that it provides end-to-end process support, covering not just software but also processes that may be supported by people, such as contact centers. These processes are typically priced on a per-transaction rather than per-seat basis.

Many companies provide the cloud computing platform such as Google, Microsoft and Amazon. Google cloud computing system includes GFS (Google File System), MapReduce and BigTable. GFS is a distributed file system, MapReduce is not only a programming mode but also parallel task scheduling model and BigTable is a distributed and large scale storage system for managing structured data. Windows provides Azure operation system to create cloud computing platform. Amazon provides the EC2 (Elastic Compute Cloud) for application hosting and S3 (Simple Storage Service) for data storage.

Cloud security

For good measure the traditional data and communication security, cloud computing data brings on new security threats and precautions.

1. Availability

Service Level Agreement (SLA) is a trust between provider and consumer to define maximum time for which resources or applications may unavailable for use. Because this agreement formalizes the relationship between cloud users and cloud service provider, it must arrange very carefully. An ideal way to reduce unavailability of resources because of a breakdown or an attack is to have backup to protect critical information. In this way consumer's information is available offline. Besides, provider should serve monitoring and notification systems to known instant by consumer.

2. Integrity

Protecting data from deletion, modification or production without permission is possible with incident response and remediation, fault tolerance, failure recovery and disaster recovery. Furthermore, digital signature is able to data integrity testing and recovers from corruption.

3. Confidentiality

Claiming confidentiality of users' data, allows for security protocols and proper encryption techniques to be enforced at different layers of cloud applications. Also customers can encrypt their information prior to uploading to cloud. Because confidentiality is correlated to authentication, protecting a user's account is the same as controlling access to cloud objects.

In addition, the biometric authentication features may connect to anti-theft and identity protection features in cloud security.

4. Multi Tenancy

To deliver secure multi tenancy there should be isolation among tenant data as well as location transparency where tenants may not have location of data in order to avoid internal or external attacks.

5. Elasticity

For providers, scaling up and down of consumer's resources gives possibility to other consumers to use previously assigned resources and this may cause confidentiality issues. As a solution of this issue, resources of consumers may place incorporate to avoid other consumers' requests on same resource.

6. Privacy

Privacy protection mechanisms must be embedded in all security solutions. For the use of encryption process, to store keys of on only either provider or consumer side enhances security; additively customer can encrypt their information prior to uploading to cloud. Cloud presents lots of legal challenges towards privacy issues involved in data stored in multiple locations. Because of the changing legal requirements according to country which is hosting servers, organizations should know where their data at all times. Security management operations should involve all security requirements, feedback from environment, policies and standards like Electronic Communications Privacy Act (ECPA), Statement on Auditing Standards 70 (SAS 70), Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), ISO/IEC 27001 and 27002 Cloud Survey Report.

7. Audit

Auditing process contains analyzing authorization and authentication logs to check whether compliances with security standards and policies are guaranteed. Three main attributes should be audited; events, logs and monitoring to provide that there are no security breaches in system. Third party auditor (TPA) verifies integrity of data in cloud on behalf of cloud client and it provides users to ensure the correctness of data.

8. Trust

In cloud environment trust mostly depends on the selected deployment model according to audit of data and applications are outsourced .Organizations must know how to act these situations: how to describe and improve it, how to handle malicious information, how to consider and ensure different security level of service according to the trust degree and how to manage trust degree change with interaction time and context. Another situation, Trusted Third Party (TTP) relationships should rely upon for confidentiality, authentication and authorization.

9. Non Repudiation

To prevent the issue of denial, cloud

provider has to ensure nonrepudiation enabled protocol or handshake is implemented so connected parties cannot dismiss their participation in an argued transaction.

10. Data Leakage

When moving to a cloud, data will be stored away from the customer's local machine or data is moving from a single tenant to a multi-tenant environment. These changes can cause data loss or leakage. For decrease effects of such problem, Data Leakage Prevention (DLP) applications should be used to protect sensitive data. Moreover, using access controls with strong encryption to consumer data ensures security even if the data is detained.

11. Deployment Models

Because of additional charge of ensuring all applications, public clouds are less secure than the other cloud models. Private and community clouds can be more secure than public clouds due to specified internal usage. In addition hybrid clouds provide more control of data and applications security.

12. Stakeholders

The importance rises about to enhance consumers' knowledge in cloud computing and awareness of security issues also increase providers' effort to make technologies secure and available. Although, cloud providers cope with assuring long term secure operation, identify and block malicious customers and fight against numerous hackers; consumers confronted downtime of cloud computing environment, leak of commercial secrets and privilege management. According to M.D. Ryan's proposed approaches' security level that they provide in descendent order is key translation in the browser, fully homomorphic encryption,
CryptDB: a weaker attacker model and hardware anchored security. Additionally, authorities and limits are should be determined with the help of policies.

13. Attacks

If attacks are identified with existed signatures, Intrusion Prevention Systems (IPS) is effective but if there is legitimate content with bad intentions, they are inadequate. If attackers access to credentials, they can eavesdrop on activities, manipulate data, return changed information and redirect clients to illegal sites. By consuming inordinate amounts of system resources such as processor power, memory, disk space or network bandwidth, attackers cause an intolerable system slowdown. Even worse, since cloud providers bill clients based on their consume, attacker may cause to consume so much processing time that becomes too expensive and clients will be forced to shut down their services. If there is a flaw in one client's application or service, an attacker could access not only that client's data, but every other client's data as well. However, attackers might be able to crack an encryption key in minutes via array of cloud servers instead of using their own limited hardware or they might use cloud to

stage other attacks, serve malware or distribute pirated software. So, cryptographic operations which are configured correctly reduce the impact of data breaches. In addition, consumers may implement Host Intrusion Prevention System (HIPS) at endpoints to protect DoS, DDoS, XSS, SQL injection phishing or zombie attacks.

Catalogue of services offered by Indian Cloud service providers (csp's)

Service	Remarks
Cloud Enablement	Cloud related services such as: • Migration • Deployment • Planning • Consulting
IaaS	On-Demand Virtual Servers • 99.995 percent uptime • Tier 4 datacenters
PaaS	Providing a cloud-based development platform for building business applications and deploying them on public or a private cloud
SaaS	A wide range of software delivered as a service via Cloud ranging from Email, Productivity applications, Business applications, Collaboration applications, ERP, CRM, Core banking etc. These CSPs cater to a wide variety of customers ranging from SMEs to large enterprises.
Private Cloud	Catering to Indian enterprise sector with a dedicated pool of computing resources.
Cloud Telephony PaaS	India-based telephony platform in the cloud. It is the simplest and easiest way to build telecom applications, IVRs, office PBX and outbound campaigns and deploy them on the Cloud.
ITaaS – Cloud based IT as a Service	Covers the entire spectrum of business processes for SMBs. Domains included are: • Manufacturing • Wellness • Retail • Education

Today's insurance challenges and cloud solutions

Going forward, we believe insurers' interest in cloud will increasingly turn into concrete action as the industry faces up to a unique set of crucial challenges now rising up the industry agenda. Each of these challenges can be tackled through the capabilities and benefits delivered by cloud-based solutions across the continuum from infrastructure to applications, business processes, and new offerings and markets. The baseline for tackling these challenges is generally using an infrastructure cloud, but the ability to address them is further enhanced by expanding up the cloud hierarchy.

These challenges include:

i. Tougher time and cost pressures — Insurers need to achieve profitability in a period of reduced premiums and investment income, while also increasing their speed to market to resist intensifying competitive pressures. These challenges can be addressed through an infrastructure cloud solution, which will boost financial flexibility, permanently reduce costs of IT ownership, and also cut operating costs by ensuring services are paid for only when they are used. Moving up the cloud continuum to applications and business processes will further enhance the speed and cost with which insurers can respond to market change. Cloud also helps insurers handle peaks in demand at lower cost and effort.

ii. Emerging market and acquisition opportunities — The rising flexibility and standardization fostered by each successive layer of cloud solutions facilitate easier and cheaper integration of new operations, acquisitions and collaborative partnerships. This enables targeted expansion into emerging geographic product markets at greater speed and at lower total cost, reduced capital requirements, and lower risk.

iii. New global market structures -- Similarly, the flexibility and adaptability of cloud boosts an insurer's ability to respond to market change and reshape its operating model to address new and emerging opportunities and challenges. Cloud also reduces the time and cost required for

piloting new projects.

iv. Need for agile and differentiated product and pricing — In combination, the improved speed to market and responsiveness enabled by cloud based applications and processes, the availability anywhere and anytime of unified customer and segment information, and the ability to apply sophisticated analytics quickly and flexibly, can transform insurers' ability to adapt and re-price their products and services in response to market and competitive change. This helps to maintain differentiation and competitive edge in a dynamic marketplace.

v. More demanding customers — Customers expect products and services that are ever more suited and responsive to their needs, and provide rising value for money. They also want consistent and coherent interactions across every channel they choose to use. The advantages of cloud in terms of cost, flexibility, agility and pervasive availability of unified customer information all help insurers to meet these demands.

vi. The workforce is undergoing dramatic changes — Like other industries, insurance is facing the challenges of an aging and increasingly mobile workforce, together with rising competition and changes in core skills. Employees need to adopt a more customer-centric mindset and culture, and have always-on availability of relevant and up-to-the-minute information and training. Employee facing cloud applications and processes can meet all these needs.

vii. Evolving sales/distribution technologies — the ways in which insurers interact and build relationships with customers have been transformed in recent years. Increasingly, product and service innovations based on online and mobile channels, personalized tailoring of products and speed of response are key to competitive differentiation. Cloud helps insurers acquire the technological and operational flexibility and customer insight to win this battle.

viii. Increasingly burdensome regulatory requirements — Insurers need their systems and data to be sufficiently robust and flexible to meet evolving and increasingly demanding regulatory requirements in areas such as capital ratios and consumer protection. Flexible cloud services offering unified, always-available data will help. Indeed, SaaS may come to be a must-have in insurance in the future, due to a combination of regulatory obligations and insurers' increasingly pervasive network of services.

Cloud computing has the potential to permanently remove such shortcomings. In fact, analytics is tailor-made for the cloud for several reasons:

- The cloud enables insurers to store an enormous amount of data and put dormant data to work.

- It provides a cost-effective platform for developing analytics models, reports

and driving business intelligence.

- It can enable an insurer to work with historical as well as real-time or transaction information as a variety of sources.

- It enables insurers to churn through vast amounts of data and decipher patterns and anomalies not only in the past, but also projected into the future much more quickly, efficiently and cost effectively.

- Insurers can also use the cloud to help design their web personalization engines, customer behavior analyses and data mining algorithms.

For all these reasons, the cloud can enable insurers to transform the quality and speed of their responses to customers' needs, both in their service interactions and also their product design and delivery.

Using DLP tools in cloud computing security

One of people's biggest concerns about adopting cloud computing is the potential risk to their data. Anytime we "lose" physical control of an asset, it's only natural to worry about it. And since data loss prevention is one of only a handful of security technologies dedicated to protecting data, it's also only natural we take a hard look at expanding it to protect that cloud-based data.

Today there are three different business problems related to cloud computing where DLP is helpful. The first is to use it as a tool to control the migration of data to the cloud. The second is as a control to protect data in the cloud. And finally, we can use DLP tools to find sensitive data that's "leaked" to the cloud.

Using DLP tools to control data migration

One of the most useful ways to use DLP for cloud computing is to monitor, and even block, data migrations to the cloud from your traditional infrastructure. The vast majority of cloud computing services rely on HTTP as their main out-of-the box communications protocol (albeit often through custom APIs). Thus, if you monitor HTTP (and HTTPS), you'll catch many potential data migrations across the spectrum of cloud service models.

All network DLP tools can monitor HTTP traffic, and I strongly suggest you stick with options that also support HTTPS monitoring natively or via Web gateway integration. Then ask your DLP vendor if they are "cloud aware" for major cloud services and destinations, which will reduce the need for custom rule writing. You can then apply any of your existing DLP content rules on a per-cloud-service basis, or merely set up generic alerts anytime the cloud is a destination for your data.

Cloud DLP limitations

One big limitation to keep in mind is your public cloud platform may only support a single network interface per instance, which

means you'll need a virtual DLP version that can monitor and forward traffic with this restriction. Keep in mind most of you don't use DLP to monitor data center-based applications as it is, and it's usually not the first technology I recommend for protecting servers.

Altogether, I see a lot of value in using DLP to monitor data migrating to the cloud and for content discovery on cloud-based storage, but I see little value in deploying DLP within a public cloud. (It may make sense in private cloud, depending on what you are using it for). Over time this will change as technology evolves and we deploy a wider variety of services in the cloud, but any cloud deployment we can protect in line with DLP is probably an application infrastructure, where we should rely more on things like application security and encryption.

DLP can be an excellent tool to enhance data security in the cloud. Use it to track data migrating to the cloud, discover sensitive data stored in your cloud, and perhaps to protect services running in the cloud. But, as with any technology, make sure it's tuned for the environment, and don't waste your time deploying it where the benefits are minimal.

The seven steps towards an effective cloud security team

I. Develop a cloud strategy

Security teams should develop and own cloud security strategies as part of their organizations' broader information strategies. They should then review and revise security policies, procedures and processes to embed cloud into the security function and governance model. This may mean adding new policy statements or simply extending existing ones to encompass new concepts. It may also have knock-on effects on the security teams' approaches to compliance and audit activities.

Focus on a Federated Model

As cloud becomes more broadly adopted, the team will have to understand and adapt to a federated security model, where the authentication and authorization between participating services are brokered and identity data is shared across the organization's boundaries. A centralized model becomes unsustainable in a world where much of what needs securing actually reside outside the organization. As ever more business services appear in a cloud context, the security team will need to encompass and address security issues related to process and technology integration.

Move closer to contracts and the business

The security team will also need to work with the legal department to ensure contracts with providers reflect the organization's security requirements. To this end, it should develop, in collaboration with the commercial department, appropriate requirements and provider assessment criteria to ensure it obtains the appropriate

levels of security, compliance and assurance around the services it is buying.

Many security teams have already been developing these skills as a result of outsourcing. Teams are changing from being providers themselves into more of a contract assurance function. They also need to become increasingly familiar with business functions in order to interpret business requirements and assess the potential impact of meeting those requirements with cloud services.

Manage multiplicity

Security teams in organizations that are using multiple cloud services also need to understand and manage the new risks this may present. For example, the organization may enter into a contract with a Software-as-a-Service (SaaS) vendor that hosts its application on the same cloud infrastructure the organization uses for some of its own legacy applications.

In this example, there is an obvious risk with availability. Less obvious is the potential risk of access to a wider set of data – the legacy data and the data in the SaaS application together might be more meaningful and therefore valuable.

Secure the exit

Upon termination of a cloud service contract, the security team needs to be satisfied that no residual sensitive data remains anywhere on the provider's system. That includes operational databases, backups and archives. It is worth considering this eventuality at procurement time so the relevant obligations can be clearly set out in the contract.

Build diverse teams

Traditionally, security teams have largely comprised in-house technical staff. However, in a cloud world, the team may need to extend to include security representatives from providers, as well as from other parts of the business. Due to the perceived risk associated with cloud, the role of the chief security officer will become increasingly critical in terms of putting all the pieces together and ensuring the organization's data and business logic are suitably protected.

Seek out security standards

It is much cheaper and easier to enter into contracts with providers if there are recognized standards against which they can be judged, rather than organizations having to draw up their own set of requirements. Cloud standards are still evolving, so the security team needs to keep abreast of any new developments.

In short, the security team needs more than ever before to facilitate good practice, especially through collaboration with the cloud service provider, rather than appear to be blocking the adoption of cloud capabilities. This means moving closer to a supporting – rather than an ownership – role.

Findings and conclusion

- Don't just rely on technology to protect your data – restrict access to sensitive information and train employees to be risk aware.
- Identify the risk and manage the potentially very damaging losses that have a reasonably high chance of occurring.

- Align investment with potential loss – including any reputational damage implications – so that you don't overspend or skimp on essentials.

- Assess your exposure and the standards you need to apply in the light of reported losses in your business sector and best practice guidance.

- Run regular checks to make sure controls remain in place and employees are adhering to protective strategies.

- Make dealing with a data breach part of your business continuity and crisis management plans.

- The industry is already aware of the changing power of big-data – & also of the challenges it faces in getting the most out of it.

The use of cloud computing in Insurance sector in India is yet to accomplish. It's being used at some level but at the highest level it's yet to be used. But when it will be used it will change the way the insurance business is done in a country of 126 crores.

Suggestions & Remedial Measures

- The remedial measures can be that more emphasis on reducing the overall cost of cloud computing.

- The government and regulator needs to make it compulsory for the insurance companies to make some part of their business through cloud computing.

- This will ultimately force the corporate to shift to cloud computing.

- This will reduce the cost and ultimately beneficiaries will be the customers with new products, less premium and tailor made products.

The future will be technological driven, it will be more dependent on technological as compared to human. If we want to be updated and innovative we need to be technology driven. In an environment which is customer centric and there are number of companies, the companies need to be different. For being different, you need to be customer centric with new tailor made products.

Organizations new to cloud say security is their number one concern. Indeed, many perceive it as a significant barrier to adoption. But those further along the cloud journey have a different perspective. While security is just as important for them,It has simply become another consideration in their risk management. Their experience informs future decisions about moving other services into (or sourcing them from) a cloud environment, thus helping them makes ever further strides along their cloud path.

References

[1] Insurance Wikipedia, en.wikipedia.org/wiki/insurance

[2] Cloud insurance, www.cloudinsure.com

[3] Jeanne G. Harris and Allan E. Alter, Accenture (2010) How Cloud Computing will Transform Insurance ,www.accenture.com

[4] Qi Zhang, Lu Cheng, RaoufBoutaba (2010) Cloud Computing: State-of-the- Art and Research Challenges

[5] Weinhardt C, Anandasivam A, Blau B, Borissov N, Meinl T, Michalk W, Stößer J (2009) Cloud-Computing, http://www.wirtschaftsinformatik.dedoi: 10.1007/11576-009-0192-8. [6]Wayne Jansen, Timothy Grance (2011) guidelines on Security and Privacy in Public Cloud Computing

[7] Data Security; Strategic Risk, www.strategic-risk.eu , November 2011by Ace Group of Insurance and Reinsurance Companies

[9] Dr. Kamal Gulati, Prateek Sharma, Divyanshu Mishra; Role of Cloud Computing in Health Insurance

[10] Source: Cloud computing information security, November 2009, ENISA

[11] Cloud Computing in the Property and Casualty Insurance Industry; www.capgemini.com [12]Mahima Joshi et al, International Journal of Computer Science & Communication Networks, Vol1(2), 171-175; ISSN:2249-5789

[13] Jiyi Wu, Qianli Shen, Tong Wang, Ji Zhu, Jianlin Zhang ; Recent Advances in Cloud Security; JOURNAL OF COMPUTERS, VOL. 6, NO. 10, OCTOBER 2011

[14] BIG DATA meaning; http://en.wikipedia.org/wiki/big_data

[15] Analytics & Big-data