Advanced Insights into Data Privacy, Application Security and Compliance Regulatory Issues with Cloud Computing in Health care.

SAMEER DASAKA[1]

ABSTRACT

With humongous increase of patient data in hospitals and healthcare centres every day, there is tremendous need for hospitals to deploy their services and data to the cloud which will increase the efficiency and makes administration more balanced and steadier. While it is a sterling approach to deploy user data and services to the cloud, it is important for healthcare centres and hospitals to understand and be aware of the potential threats in the cloud environment. With the advancement of technology, hackers try to gain access into the cloud by exploiting vulnerabilities which are unpatched for a very long period. These exploitations lead to unauthorised access and control over user information which results in immediate havoc to the user privacy and long-term damage to the goodwill of the hospitals. Technical Issues such as Access Control, Identity Management, Authentication and Authorisation needs to be addressed with immediate alacrity to safeguard the CIA traits namely Confidentiality, Integrity and Availability of user data in the cloud. This paper will elucidate on what kind of security approaches and enhancements are necessary to be taken care to prevent unauthorised data access, financial and goodwill loss in the healthcare domain.

Index Terms*:* Application Security, Cloud Computing, Compliance, Cloud Forensics, Legal and Privacy.

SAMEER DASAKA[1]: Department of Digital Forensics and Information Security, Institute of Forensic Science, Gujarat Forensic Science University, Gandhinagar, India

INTRODUCTION

In major hospitals and clinical centers, medical reports and health assessments of an individual cannot be shared with anyone who are not authorized. That at times can also be the family members of the patient. Keeping in mind the privacy of an individual, healthcare centers are approaching cloud to store patient medical information. In situations where, medical records are digitally stored in a local database at each respective healthcare centers had seen the importance of maintaining medical reports on cloud for easy access and next-step medical clarifications and appointments to the patient. Uploading all the data to the cloud raises lot of potential threat and dangers to the individual privacy. This is where the cloud data security and the vulnerabilities present in the application level due to lack of properly built security architecture raises digital privacy concerns to the patients as well as the healthcare centers.

Issues to be addressed: Technical terminologies such as Access Control, Authentication, Authorisation, Identity Management, in a centralised cloud network environment is quite important and is necessary to be addressed while considering the conspicuousness of the individual privacy when opting to go for the cloud. Cyber criminals who are constantly looking for vulnerabilities that can be exploited to gain access to sensitive patient information are always on the edge and should be stopped by making sure proper cloud security architecture is proposed, implemented with on-time secure code reviews to potentially update software from future exploitations.

It is necessary and imperative to understand that the cloud resides in the internet. Making itself more prone to internet-based or web-based attacks. The data when uploaded to the cloud, uses internet-as-a-service to maintain a fast and efficient route for the data to be transmitted. This is the place where formidable and threatening attacks like Man-in-the-Middle attacks can take place causing massive data breaches to sensitive medical information. While, maintaining cloud services will deliver convenient and invaluable support to the patients, possessing lack of proper cloud security infrastructure and architecture in unsecured network environments will cause extreme data theft and unmeasurable amplification to the healthcare centre.

To explicitly fight these security related issues which includes data and user privacy, different cloud service providers had come up with different cloud security architectures. Few of them listed below are: sHype Hypervisor Security Architecture, Resource Isolation approaches and others have been implemented to an extent to protect and safeguard the cloud threat management augmentations. With the increase of internet usage, it is required to maintain best compliance, regulatory practices on implementing secure data security policies.

All Rights Reserved © 2018 IJARCET

Identity Mismatch and Access-Control Management:

It is required for the hospital management to maintain secure identity access management systems which require users to setup multifactor authentication to sign in into their personal accounts. These can be location-based authentication, OTP's and more. Lack of proper access control management will enable hackers to access resources without user acknowledgement. Majority of data breach incidents occur when proper access control mechanisms are not enabled and have heavy business implications.

Business Continuity Management and Operational Resilience- Loss of User Data:

It is required for the hospital management to securely backup and maintain copies of user data in secure storage systems always. There might be chances that user data stored at a place can lead to deletion due to attackers and due to natural calamities. The management should implement proper steps for business continuity process and disaster recovery.

System Vulnerabilities:

It is required for the hospital management to maintain a secure code review team, who will be able to check applications source code for possible vulnerabilities which when exploited by attackers can give away sensitive information like patient bills, medical reports, appointment dates, doctor name and more. Management should make sure that the cloud service provider regularly updates their software and have frequent system vulnerability checks. Unpatched system vulnerabilities can have unforeseen business impacts. While, user data and privacy taken very seriously, patching vulnerabilities in applications will be a life saviour.

Application & Account Security Governance and Enterprise Risk Management

It is important for the management to understand that even today user account security gets compromised due to stolen login credentials. This can be considered as a severe risk to An Organisation. Once a user account login credentials are stolen, attackers can be able to penetrate and gain unauthorised access to the cloud computing services which can further allow them to manipulate data and compromise the CIA (Confidentiality, Integrity and Availability) trait. It is necessary to understand the impact An Organisation would go through if account security of an individual is compromised. Hackers will then be able to steal data which will be disastrous for the user as well as An Organisation and the Cloud Service provider.

An Organisation should be aware of these kinds of attacks and should draft and implement possible defence strategies to protect the user privacy and the goodwill of an Organisation. This can be achieved when an Organisation prohibits sharing of user credential information with anyone and should force user to main multiple authentication factors.

Impact on Application & Interface Security with DoS attack:

It is important for the hospital/healthcare management to know about the mitigation techniques the cloud service provider will offer as a first line defence technique/strategy to make sure the resources of the system which provides the cloud services are not fully utilized by the attacker. This is to ensure that patients will be able to access their information whenever needed. A Dos attack is known as the Denial of Service attack where the attacker will utilize the entire system resources and make sure that the patients cannot access their data by getting the website off the internet for a good amount of time. A DoS attack creates panic and fear for the public and patients which will eventually impact the goodwill of the hospital/healthcare centre.

Incident Response Management- Cloud Forensics and E-Discovery Investigations

Digital forensics is a branch of forensic science that deals with the investigation of cyber-crime from digitally extracted artifacts. The hospital management should make sure that the cloud service provider designs and implements possible digital forensic strategies to mitigate future cyber-attacks and have proper incident response management team to notice advanced persistent threats and take defensive approaches to stop the crime. This will be very helpful to the management to find out what were the reasons certain data breach has occurred, what is the impact, what is the quantity of sensitive data being stolen, who stole the data, gather suspicious network addresses connected to the cloud to perform the attack and more. Once, a person or a company is identified as the prime suspect, then E-Discovery Investigations can be performed to bring the person or fraudulent company to justice. This will save the goodwill of thehospital and thehospital management can know the loopholes involved in the cloud and take appropriate legal steps to save user privacy.

With the advancement of technology, there are multiple new ways for delivering and procuring IT services in the Industry. Cloud services plays a very important role in fulfilling this need. The use of cloud computing services has been drastically widespread in the recent years. International surveys estimate the cloud services revenue to reach $110 billion by the year 2020. Convenient Monitoring, Scalability, Universal Access, Elasticity, Flexible billing, Easy Metering are few of the cloud features that customers and service brokers are taking advantage of. Even though there is high demand for cloud services across the globe, yet there are many challenges to be faced when an hospital/healthcare thinks of moving its business to the cloud. Challenges like Security,

All Rights Reserved © 2018 IJARCET

User Privacy, Compliance and Legal issues are few among them.

Compliance regulations and policies generally govern the use of important and sensitive business data. The main reason for these compliance regulations is to protect and safeguard the customer data and privacy by providing security attributes like the CIA traits which is Confidentiality, Integrity, Availability and Accountability. Compliance ensures that these rules that implement the policies are properly enforced which are defined in the regulations. We can say that legal compliance is one of the most necessary non-functional requirements for indefinite number of systems. Government regulations which are pre-defined are necessary to follow which private and industrial regulations are options. These regulations usually vary from one country to another but most of them usually speak out the same meaning and carryout similar functionalities which can be customisable in accordance to their needs. In accordance with NIST (National Institute of Standards and Technology), the responsibility of all compliance issues should be taken by all hospitals/healthcare. If not, then they can be liable to heavy penalties, lawsuits, damage to goodwill and loss to business reputation.

Potential threats are not usually recognised when compliance and security related issues are addressed in the ending stages of development and testing. It is very crucial to build good quality and compliant regulatory systems to identify applications which carry potential vulnerabilities and threats. These compliant systems are required in every stage of development starting from business requirement discussions, designs, coding, review, and testing phases. The compliance regulations are usually not being understood by developers and often there is legal team available to understand and elucidate them to the management. There is always more than one regulation for consumers and service providers to be compliant with. There are numerous software and tools available in the market which are used to check the compliance of systems/products. Vender-Neutral Standard Compliance Reference Architecture is the major segment which lacks in majority of the cloud services are the most basic challenge to consumers, internal and external auditors, service providers and more. A Reference Architecture is a regular generic software architecture which has no platform dependencies for any unique domain. It can be used as a guide while designing systems for cloud services. It is very much essential as it elucidates when and where certain compliance regulations must be implied which designing and developing a software architecture. It can be used as a manual for management professionals, architects, developers, testers, auditors and compliance regulation team to understand the compliance regulation and implementation process. These compliance reference architectures are not designed for general use and are often incomplete. It is required for the management to design compliance regulations and policies as per the hospital/healthcare norms and business requirements.Since consistence is unequivocally founded on safety efforts and related strategies, plainly an acknowledged reference models depicting directions would give an approach to encourage building compliance regulatory frameworks that conform to the comparing reference controls to the cloud. A reference architecture would be very necessary to modify or build existing and new compliance reference architectures accordingly.An Organisation might use independent third-party agencies which certify compliance policies and the Organisation internal compliance assurance team to check the standards of compliance, security and privacy. If thehospital/healthcare centre plans to move their business to cloud which is setup in the United States, then, it is required for the management to fulfil the FRAMP which is the Federal Risk and Authorization Management Program accordingly.

PCI-DSS (Credit Card Industry Regulation)

A hospital/healthcare centre when handles the cardholder information is required to comply with the Payment Card Industry Data Security Standards. The card information includes ATM details, POS cards, debit, credit, prepaid cards and more. According to the PCI regulations it is required for hospitalsto have authorized users' access to the cardholder information and its activities. PCI has twelve major rules to protect cardholder data and it is required by the hospital/healthcare centre to follow them.

- Maintain proper firewalls to protect the cardholder data.
- Protect saved cardholder data.
- Encrypt communications.
- Use frequently updated anti-virus.
- Do not use default passwords.
- Develop and maintain secure systems and applications.
- Make sure not everyone has access to sensitive cardholder data.
- Identify and authenticate access to only authorised members.
- Restrict physical access to the cardholder's data or information.
- Frequently test security systems and processes.
- Maintain proper information security policies.

Compliance consistency in the cloud is a mutual obligation among specialist organizations and purchasers. The obligation of specialist organizations and customers shift considering the kind of their administration models. Because of IaaS, buyers are dependable to anchor administrations, stages, and information. Specialist co-ops are capable to anchor the framework. On account of PaaS, buyers are capable to anchor administrations and information; specialist organizations are capable to anchor stages and frameworks. On account of SaaS, buyers are capable to anchor information; specialist co-ops are mindful to anchor administrations, stages and foundations. As a rule, the absence of full control and straightforwardness makes consistence challenges in the cloud.

All Rights Reserved © 2018 IJARCET

In rundown, most specialist co-ops have distributed consistence models, plans, and executions considering their own exclusive cloud stages, frameworks, and items. The accessible RAs distributed by specialist organizations are either merchant particular; or don't pursue standard models, examples or designs. Accordingly, it is extremely hard to break down their level and extent of consistence. Customers are additionally tested to assess specialist organizations without having standard RAs and models that could be utilized as a typical reference and agenda.

As showed before, directions are composed by legal counsellors and regularly extensive and difficult to peruse. Sometimes, the standards are repetitive, equivocal, and even conflicting. Directions additionally change from nation to nation. There have been endeavours to make directions clearer and more exact by utilizing square charts, reference diagrams, and reference models. Be that as it may, there have been just a couple of endeavours to make their product engineering more exact with a specific end goal to comprehend and dissect approaches at a larger amount and in the end direct outline and usage endeavours.

The absence of full control and straightforwardness is likewise one of the consistence challenges in general society cloud. The information put away in people in general cloud could be reproduced in various locales and/or nations that could abuse protection laws of different nations. Furthermore, specialist organizations are required to guarantee the classification, uprightness, accessibility and responsibility (CIAA) of customers' information according to the legislature and industry directions. HIPAA built up a system that can control information area while looking after consistence. HIPAA recommended more research to construct purchasers' trust and consistence.

Cloud administrations like any IT stages are subjected to an assortment of security dangers. The many-sided quality and shared obligations of distributed computing are additionally another security risk that could influence the general consistence. Distributed computing is generally new and yet evolving. More research is expected to fabricate buyers' certainty and trust by recognizing potential security and consistence dangers. HIPAA built up a security reference engineering to implement cloud security. The design can be stretched out to help consistence by including consistence examples and best practices. The design proposed pursues this methodology and can deal with recognized dangers by including proper security designs.

A large portion of consistence needs to do with security. Be that as it may, consistence is frequently dealt with by various gatherings who don't have a full mastery on security. Taking a gander at a portion of the proposals in the distributions we reviewed we locate that a significant number of them are innocent and insufficient to give a profoundly secure design.

We have broken down the best in class in consenting to controls by looking at ongoing productions and studying mechanical methodologies. Controls and principles are mind boggling, potentially repetitive and even conflicting at times. A decent method to deal with consistence complexities, vulnerabilities, and covers is by applying standard models, examples, structures, and best practices. There have been endeavours to break down direction approaches and covers. Be that as it may, there has been no endeavour to make their product engineering more exact at a larger amount to in the long run guide plan and usage endeavour's. These sorts of standard methodologies could enhance consistence, security, protection and the general programming nature of cloud frameworks. We analysed how distributions and industry have thought about this specific angle as a proportion of their capacity to adapt to an expanding many-sided quality. While there are different angles that influence consistence, we have taken the best possible utilization of structures as a key point.

Trans-Border disputes

1. **Copyright Law:**It is important for An Organisation to understand that the data that is stored in the cloud storage is always protected by the copyright laws. Data such as photos, videos, source codes, graphic designs and more. Under the copyright law, any individual who creates his/her own work will automatically assigned as copyright holder. The reproduction of any work without the consent of the individual/ account holder in the cloud cannot be done. However, there are numerous exceptions to this prohibition.

We all know that cloud computing is composed of three major elements i.e. the SaaS, PaaS and IaaS, let us see who copyrights can be applicable to them.

- **SaaS**: The first initial step to be analysed if a user would likely breach the copyright by using SaaS is by viewing the terms and conditions of the cloud usage. These terms might contain a licence which will permit the user to make further software copies.
- **IaaS**: Similar to SaaS, before the user saves or downloads any saved content, it is important to read and understand the terms of use. These terms of use will regulate what kinds of data can be downloaded by the user, on what devices and with whom it can be shared. If the rules are exceeded by any individual, then copyright claims can be charged on him/her and might receive a warning letter or even face the court.
- **PaaS**: It is required for an Organisation to understand that an Organisation will not have to face any problems in terms of copyright. This is because, An Organisation will be the sole creator of a work and therefore An Organisation is known to be the copyright owner. This work is not used by any end-user under any circumstances.
- There are chances that the cloud service provider might breach the copyright laws through offering copyright content for download illegally. It is necessary for An Organisation to take wise choices while selecting their cloud provider.

All Rights Reserved © 2018 IJARCET

Statutory Rules on Private Copies

- *Statutory rules are set of guidelines that provide exceptions to download and upload copyright information to the cloud with the consent of the copyright holder.*
- *Illegal source: It is important for An Organisation to understand that having right to make a private copy doesn't apply if the source from which the copy came is created illegally.*

Intellectual Property Issues in cloud

- There are numerous transactions that take place in the 'cloud'. Online platforms allow users to upload and share data. When these transactions take place, it is necessary for An Organisation to know that the intellectual property relates to the information that contains ideas, branding, logos, signs, trademarks, hardware, software and more and protection of these intellectual property rights from various sources of potential infringement will be a daunting task for An Organisation in the cloud environment.
- Storage of information in different locations through distribution over a wider area and variety of resources will increase the safety probabilities, however at the identical time, it's its negatives. info within the cloud is really hold on in a very place that is out of user's management. Access to cloud storage information can be removed at any time and this can be additionally outside the control of the user. The cloud client isn't in an exceedingly position to observe the information handling practices of the CSP. The account may be deleted and everyone the info holds on in it's going to be lost. this can be of most concern once what's hold on is sensitive information.
- In the cloud, not even the user has any whereabouts of his knowledge. The external server could also be shifted or resettled while not his agreement. Adding to the current the conflict between privacy laws in varied jurisdictions, we tend to get the full, fuzzy image of the cloud.

Patent related Issues in Cloud

- Companies progressively emulate on innovative technologies that e.g. modify the economical scaling from a virtual machine, the fast stationing and classification of information or the speedy recovery of applications. Such innovative technologies are extremely proprietary to permit patent owners to secure future technological areas.
- *According to the EU Patent and Trademark Office Database (EPO) a record range of ninety-five,940 EU patents was granted and revealed in 2016 that amounts to a forty.2% increase. The 5 countries of origin with the biggest numbers of EU patent applications were the United States of America, Germany, Japan, France and Swiss Confederation whereby the latter had once more flat-topped the ranking in 2016, with 892 applications per million inhabitants. The quickest growing space within the technology field is patent applications for computer technology with a pair of.9% increase.*
- Also, in European nation patents for technology square measure granted, but it's a lot of customary to get a world or EU patent instead of filing for a Swiss national patent. Swiss corporations sometimes solely file a Swiss patent during this field to get the priority date, however of a lot of importance is that the EU patent. In European nation there are not any official statistics on the quantity of granted technology patents, however one will assume that they show the same tendency of accelerating numbers because the EU patents granted during this field.
- Hospitals/healthcare centres should understand that Cloud technologies area unit typically believed to trust essentially on shared environments following public standards. However, the conferred numbers show that cloud technologies are progressively subject to patent litigation. This might of course block the open use and development of future cloud-based solutions. Cloud computing technologies area unit complicated systems with immeasurable applications that area unit incorporated in varied merchandise or services. loosely written patent claims might thus bite an unpredictable vary of cloud-based solutions, making unpredictable legal risks for each business victimization cloud technologies.

Tort Law issues in Cloud and how An Organisation can fight it

- Hospitals/healthcare can file a case against the cloud provider if the services are not being properly delivered as per the service agreements. A contract could produce a state of things that furnishes the occasion of a misconduct, in order that the negligent performance of a contract could produce to associate degree action in misconduct, if the duty exists severally of the performance of the contract. The contract then creates the relation out of that grows the duty to use care within the performance of a responsibility prescribed by the contract.

Privacy Issues in Cloud and how Organisations can fight it:

Standards, Regulations- Personally Identifiable Information and Protected Health Information.

- It is required for hospitals/healthcare centres to comply with the Healthcare Insurance Portability and Accountability Act, famously known as the HIPAA. HIPAA is mainly used to ensure the privacy and security of the protected health information (PHI) and Personally Identifiable Information (PII). These PHI and PII usually

All Rights Reserved © 2018 IJARCET

includes important and sensitive information like patient medical records, medical transaction records, patient personal information, term information, insurance details and lot more. Healthcare providers like An Organisation, health insurers are said to be known as covered entities and are categorized accordingly by the HIPAA.

HIPAA regulates five most important rules that has to be followed by An Organisation.

- **Rule of Privacy**: Hospitals should always notify patients on how they use their information. It is mandatory to regulate the use of PHI and disclose it to the individual.
- **Rule of Security**: Hospitals should make sure that the user data and privacy shall be safeguarded and protected from data tampering, data modifications, deletion, unauthorised access and data breaches.
- **Rule of Transactions**: An Organisation should regulate medical transactions, standards, documenting and reporting.
- **Rule of Enforcement**: An Organisation will be liable for violating HIPAA rules under any circumstances.
- **Rule for Unique Identification**: It is mandatory that employers are required to have unique employer identification numbers known as EIN while performing medical transactions.

National and International Law related issues in Cloud and how an hospitals/healthcare centres can fight it:

From a global Law perspective, the key distinction between ancient IT outsourcing and cloud computing is "where" information resides or is processed as information could also be spread across and stored in multiple data centres across the globe. Moreover, the utilization of a cloud platform might result in multiple copies of such information being saved in multiple in numerous locations. this is often true even for a "private cloud" that's pass by one client.

In fact, hospitals and its customers shall understand that cloud computing is vulnerable to data loss and potential corruption or interruption from earthquakes, terrorist attacks, floods, fires, power loss, telecommunications failures, system viruses, denial of service attacks, or alternative tries to hurt the relevant systems. Information centres which are set in areas with a high risk of major earthquakes is also subject to break-ins, sabotage, and intentional acts of anyone and to potential disruptions if the operators of those facilities have monetary difficulties.

Key issues which needs to be addressed are:

- **Data Location and Data Protection Law**: Hospitals/healthcare centres should make a note of where their customer data is being located and which law governs the contract and settlement if there any local or national political disputes that might take place. Hospitals may or may not be able to control or address this issue by contract as International laws might not agree for An Organisation to intervene in relevance to the contractual provisions.
- **Security and Performance**: Hospitals should make sure that the cloud service provider has a secure backup of the An Organisation patient's data and should have a ready-to-implement disaster recovery plan/strategy efficiently.
- **Legislation and Regulatory** (including the data privacy law aspect): Every nation has its own rules and regulations which govern the internet space in their country. It is required for an Organisation to know that these rules and regulations which are being governed will have direct impact on the cloud service provider. Hospitals should understand possible outcomes in multiple unexpected situations to know what happens to the customer data and when.
- **Data RetentionLaw**: Hospitals should realise that there will be several legal and tax aspects in every jurisdiction which would require An Organisation and its customers to retain data longer than the cloud vendor may be prepared to.
- Other insurance related issues.

Country-Specific Laws and Legal Regulations Hospitals/healthcare centres should know:

United States of America:

- HIPAA- The Health Insurance Portability and Accountability Act, sets the standard for protecting sensitive patient data. An Organisation when dealt with cloud service provider to safeguard protected health information (PHI), the cloud must ensure that all the required physical, network, and process security measures are in place and followed.
- GLBA- The Gramm-Leach-Bliley Act (GLB Act or GLBA). Hospitals should explain how their cloud service provider will share and protect their customers' private information.
- SCA- Service Contract Act. Hospitals/healthcare centres should make sure their cloud protects electronic information.
- SOX- Sarbanes-Oxley Act (SOX). Hospitals should protect shareholders and the general public from accounting errors and fraudulent practices, and to improve the accuracy of Financial disclosures.

Australia and New Zealand.

- NZISM- New Zealand Information Security Manual. An Organisation should be practicing the rules and regulations that are laid by the New Zealand Government to safeguard and protect user data and privacy.
- The Australian National Privacy Act- An Organisation should follow the rules as per Part 96A of Information Sharing Act on sharing and protection of user data.

Conclusion

In this paper I elucidated on what kind of approach that can be taken by the management of a hospital or healthcare centre when they decide to deploy their business services to the

All Rights Reserved © 2018 IJARCET

cloud while safeguarding user data, user privacy and application security from hackers who try to gain unauthorised access to the user information by exploiting vulnerabilities at application level on cloud. Helped understand the different delivery service architectures of cloud computing. I have demonstrated the legal and compliance issues in cloud computing, and how to efficiently work on them. Presented a formal approach or strategy on understanding different kinds of operations that are required for managing the resources of cloud efficiently.

References

- A survey of compliance issues in cloud computing. Dereje YimamEmail author andEduardo B. Fernandez. Journal of Internet Services and Applications20167:5 https://doi.org/10.1186/s13174-016-0046-8
- https://www.researchgate.net/publication/302066474_A_survey_of_compliance_issues_in_cloud_computing
- Regulatory Compliance in Cloud Computing: An ITperspective
  Melanie Viljoen, Rossouw von Solmsand Vivienne Lawack-Davids.
  https://pdfs.semanticscholar.org/725b/311df61fbfe5b4f57194dc0a883c48ae1ff6.pdf
- https://www.csoonline.com/article/3191542/cloud-computing/achieving-compliance-in-the-cloud.html
- https://www.netiq.com/docrep/documents/9vpbme9olg/netiq_sb_security_compliance_cloud.pdf
- https://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf
- https://www.managementstack.com/legal-and-compliance-issues-with-cloud-based-data-management/
- https://www.researchgate.net/publication/301222790_Cloud_Computing_Legal_Issues
- Regulatory Issues in Cloud Computing -An IndianPerspective.
  Mrs. Gowri Menon-
  http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.2221&rep=rep1&type=pdf
- Privacy Regulations for Cloud Computing
  Compliance and Implementation in Theory and Practice Joep Ruiter- Faculty of Sciences, VU University Amsterdam-
  http://homepage.tudelft.nl/68x7e/Papers/spcc10.pdf

About the Author

SAMEER DASAKA:

Experienced Security Analyst, Digital Forensic Investigator, Cyber Security Consultant and Internationally recognized Certified Ethical Hacker from the EC-Council, USA with a demonstrated history of working in the information technology and services industry. Hands-on Hacking experience on various platforms like Kali-Linux, BackTrack 5R3.

Reviewer for International Journal of Digital Forensics and Cyber Security.

Conversant with APT (Advanced Persistent Threat) Technologies. Hands-on Forensic experience on tools like EnCase,OSforensics,Autopsy.

Conversant with Advanced Static and Dynamic Malware Analysis.
Conversant with Stenography and its techniques. Conversant with Anti-Forensics tools and technologies.

Skilled in Entrepreneurial Strategic Management, OWASP Top 10 methodologies and SANS Top 25 for Vulnerability Assessment Testing, Web Technologies like HTML5, CSS3 JavaScript and Extensible Markup Language, Database support expert with hands on experience on Oracle SQL, MySQL, Windows Security Administration , Exploitation, Web Application Security Assessment, Linux Security Administration, and OS Level Troubleshooting.

Good knowledge on Information Security Standards and polices like ISO 27001 and 27002.

Programming experience on Android Studio and Eclipse Luna, Atom.

Core Competencies include Security Testing, Metasploit Frameworks, Network Testing, Windows OS Hacking, Wireless Hacking, Information Gathering, Passwords Hacking, Brute-Force Attacks and different Database Injection Attacks.
Strong Cyber Security Professional currently pursuing Masters degree focussed on Digital Forensics and Information Security from the Gujarat Forensic Science University.
Studied International Cyber Conflicts from State University of New York, USA.
Studied Cyber101X- Cyberwar, Surveillance and Security from The University of Adelaide, Australia.
Entrepreneurial Strategic Management from The University of New Mexico.

All Rights Reserved © 2018 IJARCET