SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

IT NO: IT22560094

INTRODUCTION TO CYBER SECURITY

# ASSIGNMENT 1

# CLOUD COMPUTING SECURITY

# Abstract

This research focus on cloud computing security and its evolution over time. This explores topics such as cloud computing basics, security concerns and possible solutions to these issues.my investigation also delves into the evolving landscape of cloud computing evolution from the early 2000s to the present 2020s. Additionally we discuss future development areas on cloud security such as Extended detection and response (XDR), Zero trust Network Access (ZTNA) and DevSecOps security. This research creates awareness about the current cyber security issues and provides insights in to safeguarding cloud environments.

# Introduction

In this research we embark on journey through the fundamental concepts of cloud computing, the need of secure cloud computing environments and the evolution of cloud security. We explore the key threats and concerns faced by cloud computing and propose potential solutions. The evolution of cloud computing security become apparent as we trace its path from early 2000s to the present day. Also, we explore future developments in cloud computing security.

This research aims to increase awareness of the ever-changing landscape of cloud security.

# Table of Content

# 1-What is cloud computing.

Cloud computing is a technology that provides additional space with some reliable computing resources without needing to own infrastructure. It has grown along with the fields of computing and offers assorted options to fulfil the needs of businesses of all sizes. This cloud computing mechanism is used all around the world. It has become popular because this method is affordable and does not require owning the hardware. In present cloud computing focus on helping to the businesses and provide a good service. Also, in the future cloud computing will be considered the global standards. Many major cloud providers such as amazon, google, Microsoft, HP and Dropbox are working together to set those global standards. The growth of the communication technology is also supporting to the cloud computing industry's growth. this is also playing a significant role in e-commerce systems. Technology has been growing consistently in various fields. Cloud computing is of the newer technology among them. To check whether the success rate of a modern technology it will check how much people use it and how long take it. Here are some examples [1].

| Technology | Time to gain 50 million users |
|---|---|
| Telephone | 50 years |
| Radio | 38 years |
| Television | 13 years |
| Personal computers | 16 years |
| Internet | 4 years |
| Google search engine | 3 months |
| YouTube | 11 months |
| Facebook | 2 years and 10 months |
| Twitter | 3 years |
| Cloud computing | |

According to the above chart telephone took a long time to become popular but internet became popular big quickly. But cloud computing was initiated less than the ten years ago.in the above table summarize the time span of user acceptance and old and modern technologies.

Cloud computing means using internet to access and use IT services, apps, and data. These data, apps, and software's stored on big, flexible computers that might be physically exist on far away. But users do not want to know where the computer devices are without knowing that they can use those computers. According to the National institute of standards and technology (NIST) the definition of cloud computing is still changing. According to them cloud computing is [2] "a model for enabling convenient, on demand network access to shared pool of configurable computing resources such as networks, servers, storage, applications, and services. That can be rapidly provisioned and released with minimal management effort or service provider interaction" Another similar definition of cloud computing is "the applications delivered as services over internet and the hardware and system in the data centres that provides the services." These services given by cloud computing can be identified like this [3],

| Service | Description |
|---|---|
| Software as a service (SaaS) | • Regular people who want to use apps without installing them on their own computers use this service.<br>• This is like borrowing software from the internet.<br>• These apps are stored on the internet.<br>• Examples-Google.com- get documents and emails<br>Salesforce.com manages customer information.<br>Google workspace-G-mails/google Docs, google sheets.<br>Microsoft 365-office applications, emails, and collaboration tools.<br>Dropbox-store and access data from any ware.<br>Zoom-video conferencing and online meeting.<br>Adobe creative cloud-photoshop, illustrator and InDesign.<br>Slack-Communicate and project management platform. |
| Platform as a service (Paas) | • Pass is for application makers, they get different computer resources as they need them like CPUs, memory, and storage.<br>• These Computers can change power and size depending on what the user needs.<br>• These flexible computers named as "elastic servers"<br>• They can automatically get bigger or smaller to handle the work.<br>• Examples-Google's app engine-build and host web applications.<br>Microsoft Azure-Hosting and management.<br>Red Hat OpenShift-deploying and managing applications.<br>AWS (Amazon Web Services) elastic beanstalk-amazon web service platform.<br>Heroku-Developers can build, deploy, and scale web applications.<br>IBM cloud foundry-open-source platform that supports development.<br>Oracle cloud platform-application development, database management and other cloud-based solutions. |
| Infrastructure as service (IaaS) | • The lowest layer in cloud computing.<br>• This is like renting a computer that is far away.<br>• Users can get computers with specific features like how fast it can think, how much memory it has and how much storage it can hold.<br>• These computers are available over the internet. |

| | |
|---|---|
| | • Examples- Amazon elastic computer cloud.<br>Open stack-open-source cloud computing platform.<br>Eucalyptus-open-source software platform.<br>Backspace's cloud files. |

Also, there are various kinds of cloud computing's which are public cloud, private cloud, and hybrid cloud. Public clouds are like the internet. Many people all around the world use this. Most of the time public cloud is free. Private cloud is for a specific group such as a company. It is like an internal network. Hybrid cloud is for smaller groups, but it can expand to use the public cloud when it needed. Microsoft Azura is an example for this.

## 2-Cloud computing security.

Cloud computing offers many advantages, but it also has numerous challenges and issues, especially when it comes to security. Protecting sensitive information and having a dedicated server needs to have when it comes to cloud environment. Cloud computing operates by over the internet. So, it will expose both incoming dangers and outgoing dangers. Such as,

| | | | | | |
|---|---|---|---|---|---|
| Incoming dangers | Unauthorized access | Data breachers | Distributed denial of service | Malware and viruses | Phishing attacks |
| Outgoing dangers | Data loss | Vendor lock-In | Compliance and legal issues | Data portability | Data interception |

To make the cloud computing space secure, it must need to extend its capabilities. To do that implementing a trusted encryption system, strict access control, back up control and many more mechanisms can be use.

Security in cloud computing systems is paramount. The main issue centres around the protection data are sensitive information. When organizations use cloud services, they do not want to third parties review their valuable information. Because of that privacy parameter is top concern in cloud security. Users need to have confidence that their data and information will not be comprised in any situation. This requires encryption systems and strict access control systems to safeguard data from unauthorized access or data breachers.

Moreover, the internet itself having some security issues. Cloud computing is an extension of the internet. Because of that cloud computing security need to address those challenges as well. Cloud computing also allows users to access computing power that goes beyond the capabilities of their local systems. While this is more advantages it introduces several security issues. For example, data privacy, data encryption, multi-Tenancy risks, resource over allocation and many more things can be named. So, provide a good security and privacy cloud computing need to overcome these challenges. We will be going to explore key security and privacy considerations that should be using and going to use in the world of cloud computing.

## 3-Key threats and concerns in cloud security.

Under this topic we are going to explore several key threats and concerns in cloud security, along with potential solutions to identify and overcome these issues.

| Key threat | Concern | Solution |
|---|---|---|
| Data security and confidentiality | Cloud computing users expect to protect their confidential information's. | Robust encryption<br>Access control.<br>Transparent data management practices. |
| Service uptime and reliability | Cloud computing users expect high level of service uptime and reliability.<br>Doen time or service interruption can lead significant disruption and financial losses. | Redundancy and Failover.<br>Service level Agreement (SLAs).<br>Monitoring and Alerting.<br>Load balancing.<br>Data backups and Disaster recovery.<br>Security measures.<br>Regular maintenance and updates.<br>User education. |
| Data protection responsibility | Cloud computing users expect their data to be secure, private, and compliant with relevant regulations.<br>Cloud users expect their data to be encrypted both transit and reset.<br>Cloud users expect to define user roles and permissions to prevent unauthorized access.<br>Cloud users concern about where their data is stored and which country's low and regulations apply on it. | End-to-End encryption.<br>SSL/TLS for data in transit.<br>Data-at-rest encryption.<br>Identify and Access management (IAM)<br>Role base access control (RBAC).<br>Multifactor authentication (MFA).<br>Data redundancy and compliance.<br>Legal and compliance expertise.<br>Privacy assessments and audits.<br>Data classification. |
| Security Transparency | Cloud users often feel they have limited visibility and control over the security of the information move to a cloud environment.<br>They expect to have transparent security measures and check how their information is being secured. | Share security policies.<br>Compliance data with third party registries. Ex:CSA STAR.<br>Comprehensive security documents.<br>Security Audit and certifications.<br>Transparency reports.<br>Security dashboards.<br>Incident response communication.<br>Security checklist and best practices. |

| | | |
|---|---|---|
| User Authentication. | Cloud users are concerned about identity theft, unauthorized access, and potential data breaches. | Multi factor authentication (MFA).<br>Strong password policies.<br>Biometric authentication.<br>Single-Sign-On (SSO).<br>User training and awareness.<br>Credential rotation and management.<br>Role based access control (RBAC). |
| Cloud storage security. | Cloud users expect their stored data to be kept confidential and inaccessible to unauthorized individuals. | Encryption.<br>Access control authentication.<br>Identify the access management (IAM).<br>Data classification and tagging.<br>Data loss prevention (DLP).<br>Regular security audit and penetration testing.<br>Geographical data residency options.<br>Data backup and disaster recovery. |
| Virtualization Vulnerabilities. | Cloud users are concern about the security of virtualized resources. They expect that virtualization layer to be protect against various kinds of vulnerabilities and provide a secure service. | Hypervisor security.<br>Isolation and segmentation.<br>Vulnerability scanning and penetration testing.<br>Virtual network security.<br>Regular security updates.<br>Zero trust architecture. |
| Third-party cloud brokerage. | Cloud computing users concern about the transparency of third-party cloud brokerage services. Such as cloud service resellers, multi cloud management, cloud brokerage marketplace and governance and policy managements.<br>Users expect clean information about how they managed and secure their data. | Transparency and reporting.<br>Service level agreement (SLAs).<br>Data ownership and control.<br>Data portability and vendor lock in prevention.<br>User education and training.<br>Clear exit strategies.<br>Collaborative governance. |
| Risk management Strategies. | Cloud users expect their service providers address potential vulnerabilities and fix those issues. | Risk assessment and vulnerability scanning.<br>Security audits and penetration testing.<br>Threat intelligence and monitoring.<br>Incident response plan.<br>Regular security updates and patch management.<br>Regular reporting and communication. |
| Data privacy and compliance. | Cloud users concern about the privacy of their data and check whether their cloud service providers comply with data | Data encryption.<br>Access control and authentication.<br>Data classification and tagging.<br>Privacy by design.<br>Regulatory compliance commitments. |

| | | |
|---|---|---|
| | protection protocols and regulations.<br>Users expect to protect their data in well behave manner and complies with relevant laws. | Data residency options.<br>Data privacy impact assessments (DPIA).<br>User education and training. |

## 4-Solutions for cloud computing security.

Solutions for the cloud computing security is like a shield to protect the user's information and data which is stored in a cloud storage. These solutions make sure that cloud users' data does not get loss or reveals for unauthorized parties. Also, this helps for cloud services to run smoothly, and it ensure users information always be there whenever users need it. Cloud security solutions use special mechanisms like cloud IAM identities, multi factor authentication, password, and API (Application Programming Interfaces) keys, Single sign on, centralized authorization, penetration testing, whitelisting, and blacklists, and many more. It also watches out any strange activities and let the user know if something suspicious going to happen.

Big companies like Amazon, Google and Microsoft have teams of experts working on these solutions. They follow rules and different mechanisms to make sure everything stays safe under the cloud computing. Here are some examples [4],

Fix Authentication –

- Cloud IAM identity.
- Multi factor authentication.
- Passwords and API keys.
- Single sign On

Fix Authorization-

- centralized authorization.
- Role base authorization.

Find new vulnerabilities-

- Runtime application self-protection scanners (RASP).
- Dynamic application scanner (DAST).
- Static Application Scanners (SAST).
- Inner application scanner (IAST).
- Penetration tests.

Fix network security-

- whitelists and blacklists.
- Overlay network and encapsulation.
- Proxies.

- IPv6
- Network address translation.

## Fix authentication using cloud IAM identity.

Fixing authentication using cloud Identity and Access Management (IAM) is a crucial step in managing and securing cloud computing. Many cloud providers offer IAM service at no extra cost. It will give clean idea to the users who have access to what in their cloud environment. Identity and Access Management helps to avoid the confusion of who has what kind of access level to their cloud systems. It is very helpful when dealing with dozen or even hundreds of users. Moreover, it plays crucial role in ensuring the security of user's organization. it will enable the swift removal of access when an individual user leaves on that organization. Different cloud providers offer their Identity and Access Management solutions. Such as amazon IAM for Amazon web services, Azura active directory B2C for Microsoft Azura, Cloud identity for Google computer cloud and Cloud IAM for International Business Machines (IBM) cloud.

## Fix Authorization using centralized authorization.

Fixing authorization using centralized authorization is an important step in managing and securing cloud computing. It manages who can do what kind of things in the cloud environment. In the past technology identities were scattered, so it is challenging to keep track of users who access on the cloud. But single-sign-on has improved identity management abilities in a cloud environment. Because of that cloud computing can centralize the authorization and provide better security to the users and system.

When cloud organizations need to control access more precisely, deleting someone’s identity, while effective, can be too drastic. But the centralized authorization offers more effective control with greater precision and control, all in one location. In a normal application, authorization was handled internally. But in the centralized authorization divides these responsibilities between the application and a centralized authorization system. These are the three main components which are handling the authorization.

Policy Enforcement Point (PEP)- This is implemented within the application, where access is controlled. If cloud computing users lack specifications, this application restricts those users from performing any action within the cloud system. Also, this policy enforcement point consults the policy decision point for take decisions.

Policy Decision Point (PDP)- This is implemented in the centralized authorization system. It takes information from the application PEP. Such information is user identity, user requested actions, system policy matches with the user request, is this user is a legitimate user and some other information's. Policy decision point analyse that information and decide whether this user is granted for the particular action.

Policy Administration Point (PAP)- This is also implemented within the centralized authorization system. This is some kind of web interface, where the users can define who they are and what they want to do in this cloud system.

Most cloud providers offer centralized access management to provide a decision-making ability. Because of this method each system does not need to make their own decisions, they can consult this centralized system. Using this method cloud computing users can view all the access granted administrators in one place. Because this centralized authorization simplifies the access control across the various cloud organizations.

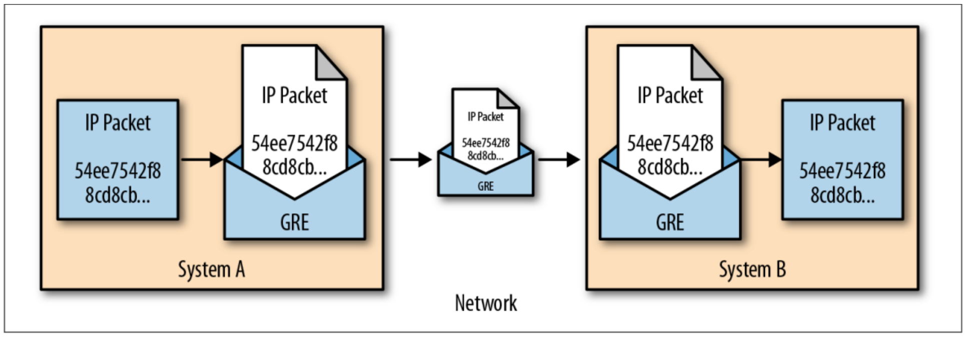
## Find new vulnerabilities using Runtime application self-protection scanners (RASP).

Discovering new vulnerabilities in cloud computing system is a critical task. If it is possible to do, it will be a huge advantage for ensure cloud security. One powerful method to achieve this is by using Runtime Application Self-Protection (RASP) scanners. This does not like the traditional scanner; RASP have different technologies rather than other scanners.

Runtime application self-protection operates in similar to Inter active security testing (IAST) technology. Because it involves to deploying an agent alongside its application code. However, RASP tool can block attacks not just the identifying vulnerabilities. IAST and RASP can impact the performance of cloud computing in some cases. Because it involves additional code running in the production environment.

RASP can provide a layer of protection to a distributed web application firewall (WAF). Both these are instruments to defend cloud computing against attacks in live production environment.

## Fix network security using Overlay network and encapsulation.



Fixing network security using overlay network and encapsulation is a crucial step in safeguarding the cloud computing digital environment. An overlay network is like a virtual network that sists on top of users exiting network. This overlay network is provided by cloud service providers. It allows users virtual system to talk to each other if they were on the same network.

To make this happen cloud security uses an encapsulation. Encapsulation work like this- when users virtual system wants to chat, their data packets are put inside another packet and sent across the cloud provider's network. It is like putting a letter inside of an envelope for secure sending. There are some common encapsulation methods using in the cloud environment. Which are VXLAN, GRE and Ip-in-IP.

Let us see an example of how this is happening. Virtual machine A on one cloud computer wants to have a chat with virtual cloud computer B. A computer sends out a packet, which gets wrapped up in another packet by the A computer. This wrapped packet travels to the B cloud computer. Then the B clod computer unwarp it and take the original packet to the B cloud computer. Even though these virtual cloud computers could be in completely various parts of the world. But they work like they are connected to the same Ethernet switch or Ip subnet.

Finally, overlay network and encapsulation creates a virtual pathway for cloud users' data. It seems like all cloud devices are Neighbours on the same network, even if they scattered all over the global. Using this method, it can enhance network security and efficiency.

# 5-Evolution of cloud security.

The evolution of cloud security is an important topic. In the early days of cloud adoption, businesses mainly had to decide if they want to use it with security as a secondary concern. But as cloud technology improves since world wide web inception cloud security becomes more secure and essential. Cloud security grows over the years and years, because of their new risks and their specific needs.

## In the early 2000s

In the early 200s, cloud security was in its infancy. This era saw a surge in the need for data canters with many businesses relying on shared hosting and dedicated servers. This concept of "cloud" emerged as a virtual environment. large technology companies like Amazon, Microsoft and google engaged an offering cloud services, with better security.

While cloud computing gained attention and businesses start to use it, cloud computing must face new challenges. Which are cyber-attacks happening on individual computers, networks, and internet-based systems. This includes malware attacks, network exploits targeting vulnerabilities and social engineering attacks like phishing. In this era cloud security mainly focus on cantered network security and access management. When use of cloud computing expanded, attackers give their attention on it. So, cloud needs to prevent those attacks. When there are trying to provide better security, it leads to evolution of cloud security.

## In the 2010s- Cloud security gaining a global momentum.

In the 2010s cloud security took significant growth and it leads to cloud computing became a part of many businesses. Unfortunately, this growth attracted more sophisticated cyber-attacks on cloud computing. For example, data breachers, crypto jacking, unauthorized access, steal sensitive data and stolen credentials happen. Because of these attacks it raises the importance of cloud security.

So, both cloud providers and organizations recognized the need of enhance cloud security measures. They implement stronger security control and promoting globally recognized countermeasures. This decade also introduced the cloud shared responsibility model. Which is clarifying the security responsibilities of cloud service providers and their organizations/customers. Major cloud providers like Amazon web servicers, Microsoft Azura and google cloud embraced this model. It helps to the businesses to understand their roles in cloud security.

Furthermore, cloud access security brokers (CASBs) gained prominence during this period. They acting as intermediaries between cloud service providers and consumer to enhance visibility, control, and security enforcement across the cloud environment. Also, these CASBs played curial role in addressing the evolving cloud security landscape. Overall, the 2010s marked a pivotal period in the evolution of cloud security.

### The 2020s- Future developments in cloud security.

Cloud security has come a long way, especially in the 2020s. With the growth of cloud technology and the rise of remote work, businesses are embracing cloud environments more than ever. How ever the security challengers are persisting. In the third section of this report, we discuss those vulnerabilities and modern threats. And, to overcome those threats and provide a good security to the users and cloud environment, various methods are using. Such as cloud IAM identity, single sign on, centralized authorization and many more. Those current developments in the cloud security were already discussed in the 4th part of this research. These advanced security features help to build strong security posture for present cloud environment.

## 6-Future developments in cloud security.

The evolution of cloud security has become increasingly vital due to the rapid growth in cloud adoption and technology growth. Also, in the post-COVID world create a need for remote work and digital transformation. As cloud technology enable remote access and digital operations, it became essential to ensure business continuity during the pandemic. However, the shift to remote access also made cloud infrastructure a prime target for cyber-attacks and vulnerabilities.

To address these challenges, cloud security needs to be sharper in the future. These technologies are crucial in defending against evolving security threats in the cloud environment.

### Extended Detection and Response (XDP)

Extended detection and response (XDR) are a technology that helps the organizations to enhance their cyber security efforts. XDR serves as an all-in-one security platform. It gathers information from various components and create unified system and it eliminates the organizational need of multiple security tools. XDR technology can enhance cloud security by enabling the detect threats and response those threats. This XDR works across the various cloud platforms and unprotected endpoints by providing comprehensive security to the organizations. Because of that organizations can protect their digital assets effectively.

| Features on XDR | Description |
|---|---|
| Identity Management Monitoring | • Also known as user and role activity monitoring.<br>• It can detect unauthorized user activities and insider threats.<br>• When it finds any unauthorized activity, it will trigger alerts to security teams. |
| Cloud log Analysis | • Also known as log processing with AI.<br>• It can analyse large volume of cloud logs.<br>• It automatically processes cloud logs and use AI algorithms to detect and response to potential risks. |
| Network flow Analysis | • Also known as network traffic analysis.<br>• It can help to complex network security issues.<br>• This will analyse network traffic across the cloud eco system.<br>• After analysing it can identify security incidents and can respond automatically by isolation infected systems. |

## Zero Trust Network Access (ZTNA)

Zero trust network access (ZTNA) is a technology that helps organizations to ensure secure remote access to their cloud services. It works by setting specific rules, which are including who can access what in the cloud computing. ZTNA let remote user to access but does not give them free rein. Instead, it starts with denying access as the default. Access is granted when a user explicitly needs it, based on numerous factors like the time, type of task, data they need and their specific actions. In this ZTNA changes cloud security by applying the idea that "Trust should be earned for each user."

Here are some Zero trust networks access tools.

- Access control lists (ACLs)
- Multi factor authentication (MFA)
- Identity and access management (IAM)
- Micro segmentation.
- User behaviour Analytics (UBA)
- Dynamic access control policies.

## Development security and Operations integration.

DevSecOps integration is a modern approach in software development that make sure security is part of the entire process. It is like adding a security guard to a building to keep it safe. In traditional cloud computing security is often an afterthought, like checking if the doors are locked after the building is already built. But in DevSecOps the security is considered right from the start. Like building strong doors and locks while constructing the building.

DevSecOps make sure that security is everyone's job not just the security teams' responsibility. It is like asking all the people in a neighbourhood to keep an eye out for anything unusual to protect their community. This way cloud computing is safer from potential threats, like cyber criminals trying to break in. Because security is thought about from the very beginning, and it is everyone's responsibility.

There are some tools that helps integrate security measures in to DevSecOps ,

| Tools | Description |
|---|---|
| Docker | Helps to create, ship, and run applications as secure, portable containers. |
| Git | It keeps track of code changes, making it easier to manage and secure the cloud computers. |
| Jenkins | Automated building, testing, and deploying code, include security checks. |
| Chef | Manages software configuration and ensure security steps. |
| Puppet | Automate software and infrastructure management while enforcing security policies. |
| Burp Suite | Scan web applications for security vulnerabilities aiding and fixing. |

# Conclusion

In conclusion, my exploration of the world of cloud computing security has revealed a dynamic landscape of challenges and solutions. We have discussed what cloud computing is and why its security is paramount. We have identified key threats and concerns of cloud computing environment. Thought my research, we have unveiled the importance of cloud security solutions. Such as cloud IAM identity for authentication and centralized authorization for secure access. We have also decribe the role of RASP scanners in uncovering vulnerabilities and the use of overlay networks to fulfil network security.

The evolution of cloud security, from early 2000s to the present and how it evolving threats is another important topic I have presented. We have seen the global momentum gained by cloud security in the 2010s and the promise for future developments in the 2020s.

Extended detection and response (XDR) and Zero trust network access (ZTNA) have emerged powerful tools, to prevent cloud security challenges in the future digital age. Also, the DevSecOps has various tools to provide effective security to the future cloud computers.

Finally, our research achieved its goal of raising awareness about cyber security. It showed that cloud computing security keep changing, so users need to stay alert on it. We suggest investing in better security and educating people in this area are the most effective steps to follow.

# References

1. How Long Does It Take to Hit 50 million Users? Chart: How Long Does It Take to Hit 50 million Users? (visualcapitalist.com)
2. The NIST definition of Cloud Computing. Mell, P., & Grance, T. (2009) (Version 15 ed.) Available: http://csrc.nist.gov/groups/SNS/Cloud-computing/Cloud-def-v15.doc.
3. Cloud Computing Definitions. Cloud Computing with Security Concepts and Practices Second Edition Naresh Kumar Sehgal Pramod Chandra P. Bhatt John M. Acken.
4. Solutions for cloud computing security. Practical Cloud Security A Guide for Secure Design and Deployment book.