International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2016 IJSRCSEIT | Volume 1 | Issue 2 | ISSN : 2456-3307

Security Issues in Various Cloud Computing : Solution and Occur-Rent Solutions

*Banoth Anantharam, Gurnadha Guptha

CSE Department, Assistant Professor, Sri Indu College of Engineering and Technology, JNTU Hyderabad, Hyderabad, India

ABSTRACT

Cloud computing modified the world around us. Currently, individuals are moving their information to the cloud since information is obtaining larger and needs to be accessible from several devices. Therefore, storing the information in the cloud becomes a norm. However, there are several problems that counter information hold on within the cloud starting from the virtual machine that is supposed to share resources within the cloud and ending on cloud storage itself problems. During this paper, we tend to gift those problems that are preventing individuals from adopting the cloud and provide a survey of solutions that are done to reduce risks of those problems. For instance, the information held on within the cloud must be confidential, protecting the integrity and obtainable. Moreover, sharing the information held on within the cloud among several users continues to be a problem since the cloud service supplier is entrust to manage authentication and authorization. During this paper, we tend to list problems associated with information held on in cloud storage and solutions to those problems that disagree from different papers that concentrate on the cloud as general.

Keywords: Information security, Data Confidentiality, Data Privacy, Cloud Computing, Cloud Security.

I. INTRODUCTION

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility.

Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance.[1] Advocates note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable business demand.[1] [2] [3] Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models.[4]

Schematic definition of cloud computing can be simple, such as seen in Figure 1

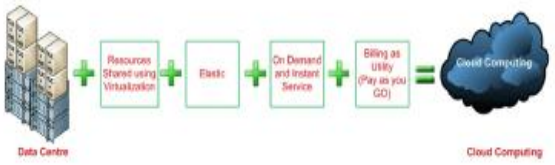

Figure 1 : Schematic definition of cloud computing

Since the launch of Amazon EC2 in 2006, the availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing has led to growth in cloud computing. [5] [6] [7].

II. CHARACTERISTIC OF CLOUD COMPUTING

Ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models

Essential Characteristics:

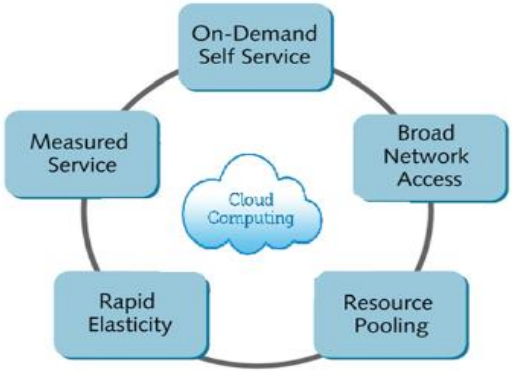

Figure 2

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data enter). Examples of resources include storage, processing, memory, and network bandwidth.
Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

III. SERVICE MODELS

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Figure 3

Software as a Service (SaaS).
The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS).
The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or

acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS).
The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

IV. DEPLOYMENT MODELS

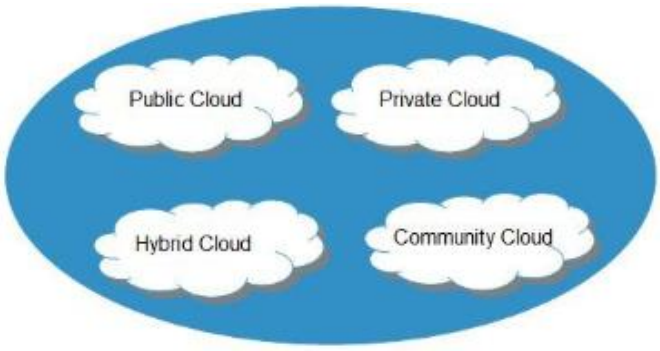

Figure 5

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

V. CLOUD SECURITY ISSUES:

These regular headlines, especially mega breaches like those at Target and Sony that led to executives at both companies resigning, have made the security of data in the cloud an executive-level and board-level concern at 61% of companies. Against a backdrop of increasingly sophisticated attacks aimed at stealing corporate data, many IT leaders feel uncomfortable with a perceived loss of control over corporate data. The Cloud Security Alliance survey identified 6 primary issues holding back cloud adoption, summarized below, and starting with the most common issues:

1. **Security of data** – It's no surprise that data security tops the list of concerns that hold companies back from cloud adoption. 73% of survey respondents indicated this is a big red flag for them. Cloud service providers are targets data breaches (e.g. email service Send Grid and online note-taking service Ever note), which makes it critical for companies to use risk mitigation strategies and tactics, such as encrypting or tokenizing data before it ever goes to a cloud service.

2. **Non-compliance with regulatory mandates** – PCI DSS, HIPAA/HITECH, GLBA, FISMA, FERPA, EU data protection, ET. Al. Whatever the regulatory acronym, you will find that 38% of companies are concerned with how they can assure compliance with regulations if their data is in the cloud. A security breach that leads to non-compliance with a regulatory mandate can result in expensive fines, loss of business, lawsuits, and potentially even criminal penalties (as in the case of ITAR non-compliance).

3. **Loss of control over IT services** – 38% of the CSA survey respondents say their fear over loss of control

keeps them from moving data into cloud-based applications. This loss of control cam is manifested in numerous ways. The cloud service provider may choose how and where data is stored; how often it is backed up; which encryption scheme is used, if one is used at all; which of its employees have physical or virtual access to the data; and more. But even if the cloud service provider invokes feelings of total trust, the fact remains that the data owner is still liable for any data breach that might occur, and this leaves more than a third of all companies hesitant to use cloud services

4. **Expertise of IT and business managers** – 34% of companies aren't jumping on the cloud bandwagon because they believe the knowledge and experience of their IT and business managers are not aligned with the skillets that cloud computing demands. For example, in addition to the technical knowledge a manager is expected to have, the person also needs financial literacy for a new computing model where services are rented, not owned, plus negotiation skills to drive a cloud provider's SLA to the company's benefit.

5. **Compromised accounts or insider threats** – 30% of the CSA survey respondents are concerned about what would happen if their accounts held by a SaaS provider were to be compromised in some way, or if an insider with that provider did a little "extra-curricular activity" and poked around in private accounts. Their concerns are not misplaced. Skyhigh's own analysis has found that 92% of companies have employees with compromised credentials for sales on the dark net. And the incidence of insider threats is much higher than otherwise known by the IT department.

6. **Business continuity and disaster recovery –** What happens to a company if it loses all access to its IT infrastructure because its cloud provider has suddenly gone out of business? It's a rare scenario, thank goodness, but it happens, and this makes 28% of the CSA survey respondents too nervous to embrace cloud computing. A company doesn't abdicate its obligation to do proper business continuity and disaster recovery planning just because it no longer operates the physical aspects of its IT infrastructure, but recovering data from a defunct cloud service – and finding an alternative home for that data – can be a huge challenge.

VI. MULTITENANCY

In [2], the author did not consider multitenancy as an essential characteristic of cloud computing. However, in CSA [24] and ENISA [25], multitenancy is considered an important part of cloud computing. However, with the many benefits mufti-tenancy offers, this leads to many challenges regarding having more than one tenant on one physical machine, which is required to utilize the infrastructure. Since tenants are in the same place, they could attack each other. Previously, an attack could be between two separate physical machines but now because two or more tenants are sharing the same hardware, an attacker and a victim can be in the same place. In figure, the difference between multi-tenancy and traditional cases is shown. The technology is used to keep tenants from each other by providing a boundary for each tenant by using virtualization. However, virtualization itself is suffering from many issues.

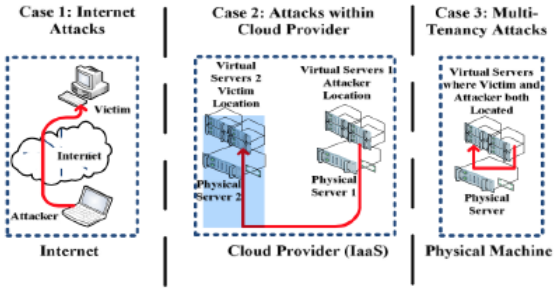

Figure 6. Difference between Multi-Tenancy and Traditional Cases.

VII. VIII. VIRTUALIZATION SECURITY ISSUES

Virtualization is an important component of cloud computing. Now it is getting more attention from academic and industrial communities. Vitalization means separation of underlying hardware resources from provided resources. By using virtualization, two or more operating systems might run in the single machine with each having its own resources.

A. Cross Virtual Machine(VM) Side-Channel Attacks

This attack requires the attacker to be in another virtual machine on the same physical hardware with the victim. In this attack, the attacker and victim are using the same processor and same cache. When the attacker

alternates with the victim's VM execution, the attacker can attain some information about the victim's behavior. In [27], there is an example of VM side-channel attack and how the attacker can infer some information about a victim. The timing side channel attack is one kind of VM side channel attacks [28]. This attack is based on determining the time needed by various computations.

Determining this time can lead to leaking sensitive information such as described in [28]. This attack can help in leaking some sensitive information such as to the one who performs this computation or sometimes leaking information out of cloud provider itself. This attack is hard to detect because the owner of VM can check other VMs due privacy concern.

Sometimes cloud providers can detect a side channel attack but to protect their reputation but they do not announce it. Moreover, there is another type of side channel attacks which is energy-consumption side channel [29].

B. VM Image Sharing

VM can be instantiated from a VM image. A shared image repository can be used to share VM images or a user can have his own VM image [30]. Since there is a repository for sharing VM images, some malicious users could take advantage of this feature in order to inject a code inside a VM [31]. This will lead to a serious problem. For example, a VM image may contain malware. This malware is coming from the user who used it before [31]. If the image is returned without properly cleaning it, sensitive data could be leaked [30].

C. VM Isolation

Since VMs run in the same hardware, they share all com-ponents such as processor, memory, and storage. Isolating of VM logically to prevent one from intervening with another is not enough since they are sharing computation, memory, and storage. Therefore, the data may leak when it is in computation or memory or storage. This is a serious issue. Hence, isolation should be at the level of VM and hardware such as processor, memory, and storage [32].

D. VM escape

The VMs or a malicious user escape from the virtual machine manager(VMM) supervision [33]. VMM controls all VMs and it is the layer that controls how the VM or a user who uses the underlying resources such as hardware. One of the most serious scenarios is that malicious code can go through unnoticed from the VMM and then can interfere with the hypervisor or other guests [31].

E. VM Migration

VM migration process suspends the running VM, copies the status from the source Virtual Machine Monitor (VMM) to the destination VMM and resumes the VM at the destination [11]. In virtual machine migration, the running VM is suspended, has its status copied to the virtual machine monitor (VMM) from its source VMM, and is resumed on the destination VMM [34]. In [35], VM migration is defined as the moving of a VM from one physical machine to another while it is running without shutting it down. Fault tolerance, load balancing, and maintenance are some causes of VM migration [30], [36]. The data and the code of VM [35] are exposed when transferring in the network between two physical hardware locations when they are vulnerable to an attacker. Also, an attacker could let VM transfer to a vulnerable server in order to compromise it. When hen an attacker compromises the VMM, he can get a VM from this data center and migrate it to other centers. Therefore, he can access all resources as a legitimate VM [37]. Therefore, this process incurs more challenge and needs to be secured [30] In order to prevent attackers from benefiting.

F. VM Rollback

This is a process of rolling back a VM to its previous state. Since this process adds more flexibility to the user, it has more security issues. For example, a VM could be rolled back to previous vulnerable state that has not been fixed [38] or it can roll back to an old security policy or old configuration [30]. In another example, a user could be disabled in a previous state and when the owner of the VM rolls back, the user can still have access [30].

VIII. MOBILE CLOUD COMPUTING

A. Limitations of mobile devices

With the advancement in mobile devices such as more Processing, storage, memory, sensors and operating system capabilities, there is a limitation with regard to energy resources needed for complex computation. Some of the application in mobile devices is data-intensive or compute-intensive application. Due to battery life, the mobile device cannot run them. Therefore, the cloud computing is needed to run those complex computations. The mobile device's application augments the processing tasks to the cloud computing.

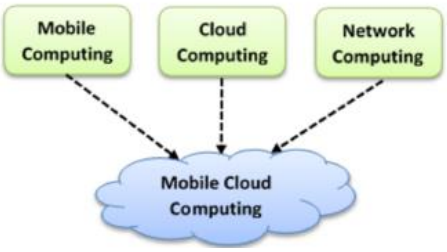

Figure 7. Mobile cloud computing

B. Mobile Cloud Computing

Mobile cloud computing is using the mobile as front end and the cloud as back end for the storage and computation.

In the figure, mobile cloud computing consists of mobile computing, cloud computing, and network.

Three schemes are proposed for confidentiality and integrity of mobile device's files stored in the cloud. The first scheme is encryption based Scheme (ENS). In this scheme, the mobile device encrypts the file and gets its hash code. The encryption key is a concatenation of the password entered by a user, file name changed to bits and file size to defend brute force attack on a cloud server since the length of the password is limited. Only the file name is kept in the file and everything related to the file is deleted. When downloading the file from the cloud server, only the password is needed to decrypt the file. This process will need more processing on the mobile device side. They proved the confidentiality and integrity of the file using this scheme when it is stored in a distrusted clouds server. In order to overcome the power consumption in the first scheme, a coding based scheme is proposed. This scheme is not using encryption function since it consumes less power. The confidentiality of the file is protected by using matrix multiplication and the integrity is ensured by using hash-based message authentication code. The file is divided to many blocks and each block is divided to many chunks and each chunk in n bits. Each block represents matrix with chunks number as rows and bits as columns. A code victor matrix is created from the entered password. For confidentiality, each matrix is multiplied by the code victor matrix which results in secrecy code. For the integrity, all secrecy codes are concatenated and hashed. The result of the previous is the integrity key. The file is hashed with the integrity key which results in message authentication code. The third scheme is Sharing based Scheme (She) which applies X-OR operations on the file. This scheme needs less computational power. Hash-based message authentication code is used to verify the integrity of file while X-or operation is used to protect the confidentiality of the file.

Khan et al. propose a new scheme called block-based sharing scheme. This scheme overcomes all limitations of the previous schemes proposed in [76]. They use X-OR operation. First, they extend the password entered by a user in order to be the same as block size. For example, the Block size is 160 bit and the password entered by the user Is 60 bits. In this case, they extend 60 bits to be 160 bits.

Second, they divide a file to blocks with the same size. After That, they X-or the first block with first extended password.

The second block is X-ORed with extended password after shifting each bit to the right. Therefore, each block is x- ORed with distinct password with size equal to the size of block. For integrity, they hash the concatenation of the file name, extended password and file size in order to get an integrity key. Then, they hash the file with the integrity key in order to get message authentication code. Once that done, only cipher text, message authentication code, and the hash of file name to the cloud. The hash of file name is sent for file retrieval. This scheme results in less energy consumption, memory utilization, and CPU utilization.

In, the authors used homomorphism encryption, multi-cloud computing and mobile. They used multiple cloud

schemes for storing the data to avoid data lock in and used homomorphism encryption to run computations without down-loading the data back and forth between cloud computing and mobile to avoid the communication costs. Since encryption is expensive for the mobile devices, there are some propositions to avoid using it.

In [79], Bahrami1 et al. proposed a lightweight method for data privacy in mobile cloud computing. They used JEPG file as their case study because it is a common file in mobile.

They divide the JEPG file into many splits, distribute them to many file based one predefined pattern, and scramble chunks randomly in each split file with help of pseudo-random permutations with the chaos system. After that each file is sent.

To MCCs. For retrieval process, the split files are collected from MCCs. Each split chunks are rearranged by using the chaos system. After that, all split files is rearranged based pattern, predefined before. They used this method because it is low in computation and works effectively in the mobile. When they compared it with encrypting the JEPG in the mobile and sending it, they found their solution is more efficient. Their proposed method has two requirements: balancing computation overhead with maintaining the security and avoiding offloading the file to the mobile cloud computing for encryption by making the file is meaningless before sending it.

IX. CONCLUSION

Cloud computing is an rising technology which will receive a lot of attention within the future from business and academe. The price of this technology is a lot of engaging once it is compared to building the infrastructure. However, there square measure several security problems returning with this technology as happens once each technology matures. Those problems embody problems associated with the previous problems with the net, network problems, application problems, and storage problems. Storing information in a very remote server results in some security problems. Those problems square measure associated with confidentiality of knowledge from unauthorized folks in remote sites, the integrity of keep information in remote servers and therefore the convenience of the information once it's required. Also, sharing information within the cloud once the cloud service supplier is mistrusted is a difficulty. However, we tend to mention some techniques that defend information seen by the cloud service supplier whereas it's shared among several users. Many studies are conducted to get the problems that have an effect on confidentiality, integrity, and convenience of knowledge to search out an answer for them. Those solutions can cause safer cloud storage, {which can which can which is able to} additionally cause a lot of acceptance from the folks and therefore the trust on the cloud will increase.

X. REFERENCES

[1]. "What is Cloud Computing?" Amazon Web Services. 2013-03-19. Retrieved 2013-03-20.

[2]. J Baburajan, Rajani (2011-08-24). "The Rising Cloud Storage Market Opportunity Strengthens Vendors". It.tmcnet.com. Retrieved 2011-12-02.

[3]. Oestreich, Ken, (2010-11-15). "Converged Infrastructure". CTO Forum. Thectoforum.com. Archived from the original on 2012-01-13. Retrieved 2011-12-02.

[4]. "Where's The Rub: Cloud Computing's Hidden Costs". 2014-02-27. Retrieved 2014-07-14.

[5]. "Cloud Computing: Clash of the clouds". The Economist. 2009-10-15. Retrieved 2009-11-03.

[6]. "Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner. Retrieved 2010-08-22.

[7]. Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld. Retrieved 2009-06-02.

[8]. E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in HighPerformance Cloud Auditing and Applications. Springer, 2014, pp. 3-33.

[9]. I. Gul, M. Islam et al., "Cloud computing security auditing," in Next Generation Information Technology (ICNIT), 2011 The 2nd Interna- tional Conference on. IEEE, 2011, pp. 143-148.

[10]. E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanceddata security model for cloud computing," in Informatics and Systems (INFOS), 2012 8th International Conference on. IEEE, 2012, pp. CC- 12.

[11]. S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in Information Security for South Africa (ISSA), [12] 2010. IEEE, 2010, pp. 1-7.
[12]. F. Sabahi, "Cloud computing security threats and responses," in Commu-nication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, 2011, pp. 245-249.
[13]. X. Wang, B. Wang, and J. Huang, "Cloud computing and its key techniques," in Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on, vol. 2. IEEE, 2011, pp. 404- 410.
[14]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, vol. 34, no. 1, pp. 1-11, 2011.
[15]. J. Yang and Z. Chen, "Cloud computing research and security issues, "in Computational Intelligence and Software Engineering (CiSE), 2010International Conference on. IEEE, 2010, pp. 1-3.
[16]. M. Lori, "Data security in the world of cloud computing," Co-published by the IEEE Computer and reliability Societies, pp. 61-64, and 2009.
[17]. C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," Network, IEEE, vol. 24, no. 4, pp. 19-24, 2010.
[18]. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing,"[19] Information Sciences, vol. 258, pp. 371-386, 2014.
[19]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1-9.