Original Article

The Layers of Cloud Computing Infrastructure and Security Attacking Issues

[1]Firas Hanna Zawaideh, [2]Waheed Ali H. M. Ghanem, [3]M. Hafiz Yusoff, [4]Syarilla Iryani A. Saany, [5]Julaily Aida Jusoh, *[6]Yousef A.Baker El-Ebiary

[1]Asst. Prof. Dr., Cyber Security Department, Faculty of Science and Information Technology, Irbid National University, Jordan, Email: F.Zawaideh@inu.edu.jo
[2]Asst. Prof. Dr. Faculty of Engineering, University of Aden, Yemen. And Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu, Terengganu, Malaysia, Email: waheed.ghanem@gmail.com
[3]Assoc. Prof. Dato' Dr., Deputy Vice Chancellor for Student Affairs, UniSZA, Malaysia, Email: hafizyusoff@unisza.edu.my
[4]Assoc. Prof. Dr., Faculty of Informatics and Computing, UniSZA, Malaysia, Email: syarilla@unisza.edu.my
[5]Dr., Faculty of Informatics and Computing, UniSZA, Malaysia, Email: julaily@unisza.edu.my
*[6]Assoc. Prof. Ts. Dr., Faculty of Informatics and Computing, UniSZA University, Malaysia,

***Corresponding Author: -** Yousef A.Baker El-Ebiary

*Assoc. Prof. Ts. Dr., Faculty of Informatics and Computing, UniSZA University, Malaysia, yousefelebiary@unisza.edu.my
https://orcid.org/0000-0002-4392-8015
Doi: 10.47750/pnr.2022.13. S05.124

Abstract

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet. Cloud computing is not a computer network only it's about hosting and services that are provided, run, and maintain over that network. Application or documentation is hosted on a single company server and accessed via the company network with network computing. Cloud computing is bigger than that it Includes multiple companies, multiple servers, as well as multiple networks. In this paper, we mainly discuss three main issues of cloud computing issues in the cloud, Attacks on cloud infrastructure, and security at different layers in the cloud. The main objectives of this research are to identify the meaning of cloud computing, get knowledge about the history of cloud computing, identify issues in cloud computing, identify challenges in cloud computing, and identify solutions for the issues in cloud computing. The research also touches on the cloud services are now an integral part of corporate life, bringing with them the opportunity to accelerate business with their fast-tracking capabilities, allowing us to accelerate our resources, and provide new opportunities for collaboration. The world today is becoming increasingly cloudy, and the effects of businesses and consumers alike are far-reaching. Cloud Computing brings many benefits to its users such as reduced costs, easy shipping, scale as you want, etc.

Keywords: Cloud Computing, Availability, Auditability, Trust, Access management

I.INTRODUCTION

A. Background

First, cloud computing is not a network computer. With network computing, application or documentation hosted on a single company server and accessed via the company network. Cloud computing is bigger than that it Includes multiple companies, multiple servers, as well as multiple networks. And, in contrast network computing, cloud services and storage are available from anywhere in the world via the Internet communication; with a computer network, access is more than company network only. Cloud computing is also not a traditional release, where the company subcontracts its computer services to a third party. While the output firm can hold company data or applications, those documents and programs are accessible only to corporate employees via the company network, not to worldwide via the Internet [1]. Therefore, with the exception of the superficial similarities, networking computing and outsourcing are not the same cloud computing.
Cloud computing has since seen the emergence of a large business transition including professionals from a position-based infrastructure in cloud-based programs in pursuit of more computational power. Cloud types such as Private, Public or Hybrid can be accepted depending on the need of the application. Cloud Provider offers three types of services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Depending on the need for the application the user can request or receive services from the cloud provider [2, 3].

B. The Problem

The public cloud offers cost-effective services that pay for what you use. Increased recruitment, durability and third party control have a high risk of data leakage or attacks within the infrastructure. Many app services may require compliance with compliance requirements that require the establishment of SLA's with the provider [3]. The cloud state of the community does not provide control of underlying infrastructure and it is difficult to conduct forensic analysis in the event of a disaster; this increases the risk of sensitive data. Here mainly discuss problems are,

- Issues in public cloud models that features such as high employment, durability, etc. they have a very safe risk of catching sensitive data.

- An overview of the different strategies and attack methods used in the cloud infrastructure that could lead to leaked confidential data.
- Security implementation in various areas of cloud infrastructure and highlights potential solutions and SLA's to improve the security of underlying infrastructure.

C. Objectives

- To identify what is cloud computing?
- To get knowledge about history of cloud computing
- To Identify advantages and disadvantages
- To identify issues in cloud computing
- To identify challengers in cloud computing
- To identify solution for the issues in cloud computing

D. The proposed solution.

Strengthen trust between provider and customer by establishing various SLA's compliance standards and addressing the issues described in the problem section

II. LITERATURE REVIEW

A. Origin of the term "Cloud Computing"

Google "cloud computing" search resulted in 72,500,000 hits (October 3, 2013). Apparently it is one of the hottest buzz words on a computer. It is an analogy to computers connected to the Internet that are often plugged into a cloud-like border in the numbers of initial power presentations. The most popular words were used by Eric Schmidt (then Google CEO) in 2006 at an industrial conference. A company called Net Centric (now unemployed) applied for the 'cloud computing' trademark in 1999 with educational services(Ref-1). According to the first installment of Wikipedia (since its removal) it was first used in educational publications by Ramnath Chellappa of the Department of Management at the University of Texas, Austin in 1997 [4].

B. Cloud Access device

Cloud servers can be accessed by PC, Laptop, Tablet, or Smart phone. One might ask if there is anything else specifically designed to access services in the cloud especially because when there is a large computer power found in the cloud why should the access device also require computing power. In addition, PCs and their descendants have an inflamed OS, take minutes to start, expire, need virus protection, and are expensive. Smaller clients have a better graphics interface, are more expensive than PCs, are timeless, and do not need virus protection [5].

However, they are not compatible with mobile phones. In 2011 Google designed a low-cost, lightweight client called Chromebook (Ref-3) to reach the cloud. It has a Linux-based OS, a built-in Chrome browser, a media player, virus proof, and boots in less than 10 seconds. Made by several competing manufacturers including Google [6]. The biggest criticism of Chromebook is that it relies entirely on the cloud to do anything useful.

C. John McCarthy's Memo

In 1957, John McCarthy had visited the Massachusetts Institute of Technology and had begun work on Artificial Intelligence. At that time MIT had an IBM 704 mainframe computer used in batch mode.About a day to get a print with the calculation results. Often, after impatiently waiting for the day, a minor syntax error in the system can lead to system failure [7].

Usually it took three or four attempts to get one useful result from a computer. McCarthy, who joined MIT in 1959, wrote in frustration, a letter to the Director of the Computer Center suggesting that teletypers writers from faculty offices be connected to a computer that allows shared time-shared computer use by many people [8].

The idea was revolutionary. Fernando Corbató, former Associate Director of Computer Center at MIT, challenged his team to design what is known as the Compatible Time Sharing System (CTSS). The program came into effect in 1961. When a computer is not allocated 'allotted time, the next question is why not using a computer as a power consumption. In a 1961 speech, on the occasion of the MIT centenary celebrations, McCarthy stated, "If the computers of the kind I have advocated become computers of the future then computers someday will be organized as a public utility just as a telephone system is a public utility. The computer utility could become the basis of a new and important industry." [9].

D. Cloud Computing History

1959 John McCarthy's note on the need to share computers from time to time. 1961 John McCarthy's speech proposing that computers should be something like a telephone service. In 1966 Douglas Parkhill published a book entitled Computer Challenges. 1995 Amazon begins selling books using the World Wide Web. 1999 Salesforce.com provides software service on the World Wide Web for free. In 1999 Ian Foster and Carl Kesselman published a book entitled The Grid: Blueprint for a new computer infrastructure and development of Globus toolkit to build a computer grid. 2004 Google launches a free email service. 2006 Amazon introduces payment for using computing (Amazon Web Services) and Elastic Cloud Computing (EC2). 2006 Google begins providing Google Apps with 2 GB of free disk space on their infrastructure. In 2010 Microsoft started providing a cloud service called Azure. 2011 IBM offers smart cloud. 2012 CloudBolt has been

launched. It develops a hybrid cloud management platform that helps organizations build, deploy and manage private and public clouds [10].
The openQRM for the 2013 cloud management platform is being released. In 2014 Amazon launched AWS Lambda, the first vendor of public cloud infrastructure that provides a non-server server. 2015 Citrix Systems launches Citrix Cloud, a cloud management platform that allows organizations to use desktop and cloud-based applications to eliminate users. The services of IBM Cloud 2016 are released to the IBM Cloud community. 2017 Amazon Web Services starts using pay per second for Linux virtual machines. The 2018 Apache CloudStack is being released. 2019 CDN Market is estimated to be more than US $ 10 billion per year. 2020 The global cloud computing market is estimated to exceed US $ 241 billion at the time, with companies such as Amazon Web Services and Salesforce quickly becoming global leaders in their respective fields [11].

E. Advantages and Disadvantages of Cloud Computing

Advantages [12, 13, 14]:

- Easy implementation. Cloud hosting allows a business to maintain the same business plans and processes without having to deal with background technology. Easily controlled by the Internet, cloud infrastructure can be accessed by businesses easily and quickly.
- Accessibility. Access your data anywhere, anytime. Internet cloud infrastructure increases business productivity and efficiency by ensuring that your app is always available. This allows for easy interaction and sharing between users in multiple locations.
- No hardware required. Since everything will be hosted in the cloud, visible storage space is no longer needed. However, backing up should not be considered in the event of a disaster that could leave your company's product standing.
- Cost per head. The cost of high technology is kept to a minimum with cloud hosting services, enabling businesses to spend more time and resources on improving company infrastructure.
- Flexibility for growth. The cloud is very scary so companies can add or remove resources depending on their needs. As companies grow, their system will grow as well.
- Proper recovery. Cloud computing brings faster and more accurate retrieval of applications and data. During a short break, the recovery system works very well.

Disadvantages [15, 16, 17]:

- It is no longer controlled. When you deploy services in the cloud, you provide your information and information. Companies with internal IT staff, will not be able to handle the challenges alone. However, Stratosphere Networks has a 24/7 live help desk that can fix any problems quickly.
- It may not get all the features. Not all cloud services are the same. Some cloud providers tend to offer limited versions and enable only the most popular features, so you may not get all the features or customization you want. Before you sign up, make sure you know what your cloud service provider is offering.
- It does not mean you have to finish servers. You may have a few services that you can handle which means less for your IT staff, but that doesn't mean you can let go of all your servers and staff. While it may seem too expensive to have data centers and cloud infrastructure, redundancy is key to backing up and recovering.
- No Redundancy. The cloud server is inactive and has not been backed up. Since technology may fail here and there, avoid burnout by purchasing a retrenchment plan. Although it is an additional expense, in most cases it will be worth it.
- Bandwidth issues. For it to work properly, clients must plan accordingly and not pack a large number of servers and storage devices into a small set of data centers.

F. Issues in Cloud

Public cloud infrastructure has been highlighted in many security issues thanks to Multi-tenancy, Vendor Lock-in, Data security management, service exchangeability and SLA management. As cloud providers offer free trial accounts to new users, there is a potential risk to existing customers for loss of infrastructure control or data security breaches [18].
Multi-Tenancy: The ability of the cloud to provide services to a wide range of users without contact. This is achieved through Virtual Machines (VM's) and hypervisors, which separate different users from each other. The hypervisor isolation itself is a security issue as it can be broken and attackers can use the back to gain access to other users. Placing competitors on the same machine can create competition for bandwidth and resources.
Stability: It is a feature of the cloud to increase / decrease resources controlled by a set of rules to meet the required demand. The biggest problem with this is that while it helps users to go up / down according to demand, it is a direct risk to the data used in the extracted resources. If a Cloud provider does not follow the appropriate compliance rules to clear the extracted resources before assigning it to another user, it creates a high security problem for sensitive first-time data.
Availability: It is a guarantee made by the cloud provider to maintain the integrity of the database and to keep it available at the user's request. There should be trust and agreements between the provider and the user for acceptable unavailability of resources and data security in the event of failure. There must be Service Level Agreements (SLA's) that clearly define the circumstances in the event of a failure and return of the data and an acceptable rest period. If appropriate methods or SLAs are not available between the user and the provider, it creates a data loss security issue.

Integrity and Privacy: If cloud computing is poorly designed, it may grant access to an unauthorized user to alter, delete or access sensitive data from another cloud user. Methods such as encryption and integrity checking need to be in place to verify the accuracy of the data. The provider should also have a data record held to recover in the event of a disaster or failure. Methods such as an encrypted SSH connection, an RSA certificate for an incoming SSH connection to ensure user access to resources should be available. Providers should use the ACID model (Atomicity, Consistency, Isolate and Durability) to ensure data security.
Accessibility Management: The cloud design should include various access methods such as MFA (Multi-Factor Authentication) for administrators who have the right to avoid accidental data damage or Federated Access with Trusted third-party to allow temporary access to resources. API access must be enabled to authenticate legitimate users as the integrity of cloud services is linked to their security.

G. Attacks on cloud infrastructure

Cloud providers need to have appropriate ways to reassure their cloud users by asking for their credit card details before providing free time services. There are two types of attacks: external attacks - when the attacker tries to penetrate the system and internal attacks - when the attacker tries to attack users within the network. Attackers can try to attack other users in the cloud from within the cloud infrastructure [19, 20].
Zombie Attack: In these types of attacks, the attacked machine is sent a request for resources from innocent users. The number of such applications is so high that the compromised machine becomes the victim of a Distributed Denial of Service (DDoS) attack that destroys all its resources.
Service Injection Attack: In this type of attack, the user can attack within the code of installing cloud infrastructure on some services that provide access to other user information.
The attack on Virtual Machine: The attacker can try to penetrate the VM to gain access to core infrastructure thus gaining access to various VMs' hosted by other users.
Man-in-Middle Attack: This method is used to listen to communication on the victim's machine, this is the result of incorrect encryption or Secure Sockets Layer (SSL) connection certificates. The attacker is trying to spend a secret day stealing identity and acquiring infrastructure.
Meta-data spoofing attacks: These types of attacks are performed to analyze the basic details of the application services. This helps the attacker to launch an attack on a particular service thus disabling the entire application.

H. Security at different layers in cloud.

Application Level Security issues: Most applications are web-based and use the SSL / Transport Layer Security (TLS) protocol to establish connection with a web browser. Attackers can attack web browser authentication to access cloud resources using eXtensible Markup Language (XML) tokens. The vulnerability of XML such as cheating access token without affecting XML encryption and signing has a high security risk. Strategies such as using CloudProtect (which stores user data in an encrypted way) middleware can help reduce the risks associated with explicit data exposure. Regular access to data for processing is stored in plain text, and all other data including access key is encrypted and stored. Definition of policy can help define who can access which data [21, 22].
Better service quality (QoS) should be available on demand as it affects performance during a DDoS attack. The State of Workflow should be protected because the attacker can use this data in the middle and thus risk the results.
Network Level Security issues: The network forms the backbone of the cloud system, a key component that helps integrate various cloud features. Attacks such as DDoS at Network level are hard to detect. Attacks such as DNS poisoning, Port scanning, ARP extraction, and IP fraud are common in network infrastructure. A security problem related to network access, authorization, authentication, penetration attacks, and seizures can all threaten cloud formation. Internal access (NIDS) systems can be used to reduce these attacks and to protect the network infrastructure from external and internal attacks.
Data Storage Level Security issues: Protecting data entry, data rest, data storage, data retrieval and forensic analysis in the cloud system is a major challenge. Data entry is affected by incorrect encryption methods and improper use of the protocol. While data breaks are affected by incorrect encryption process, incorrect storage policy, unchecked access right and failure to separate data from other users. The robustness of cloud computing helps to distribute and deliver resources on demand; data should be cleared and replaced by 0 when resources are released, this helps prevent data from being compromised. Data fixes are data that has been left out of excluded resources that may be compromised when they are assigned to other users. This also creates forensic investigation challenges as it is difficult to find a repository for data in the cloud system. Data acquisition is a very important challenge with the cloud as data response provisions must be available in the event of a disaster.
Virtualization Level Security issues: Virtualization and hypervisor allow cloud providers to integrate features to support multiple hits, durability and other storage support where needed. The only thing that separates the various users from each other is the hypervisor, which separates and prevents users from having full access to the underlying machine. Multi-tenancy has a high security problem as attackers can install Virtualization based malware and rootkit to break the hypervisor and gain access to other user's OS (Operating System). Sharing VM photos also poses a security risk of creating an attack on the outside of the attackers. If an attacker uses unlicensed or expired software, there is a high risk of non-compliance. The cloud provider needs to have strategies for analyzing the integrity of VM cloud performance and having a compliance agreement such as SLA will ensure that users do not touch other employers in the cloud.
Authentication and Access control level issues: Data is transferred from customers to the cloud via the Internet, this alone creates a high security problem as data needs to be verified and authenticated before it can be accessed in cloud

infrastructure. The language verification organization (SAML) protocol can be used to authenticate users and authenticate their basic authentication. XML-based Simple Object Access Protocol (SOAP) can deal with signature folding attacks that could jeopardize official user data.
A secure cloud partnership to authorize temporary users using reliable third-party authentication and encryption for authentication and authentication can improve the security of cloud infrastructure. Cryptographic-based cryptography (HIBC) can be used with integrated access, where both authorized organizations authorize encryption and provide single sign-in access. Identity providers must have a limited level of access provision and policies to allow only authorized users in that particular resource. Standards such as the eXtensible Access Control Markup Language (XACML) can be used to improve access policies. Using the Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) and active authorization systems can help manage cloud access [23].

III.METHODOLOGY

A. Solutions to mitigate security issues [24]:

Shared cloud infrastructure has many problems as discussed in the previous section which threaten security. It is the responsibility of the Customer and the cloud provider to manage security. The cloud provider is responsible for maintaining the integrity, accessibility, and severity of the cloud infrastructure, and it is the responsibility of the cloud user to use the security of their applications.
Compliance and SLA Agreements: It is a good practice for cloud providers to find and adhere to standards compliant with the Payment Card Industry Data Security Standard (PCI DSS) for payment and data security systems, the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) for control. and responding to sensitive information, the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) and the Federal Information Processing Standard (FIPS) are required by the US government, this will help increase security and trust between the provider and their customers.
SLA agreements must be in place for best practice, security measures, access to services, data protection and integrity. The user must be able to resolve security issues regarding infrastructure security by signing Non-Disclosure Agreements (NDAs) and SLAs so that the user is aware of any sub-contracts or issues between them that could pose significant security risks. SLAs to deal with availability and information for any available rest period may help the user to successfully protect his or her data without affecting his or her request.
Compliance with privacy means that data owners are responsible for the security of their data even when hosted by a cloud provider. It is also the responsibility of the owner to comply with various laws and regulations on where data is handled. Information may be held in any country or place to improve its availability, it is the responsibility of the user and the provider to comply with the site's compliance laws as European standards.
Providers must adhere to the Economic Cooperation and Development (OECD) security guidelines and Asia-Pacific Economic Cooperation's (APEC) Privacy Policy to protect the privacy of personal information in the Asia-Pacific region (APAC), while the European Economic Area adheres to standards such as HIPAA, SOX, PCI DSS, Occupational Safety and Health Administration (OSHA), etc., This ensures the best ways to protect data from any security issues raised [25].
Auditability: Providers need to have procedures that can help users identify the cause of the failure or analyze an attack attack. This can be done in accordance with compliance such as the Statement of Audit Standards (SAS) No. 70, which will help users to manage and investigate their infrastructure effectively and possibly conduct criminal investigations when needed. That can be achieved effectively by having the right SLAs in place.
Trust: This not only describes the trust the user shows in the provider that his or her data will be accessible and protected from disasters but also describes the trust that should be in the user who will not misuse the cloud infrastructure affecting other users. user and any Trusted third party using appropriate methods such as NDAs and SLAs to legally bind them and prevent them from any potential harm.
Access management: Applications stored in the cloud need to be protected by encrypting data transfers, establishing authentication mechanisms such as integrated access to temporary connectivity tokens and the MFA with access to the selected option for administrators so that one can download the entire application process. The SSL / TLS protocol should be used in conjunction with encrypted XML tokens using the STAMP bit to verify that someone has modified user data. Using this will ensure the most secure connection between the user's web browser and the cloud system.
Tools like XArp 2 should be used that can accurately detect ARP extinction attacks. Strategies like IDS across the region can help monitor and warn of any such attacks, eliminating one point of failure during a DDoS attack. Providers must have a solid firewall in place to protect cloud infrastructure from losing control of the system.
Access to Cloud Storage Data needs to be monitored and managed properly. Sensitive information such as login, personal information, and payment data should be kept encrypted and secure. Every user who needs access to data should need an encryption key that can be authorized by processes such as administrative services necessary to provide an additional layer of security. Steps must be taken to protect the Cloud Management Layer (CML) which is a microkernel that can expose and provide access to all rights at the regulator level which can create many security issues [26].
VM and Hypervisors should be updated regularly and upgraded as any security deficiencies in this will lead to attacks that control the entire cloud infrastructure, thereby leading to the closure of the service to other users. Employers in hypervisors should not be able to control the kernel of its machine, which can affect other employers on the same machine.
Access to APIs should only be granted to certain users when verifying the application, this eliminates the abuse of APIs by the attacker. Users should be informed of the various steps and steps taken by the cloud provider (Risk-Profiling) to identify the risks associated with the data and their use.

IV.FINDINGS

Cloud services are now an integral part of corporate life, bringing with them the opportunity to accelerate business with their fast-tracking capabilities, allowing us to accelerate our resources, and provide new opportunities for collaboration. The general organization uses, on average, 1,935 cloud services including business-ready services purchased by the IT department such as Office 365 to lesser-known and risky services such as Mega. As such, sensitive data inevitably makes its way to the cloud, with 21% of all cloud files containing some form of sensitive content, see Figure 1 [27].

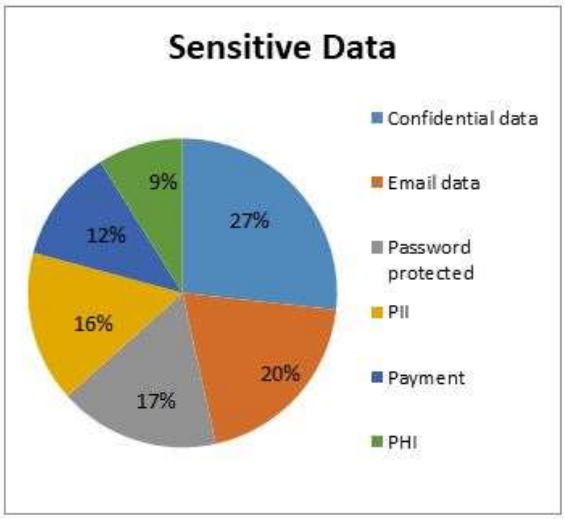

Figure: Pie chart of Sensitive data

Here are the most interesting findings from the reports.

A. 21% of files in the cloud contain sensitive data

The most common type of sensitive content found in the cloud is confidential data (e.g. financial records, business plans, source code, trading algorithms, etc.). Sensitive data uploaded to the cloud, by itself, is not a bad thing, but we have found that the data can be compromised if misused internally or distributed outside of the policy.

B. The sharing of sensitive information through open, public links has increased by 23% over the years.

One of the key features of the cloud is seamless integration and file sharing. We are increasingly seeing organizations sharing files / folders by creating links within the cloud service pointing to a file / folder. The problem with this method is that these types of shared links and their subfolders / folders can be accessed by anyone with the link. This means that when a link is shared, there is little way to stop the recipient of that link from transmitting it to others, thus greatly increasing the risk of data loss. In addition, it is surprisingly difficult for IT security teams to track how many publicly shared links are available and whether they have been shared by unauthorized groups. Compounding this problem is that 21% of the data in the cloud is sensitive, so it is very likely that a large percentage of those shared links are clearly pointing to files / folders that contain sensitive data [28]-[33].

C. The central organization has 2,200 cases of individual malpractice in the cloud

The rapid adoption of cloud services did not stop at SaaS services such as Office 365, Box, or Saleforce. Amazon Web Services (AWS) has been silent on switching server and data infrastructure to cloud-based services, categorized as Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS - consider wireless server use as AWS Lambda). Today, 65% of organizations worldwide use some form of IaaS, 52% of PaaS. However, the individual services that customers can use on IaaS platforms come with deep and often complex depth settings. Not surprisingly, we see that the average organization has 2,200 IaaS instances of inconsistent monthly. These include factors such as the lack of EBS encryption or incorrect configuration of EC2 group ports that may allow unrestricted access [34]-[39].

D. The central organization meets accounting threats that account for 12.2 cloud attacks per month

On average, organizations encounter 12.2 cases each month where an unauthorized third party uses stolen account credentials to gain access to company data stored in the cloud service. These incidents affect 80.3% organizations at least once a month. Additionally, 92% of companies have cloud information sold on the Black Web.

E. Cloud use has grown by 15% since last year, reaching an all-time high

The central organization now uses 1,935 cloud applications, an increase of 15% over the previous year. Divided by service type, business applications (e.g. Office 365, Saleforce, etc.) 70% of cloud services used by the central company, while cloud-based consumer applications (such as Facebook or Pinterest) represent another 30%.

V.DISCUSSION

The world today is becoming increasingly cloudy, and the effects of businesses and consumers alike are far reaching. The cloud not only provides new ways to access computer and data capacity quickly and inexpensively, but it can also boost new capabilities and put companies at a faster pace of using disruptive practices and technologies as they are developed and matured. DevOps, internet of things, artificial intelligence, edge computing, cryptocurrency - all of this depends on the mitigation, performance, and ubiquitous cloud. In many ways, the word cloud has come to mean more than just cloud technology, privately; rather, it redefined how technology is incorporated into everything we do and changes the way it is built and delivered.

If we discuss about the benefits, there are so many benefits of cloud computing. Some of them are,

A. Cost Savings

If you are worried about the price of prices that will come with making changes to the computer, you are not the only 20% of organizations concerned about the initial cost of using a cloud-based server. But those who are trying to measure the pros and cons of cloud use need to look at more than just the initial price they need to consider ROI.

Once in the cloud, easy access to your company's data will save you time and money at the start of projects. Also, for those who are worried that they will end up paying for features they do not need or do not want, many computer services are paid for as you go. This means that if you do not use what the cloud offers, at least you will not have to spend money on it.

The pay-as-you-go system also works in the database needed to serve your participants and customers, which means you'll get exactly the space you need, and you won't be charged for any space you don't offer. When combined, these factors lead to lower costs and higher returns. Half of all CIO leaders and IT leaders surveyed by Bitglass reported cost savings in 2015 due to the use of cloud-based systems.

B. Security

Many organizations have concerns about security when it comes to adopting cloud-computing solutions. After all, when files, programs, and other data can be kept secure on the site, how do you know if they are protected? If you can get far away from your data, then what is stopping cybercriminal from doing the same thing? Well, sure, actually.

First, the full-time job of cloud hosting is to carefully monitor security, which is much more efficient than the standard internal system, where an organization has to divide its efforts among thousands of IT concerns, security alone. And while many businesses are reluctant to publicly consider possible internal data theft, the fact is that a very high percentage of data theft comes from within and is perpetrated by employees. If so, it can be very safe to keep sensitive information inactive.

C. Flexibility

Your business has a limited amount of focus on differentiating between all of its operations. If your current IT solutions force you to pay more attention to computer and data storage issues, you will not be able to focus on achieving business and customer goals. On the other hand, by relying on an outside organization to take care of all the infrastructure and infrastructure, you will have more time to contribute to the aspects of your business that directly affect your content.

D. Mobility

Cloud computing allows mobile access to company information via Smartphones and devices, which, given the more than 2.6 billion smartphones used worldwide today, is a great way to ensure that no one is left out. Employees with busy plans, or who live far away from the corporate office, can use this feature to keep up to date with customers and co-workers.

With the cloud, you can provide easily accessible information to mobile sales employees, freelancers, or remote employees, to find a better working life balance. Therefore, it is not surprising to see that employee satisfaction organizations listed as the most important ones can achieve 24% chance of increasing cloud use.

E. Increased Collaboration

If your business has two or more employees, then you should be making collaboration a priority. After all, there is no point in having a team if it can work as a team. Cloud computing makes collaboration easier. Team members can view and share information easily and securely on a cloud-based platform. Some cloud-based services even offer shared community space to connect employees across your organization, thus increasing interest and engagement. Interaction is possible without a cloud-computing solution, but it will not be easy, or effective.

F. Quality Control

There are a few risk factors for business success such as poor quality and inconsistent reporting. In a cloud-based system, all documents are stored in one place and in one format. Since everyone gets the same information, you can keep data consistent, avoid human error, and have a clear history of any updates or updates. On the other hand, handling data on silos can lead to employees risking saving various types of documents, leading to confusion with refined data.

G. Sustainability

Given the current state of the environment, it is no longer enough for organizations to put up a recycling bin and claim to be doing their part to help the planet. Real sustainability requires solutions that deal with disruption at all levels of the business. Cloud hosting is very environmentally friendly and leads to low carbon emissions.

Cloud infrastructure supports environmental performance, enabling tangible services rather than virtual products and hardware, reducing paper waste, improving energy efficiency, and (if provided that allows employees access to any internet connection) to reduce passenger-related emissions. The Pike Research report predicted that data center power consumption would decrease by 31% from 2010 to 2020 based on the adoption of cloud computing and other visual data options.

H. Loss Prevention

If your organization is not investing in a cloud-computing solution, then all your important data is seamlessly integrated with the office computers they live in. This may not seem like a problem, but the fact is that if your local hardware encounters a problem, you may permanently discard your data. This is a much more common problem than you can see that computers can work well for a number of reasons, from viral infections, to age-related hardware corruption, to a simple user error. Or, despite good intentions, they can be misplaced or stolen (more than 10,000 laptops are reported missing every week at major airports).

If you are not in the cloud, you are in danger of losing all the information you have stored locally. With a cloud-based server, however, all the information you upload to the cloud remains secure and easily accessible from any computer with an Internet connection, even if your regular computer doesn't work.

I. Automatic Software Updates

For those who have a lot to do, there is nothing more annoying than having to wait for system updates to install. Cloud-based applications have updated themselves and updated themselves, instead of forcing the IT department to do the organisation's manual review. This saves valuable time and IT staff and the money spent on consulting with outsiders of IT. PCWorld calculates that 50% of indicated cloud users need internal IT resources as a cloud benefit.

J. Competitive Edge

While cloud computing is growing in popularity, there are still those who choose to keep everything in place. That is their choice, but doing so puts them at a different risk when competing with those who have the benefit of the cloud in their hands. If you use a cloud-based solution ahead of your competitors, you will be moving forward with the learning curve by the time they arrive. A recent Verizon study showed that 77% of businesses feel that cloud technology gives them a competitive advantage, while 16% believe the profit is significant.

VI. CONCLUSION

Cloud Computing brings many benefits to its users such as reduced costs, easy shipping, scale as you want, etc. I have explored how various aspects of the cloud deal with security issues and how attackers can be exploited to gain control of the system or cripple it. Solutions to address security concerns remain a challenge, and the dynamics of the cloud make it difficult to implement the same. Separation and encryption for cloud user data prevents data leaks and privacy. We still need strong authenticity and access to communications that will protect you from any hijacking or spoof data on the go or at rest. Strong encryption algorithms should be used to protect privacy and other user data. Compliance standards help increase the security of any cloud infrastructure and help take precautionary measures. New compliance standards will change and adhering to them will definitely improve security. Providers and users should have clear SLAs that explain each other's concerns and make it clear that they are not harmful to each other.

REFERENCES

1. Modi, C., et al., "A Survey on Security issues and solutions at different layers of cloud computing." J.Supercomput. 63(2), 561-592, February 2013.
2. Tanase, Matthew “2003). "IP Spoofing: An Introduction” The Security Blog. Retrieved February 10, 2012.
3. Rohit Bhadauria, Rituparna Chaki “A Survey on Security Issues in Cloud Computing” international journal of computer applications Volume 47 - Number 18.2012
4. Ruiping Lua and Kin Choong Yow, “Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network,” IEEE Network, vol. 25, no. 4, 2011.
5. Klaus Pl¨ossl, Hannes Federrath, and Thomas Nowey “Protection Mechanisms against Phishing Attacks” http://www-sec.uni-regensburg.de/publ/2005/ PlFN2005Trust Bus05Phishing.pdf
6. “Security Guidance For Critical Areas Of Focus In Cloud Computing V3.0”, https://cloudsecurityalliance.org/research/security-guidance/
7. Y. Chen, V. Paxson, and R. Katz, "What’s New About Cloud Computing Security?," 2010
8. Hadoop: What it is, how it works, and what it can do, http:// strata.oreilly.com/2011/01/what-is-hadoop.html, Retrieved October 23, 2013.
9. J Van Hoboken, A Arnbak and N Van Eijk, Obscured by Clouds or How to Address Government Access to Cloud Data from Abroad, http:// ssrn.com/abstract=2276103, Retrieved October 23,2013
10. Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki” A Survey on Security Issues in Cloud Computing” http://arxiv.org/ftp/arxiv/papers/1109/1109.5388.pdf
11. Center Of Protection Of National Infrastructure Information Security Briefing cloud-computingbriefing.pdf.
12. Brian Hayes. Number 7 (2008).cloud computing.portal the acm digital library. Volume 51, Pages 9-11
13. Velte, Toby; Velte, Anthony; Elsenpeter, Robert C. Cloud Computing, A Practical A pproach. http://cdn3.j2ski.com/k0ac/15-prof-verdie-schowalter/5SucP48xvm1O-cloud-computing-a-practical-approach.pdf
14. Nick Antonopoulos,Lee Gillam.(2017). Cloud Computing.springer link.

15. Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao.(2008). Cloud Computing: A Perspective Study, Rochester Institute of Technology.
16. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. Number 4 (2010).A view of the cloud computing.portal the acm digital library. Volume 53, Pages 50-58
17. Eric knorr,Galen Gruman.April (2008).What cloud computingreally means.
18. P.Y. Thomas . 12 April (2011). Cloud computing: A potential paradigm for practising the scholarship of teaching and learning. The Electronic Library.
19. Chunye Gong; Jie Liu; Qiang Zhang; Haitao Chen; Zhenghu Gong.(2010). The Characteristics of Cloud Computing. IEEE.
20. Sean Marston,Zhi Li,Subhajyoti Bandyopandhyay,Juheng Zhang,Anand Ghalsasi. April 2011. Cloud computing — The business perspective.Science Direct.
21. Borko Furht,Armando Escalante.(2010). Handbook of Cloud Computing. Springer.
22. Tharam Dillon; Chen Wu; Elizabeth Chang.(2010). Cloud Computing: Issues and Challenges. IEEE.
23. Ling Qian,Zhiguo Luo,Yujian Du,Leitao Guo.(2009). Cloud Computing: An Overview.Springer Link.
24. Won Kim, January-February (2009). Cloud Computing: Today and Tomorrow. JOURNAL OF OBJECT TECHNOLOGY. Sungkyunkwan University, Suwon, S. Korea
25. Shivaji P. Mirashe, N. V. Kalyankar.(2010). Cloud Computing.arxiv.org.
26. Yashpalsinh Jadeja; Kirit Modi.2012. Cloud computing - concepts, architecture and challenges. IEEE.
27. CHEN Quan,DENG Qian-ni.(2009). Cloud computing and its key techniques.cnki.com
28. Alexa Huth and James Cebula.(N/A). The Basics of Cloud Computing.US-CERT. Sean Carlin, Kevin Curran.(2013). Cloud Computing Security.IGI Global.
29. Matthew N.O. Sadiku; Sarhan M. Musa; Omonowo D. Momoh.(N/A). Cloud Computing: Opportunities and Challenges. IEEE.
30. Partono Prasetio, A., Duc Tai, T., Jade Catalan Opulencia, M., Abbas, M., A. Baker El-Ebiary, Y., Fadhil Abbas, S., Bykanova, O., Samal, A., & Iswanto, A. (2022). Impact of the COVID-19 pandemic on religious tourism amongst Muslims in Iraq. HTS Teologiese Studies / Theological Studies, 78(4), 6 pages. doi:https://doi.org/10.4102/hts.v78i4.7565
31. Yousef A.Baker El-Ebiary, Samer Bamansoor, Waheeb Abu-Ulbeh, Wan Mohd Amir, Syarilla Iryani A. Saany, M. Hafiz Yusoff. “Using Interval Manager Mobile Application in Saving Time and Cost” Vol. 68, Editor’s Issues, Oct. 2020, pp. 82-85, IJETT, Doi: 10.14445/22315381/CATI1P214. Scopus, ISSN: 2231-5381
32. Yousef A.Baker El-Ebiary, Samer Bamansoor, Waheeb Abu-Ulbeh, Wan Mohd Amir, Syarilla Iryani A. Saany, M. Hafiz Yusoff. “A Prognosis of Chinese E-Governance” Vol. 68, Editor’s Issues, Oct. 2020, pp. 86-89, IJETT, doi: 10.14445/22315381/CATI1P215. Scopus, ISSN: 2231-5381
33. Yousef A.Baker El-Ebiary, Waheeb Abu-Ulbeh, Najeeb Abbas Al-Sammarraie, M. Hafiz Yusoff , W. M. Amir Fazamin W. Hamzah, Syarilla Iryani A. Saany. “The Role of ICT in Special Educational Needs – A Case Study of Malaysia” Vol. 68, Editor’s Issues, Oct. 2020, pp. 90-93, IJETT, doi: 10.14445/22315381/CATI1P216. Scopus, ISSN: 2231-5381
34. W. M. Amir Fazamin W. Hamzah, Waheeb Abu-Ulbeh, Najeeb Abbas Al-Sammarraie, Yousef A.Baker El-Ebiary, M. Hafiz Yusoff, Syarilla Iryani A. Saany, Azliza Yacob. “The Integration of Learning Management Systems with PLE – a Review Paper” Vol. 68, Editor’s Issues, Oct. 2020, pp. 94-96, IJETT, doi: 10.14445/22315381/CATI1P217. Scopus, ISSN: 2231-5381
35. Syarilla Iryani A. Saany, Waheeb Abu-Ulbeh, Najeeb Abbas Al-Sammarraie, Yousef A.Baker El-Ebiary, M. Hafiz Yusoff, W. M. Amir Fazamin W. Hamzah, Yanty Faradillah. “A New E-Learning Technique Using Mobility Environment” Vol. 68, Editor’s Issues, Oct. 2020, pp. 97-100, IJETT, doi: 10.14445/22315381/CATI1P218. Scopus, ISSN: 2231-5381
36. Aledinat Lowai Saleh, Syed Abdullah Fadzli, Yousef El-Ebiary. “Arabic Language Documents’ Similarity and its Challenges (A Review)” Vol. 68, Editor’s Issues, Oct. 2020, pp. 88-96, IJETT, doi: 10.14445/22315381/CATI2P214. Scopus, ISSN: 2231-5381
37. Belal Alifan, Mokhairi Makhtar, Yousef El-Ebiary. “Propose Model for Consumers’ Perceptions and Acceptance of e-Health Systems and Services in Jordan” Vol. 68, Editor’s Issues, Oct. 2020, pp. 1-10, IJETT, doi: 10.14445/22315381/CATI3P201. Scopus, ISSN: 2231-5381
38. Hazem M Bani Abdoh, Syarilla Iryani A. Saany, Hamid H. Jebur, Yousef El-Ebiary. “The Effect of PESTLE Factors on E-Government Adoption in Jordan: A Conceptual Model” Vol. 68, Editor’s Issues, Oct. 2020, pp. 19-23, IJETT, doi: 10.14445/22315381/CATI3P203. Scopus, ISSN: 2231-5381
39. Y. A. B. El-Ebiary, N. A. Al-Sammarraie, Y. Al Moaiad and M. M. S. Alzubi, "The impact of Management Information System in educational organizations processes," 2016 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), 2016, pp. 166-169, doi: 10.1109/IC3e.2016.8009060.