Security Issues in Cloud Computing: A holistic view

SUBODH KUMAR
B. Tech, M. Tech (Computer Science & Engineering)
research.subodh@gmail.com

VIJAY ANANT ATHAVALE
Professor & Dean (Engineering),
Panipat Institute of Engineering and Technology,
Haryana, INDIA
vijay.athavale@gmail.com
(Corresponding Author)

DIVYE KARTIKEY
B. Tech (Electrical and Electronics)
divyekartikey21591@gmail.com

Abstract- In recent years, cloud computing has developed into one of the fastest growing areas in the IT industry and a key driver for achieving an organization's mission. Some examples of cloud computing are: Google apps, data centre services, infrastructure, software, virtualization and platform-as-a-service. Microsoft, HPE, IBM, Amazon Web Services, Google, SalesForce, NetSuite, and VMware are some of the leading cloud computing companies. Despite the numerous benefits of cloud computing, it presents many unique security issues and challenges due to which companies are concerned about the security of their data once it leaves the firewall. Nowadays, security is a top concern for IT professionals worldwide and want to ensure their cloud data to be prevented from being leaked, stolen or deleted.

This article seeks to present a comprehensive picture of cloud computing security, as well as identify and analyse the most vulnerable security concerns and cloud computing threats, so that end users and service providers are aware of the important security concerns and threats associated with cloud computing.

Keywords- Cloud Computing, Security issues, Data breach, Personal information, Cyber attack

1. Introduction

Cloud computing is the on demand availability of technology enabled services to the people and organisations by allowing convenient network access to a shared pool of configurable computing resources like: storage, networks, servers, applications, and services over the internet, from anywhere, at any time, from data centres around the world. Some examples of cloud services are Microsoft, HPE, IBM, Amazon Web Services, Google, SalesForce, NetSuite and VMware.

The overcapacity of today's huge corporate data centres, the accessibility of broadband and wireless networking, the dropping cost of storage, and continuous advancements in networking technology are all driving forces behind the rise of cloud computing.

Cloud computing is growing rapidly as a means of renting computing and storage infrastructure services (known as IaaS or Infrastructure as a Service), building and personalising remote platforms for business processes (known as PaaS or Platform as a Service), and renting entire business applications (known as SaaS or Software as a Service). The cloud infrastructure is further classified as Public, Private and Hybrid Cloud.

Latest numbers show that the cloud is providing organizations with a 21% reduction in product time to market, a 17% reduction in IT maintenance costs, a 15% reduction in IT spend, and an 18% increase in employee productivity. With these types of metrics in hand it's no surprise that 60% of CIOs state that the cloud has become their 1st priority [1].

According to a recent research by the Cloud Security Alliance (CSA), the development in cloud computing has introduced many security concerns, and the security of data in the cloud is now a broad-level issue for 61 percent of enterprises. 77 percent of respondents of a survey conducted in 2018 have stated that the cloud computing security risk has become a major concern.

Although most business owners believe that the cloud environment is more secure than an on-premise infrastructure, there are still a number of concerns which need to be addressed [2]. A survey of IT executives revealed that some of the top security issues that hold back cloud adoption at their companies include data breach, data loss, insider threats, DoS (Denial of Service), cryptojacking, account hijacking, insecure APIs, disaster recovery and business continuity. In terms of cloud security, password monitoring is crucial. Your cloud account gets less secure the more people that have access to it. The information saved in the cloud will be accessible to anyone who knows your password. As per a research by Skyhigh, an enterprise experiences around twenty three cloud-related threats every month [3].

Two commonly used categories for classifying cloud computing are:

1. Service boundary
2. Service type

From the perspective of *service boundary*, cloud computing can be categorized as:

i. Public Cloud
ii. Private Cloud and
iii. Hybrid Cloud

The service provided to external parties when the infrastructure is completely outside the customer or company's firewall is called the *Public Cloud*.

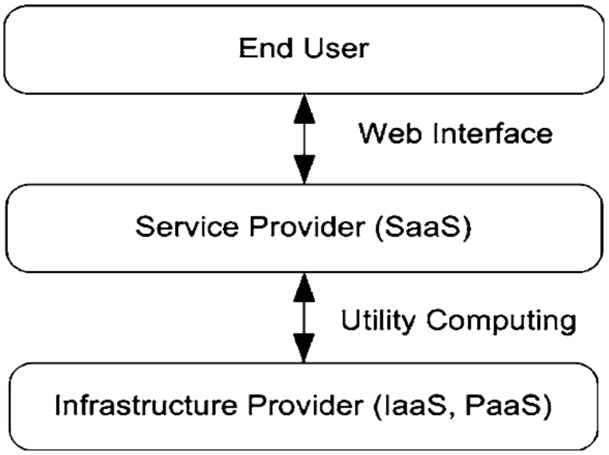
When IT services are placed on top of large scale consolidated and virtualized infrastructure within an enterprise firewall and used on the basis of ‘per transaction’ which the corporations create and operate, it is called *Private Cloud*.

When the resources are shared between a public and private cloud by a secured network, it is called *Hybrid Cloud*. Examples of hybrid cloud include Amazon's VPC (Virtual Private Cloud) services and Google.

From the perspective of *service type*, cloud computing can be categorized as:

i. IaaS (Infrastructure as a Service)
ii. PaaS (Platform as a Service)
iii. SaaS (Software as a Service)

SaaS caters to end users, whereas IaaS and PaaS cater to Independent Software Vendors (ISVs) and developers leaving a margin for third-party application developers.



Business model of Cloud Computing [4]

2. Security Objectives

- ✓ To ensure that information is always available.
- ✓ To maintain the *integrity* of information and services.
- ✓ To protect the *privacy* of information stored on participating systems.
- ✓ To verify the *authenticity* of communicating partners.
- ✓ To provide control over *access* to services or their components in order to ensure authorised service use.
- ✓ To ensure that origin and delivery of data is not *repudiated*.
- ✓ To ensure that there will be *no data leakage* after separation of data and processes on the virtual level of cloud between various applications.
- ✓ To maintain the same *level of security* during addition or removal of resources on a physical level.

3. Research challenges

Despite the fact that cloud computing has been publicly accepted by the industries, many current concerns remain unresolved, and new challenges continue to emerge from industry applications. Some challenging research concerns in cloud computing include:

- Data security
- Server consolidation
- Software frameworks
- Storage technologies
- Data management
- Traffic management and analysis
- Virtual machine migration
- Automated service provisioning
- Energy management

4. Dimensions of cloud security

Following are some of the cloud security concerns and implications:

4.1 Cloud platform, infrastructure and hosted code

This includes risks in networking, storage, and the possibility of virtualization.

1) Data location: While using the cloud, users likely have no idea where their data is stored. In fact, they might not even know in which country their data will be stored.

2) Data segregation: Cloud data is typically stored in a shared environment. Hence, encryption errors can render the cloud data completely useless, and even standard encryption can make data availability more difficult.

3) Investigative support: Data and logging for customers may be co-located and scattered across the hosts and data centres which are constantly changing. In such a situation, cloud services are extremely difficult to analyse.

4.2 Data

Cloud data services are vulnerable to a variety of security threats which may be 1. traditional security threats like illegal invasion, network eavesdropping & denial of service attacks; 2. specific cloud computing threats like data lock-in, data integrity, provenance, data remnant & data confidentiality and 3. user privacy threats like side channel attacks, virtualization vulnerabilities & cloud service abuse.

4.2.1. Integrity: Data integrity involves ensuring and maintaining data accuracy and completeness which means data should not be tampered with, inappropriately edited, destroyed, or maliciously fabricated in any way.

Concern: What happens to my cloud data? [5]

Data, in today's competitive economy, is the most valuable asset that businesses and individuals have. The foremost concern in cloud computing is about data integrity, data confidentiality and provenance. Concerns regarding the security of data hosted on public cloud server architecture are increasing. If the cached data isn't properly secured and removed on a regular basis, it might become like a gold mine for data thieves.

Providers such as Google, Yahoo, and AOL are required to save search data for eighteen months before removing individual client information such as cookies and IP addresses for any internal purposes. However, there have been incidents where even anonymized data has been compromised. The well-known example is when the Massachusetts Group Insurance Commission's anonymised health information was analysed to expose the medical history of the state's governor. This instance demonstrated that adding harmless and neutral data into anonymised data can disclose information that is sensitive.

Few other concerns are related to data lock-in and data location. For instance, 45 out of every 100 users of Linkup's online storage service were affected when their password-protected data got lost with a third-party storage provider, Nirvanix [6].

The main concerns of customers related to data integrity are as follows:

a) What ensures data integrity in the cloud and protects data loss?
b) Will my information related to business be kept private? How can I ensure that my personal information is kept private?
c) If the service provider is likely to fail, how can I avoid having my data locked out?
d) How can I be confident that data isn't left behind in storage (that is, when a delete

operation is performed, each and every bit is truly wiped out)?

e) How can I be sure that changes to my data are correctly tracked and each time a request is made, I receive the right copy?

f) When many cloud parties are engaged in the processing, how can data confidentiality and integrity be maintained?

4.2.2. Privacy and security: Customers have concerns about their privacy and data security.

Concern regarding the data security:

Is the physical and software infrastructure of my cloud-services providers secure?

According to a recent Novell survey, 87 percent of enterprises respondents see hybrid clouds as a future data centre evolution, and 92 percent believe that internal IT will be migrated to the public cloud at some point. On the other hand, security concerns were raised by nine out of ten respondents [7].

Concerns with migrating to the cloud and hosting apps in a remote multi tenant environment include:

a. Are the cloud data centres physically secure from cyber-attacks?
b. How is my application protected against harmful attacks in a shared virtualized infrastructure (VMs, storage, and network)?
c. How does my application, which is hosted using a common software stack (PaaS and SaaS) be affected by potential common stack vulnerability?
d. How do I ensure security isolation when my internal applications can communicate with cloud based shared workflow in a hybrid cloud environment?
e. Should I rely on cloud service providers' APIs and interfaces?
f. How can it be ensured that no fraudulent activities occur now when I have released execution control?

4.2.3. Third party data control*:* The storage infrastructure and, as a result, data ownership are both with the cloud service provider. As a result, the client may demand verifiable verification even if the cloud provider guarantees data integrity and confidentiality.

4.3 Access

This includes user identity management, encrypted data exchange, and cloud access (authentication, authorization, and access control or AAA).

1) *Privileged user access:* Sensitive data processed outside the company carries an inherent level of risk as outsourced services bypass the physical, logical, and personnel controls.

2) *Long-term viability:* Availability and surety of getting the data back in case the cloud computing provider will become bought out and absorbed by a big company.

3) *Confidentiality:* As the outsourced data is stored in the cloud and out of the owner's direct control, data confidentiality is the property that the contents are not made available or disclosed to unauthorised users.

4) *Access controllability:* It refers to a data owner's ability to selectively restrict access to data that has been outsourced to the cloud. Legal users can be granted access to the data by the owner, and various users should have varied access privileges for distinct data components. As a result, in untrusted cloud environments, access permission must be handled alone by the owner.

5) *Multi party processing (Trust):* In this scenario, one party may use some of the data provided by the other. Therefore, it becomes essential for participating cloud computing parties to protect the privacy of their own data in the absence of effective encryption.

Concern: Are cloud services which users are using truly mine, and will all of my legitimate users be able to access them in a seamless and secure manner? [op. cit.]

User authorization, authentication and access control (AAA) is another major concern for cloud security.

The first concern is access management, which entails transferring standard company directory structures such as LDAP and Active Directory to a cloud PaaS or SaaS provider in order to give organisational role-based access.

The second concern is identity management, which includes authentication, identity theft and phishing.

The main concerns of customers are as follows:

a. How can I ensure that an employee who has left the company does not gain unauthorised access to my cloud?

b. How can proper levels of cloud service authentication be ensured? What's the best way to manage multi-device access?

c. In a multi cloud scenario, how do I ensure that I provide access to users to different security domains so that the workflow which happens end to end is seamless? Similarly, in a hybrid cloud, how do I create identity structure and ensure a minimum common access control?

4.4 Compliance

Regulatory authorities are paying attention to cloud because of its magnitude and disruptive impact, particularly in regards to security audits, data location, operation traceability and compliance problems.

1) *Recovery:* A cloud service provider should inform the clients regarding 'what will happen to their data and service in the case of a disaster', even if clients don't know where it is stored.

2) *Service continuity (Availability):* It refers to issues like internet outages, power outages, service disruptions, and system bugs that could jeopardise cloud computing's viability.

The following are some common examples of such issues [8]:

2a) In November 2007, RackSpace, Amazon's competitor, stopped its service for 3 hours because of power cut-off at its data center;

2b) In June 2008, Google App Engine service broke off for 6 hours due to some bugs of storage system;

2c) In March 2009, Microsoft Azure experienced 22 hours out of service caused by an OS system update.

Currently, a public cloud service provider that uses virtualization, defines service reliability as 99.9 percent in service level agreement (SLA) [op. cit.].

3) *Service migration:* Cloud migration services refer to the process of migrating a business to the cloud and the solutions that are used to do it. Cloud service providers (such as Azure, AWS, and Google) all provide tools and services to assist in workload and application migration.

4) *Abstraction:* An abstract set of service end points is provided by the cloud. If a user does not know which physical computer, MAC address, storage partition, network port, switches and other components that are truly involved, it becomes very difficult to isolate a specific physical resource that has been compromised or is under threat in the event of a security incident.

5) *Lack of execution controls:* The remote execution environment is not under the control of the external cloud user. As a result, key issues such as memory management, input-output calls, external shared utilities accessibility and data are hidden from the user's view.

5. The worst hacks, cyber attacks, and data breaches since year 2018

Year 2021 (till May)

1. *Air India*: (February, 2021) A cyber attack on the Air India passenger service system breached the data of around 4.5 million people [9].

2. *Dominos*: (May, 2021) A cyber attack on domino's database compromised the data of millions of customers who have ordered food online [10].

Year 2020

1. *Zoom (April, 2020):* At the peak of COVID-19 pandemic, when many users were using Zoom for official works, a data breach compromised the data of 5,00,000 users and their credentials were put on the dark web [11].

2. *Microsoft – 250 million records*: According to Microsoft, the data breach took place in january. A change made to the database's network security group, containing misconfigured security rules, was responsible for the incident [12]. The servers [13], had around 250 million records, with personal information such as email id, IP addresses, and many more.

3. *Wattpad – 268 million records:* The data breach exposed around 268 million records. The stolen data was then put on various hacking related forums as per BleepingComputer [14]. Personal details which got exposed were usernames, email id, IP addresses and bcrypt hashed passwords.

4. *Broadvoice – 350 million records:*Bob Diachenko, a cyber security expert, found [15] an exposed cluster of databases belonging to the Voice over IP (VoIP) telecommunications vendor Broadvoice which contained 350 million records.

5. *Estée Lauder – 440 million records:* Jeremiah Fowler, a cyber security expert, detected [16] a database online that contained what he says was "a massive amount of records." The database belonged to cosmetics giant Estée Lauder and contained a total of 44,033,6,852 records.

6. *Sina Weibo – 538 million records:* A hacker [17] hacked Weibo and stole a database including the personal information of 538 million users and the data was put on sale on the dark web.

7. *Whisper – 900 million records:* An unprotected database, containing 900 million Whisper posts, and all the metadata related to those posts, was found online earlier in March. According to The Washington Post [18], the database was discovered by independent researchers and consultants Matthew Porter and Dan Ehrlich, who said they were able to access almost 900 million user records from the app's release in 2012 to the present day.

8. *BlueKai – billions of records:* Anurag Sen, a cyber security expert, found an unsecured BlueKai database accessible on the open Internet. There were billions of records in the database, including names, home addresses, email addresses, and web browsing activities such as purchases and newsletter unsubscribes. According to Cyware [19], BlueKai tracks 1.2% of all web traffic and tracks some of the world's biggest websites: Amazon, ESPN, Forbes, Glassdoor, Healthline, MSN.com, Levi's, Rotten Tomatoes, and The New York Times. Given the volume of data on this unsecured server, this was one of the largest cybersecurity breaches of 2020.

9. *Keepnet Labs – 5 billion records:* In March 2020, Bob Diachenko reported [20] coming across a leaky Elasticsearch database which appeared to be managed by a U.K.-based security company, according to SSL certificate and reverse DNS records.

10. *Advanced Info Service (AIS) – 8.3 billion records:*Justin Paine, a security researcher, discovered [21] an open ElasticSearch database when browsing BinaryEdge and Shodan on May 7.

11. *CAM4 – 10.88 billion records:* Anurag Sen, at Safety Detectives, discovered [22] a data breach in an adult live-streaming website CAM4.com. According to the research team, the database was more than 7 terabytes with traces from the production environment dating from March 16, 2020 and increasing daily, containing 10.88 billion records.

12. *Facebook's data breach* – 267 million records [23]

13. *Instagram, TikTok, and YouTube breach* – 235 million records [24]

14. *Cit0Day* – 226 million records [25]

15. *Unprotected Google Cloud Server breach* – 201 million records [26]

16. *MGM* – 142 million records [27]

Year 2019

1. *Quest Diagnostics - 11.9 million records hacked:* In early June, lab-testing company Quest Diagnostics

announced [28] a data breach exposed the personal information of approximately 11.9 million users which included credit card details, medical information and Social Security numbers.

2. *Houzz - 48.9 million records hacked:* Home design website Houzz [29] informed its customers that hackers had accessed usernames and encrypted passwords, as well as publicly visible profile information. The company's breach FAQ was ambiguous, but according to ITRC, 48,881,308 accounts were affected. Houzz stated no financial information was taken and that the intrusion was discovered in December 2018.

3. *Capital One - 100 million records hacked:* Capital One, in july, announced that a hacker stole the information of over 100 million Americans and 6 million Canadians [30]. The data accessed during breach included sensitive data, like Social Security numbers.

4. *Dubsmash - 161.5 million records hacked:* InFebruary, Dubsmash announced [31] that hackers accessed 162 million users' names, email and hashed passwords. The stolen data was then put on sale on the dark web.
5. *Zynga - 218 million records hacked:* Zynga announced in October [32] that Customers who played the "Draw Something" and "Words with Friends" games had their account log-in information obtained by a hacker on Sept. 12. The hacker gained access to the log-in details, usernames, email and Zynga account IDs of around 218 million consumers who downloaded the games on iOS and Android before September 2, 2019.

Year 2018

1. *UK government website cryptojacking* in February 2018, due to which countless website visitors became victims of cryptojacking. It is a crime in which personal electronic devices are used without user consent for cryptocurrency mining. Over 4,000 websites, including UK government, US, and Australian services, all experienced the same security issue at once due to a vulnerable third-party plugin used for website accessibility [33].

2. *Ticketmaster* during the months February to June 2018, due to which up to 40,000 customers were affected. The hack exposed personal information such as names, addresses, email addresses, phone numbers, payment information, and Ticketmaster login credentials. The intrusion of third-party code on Ticketmaster's web domain resulted in the installation of credit card skimming malware on the site. The cyberattack was later linked to the Magecart effort, according to researchers.

3. *Under Armour* (March, 2018), a seller of fitness related equipment and accessories, revealed data of 150 million accounts was hacked. Usernames, email addresses, and hashed passwords were stolen.

4. *Aadhaar (*March, 2018) database contained the information of at least 1.1 billion Indian citizens. A data leak caused by a state-owned utility company allowed anyone to download information belonging to all Aadhaar holders, including their private data and financial details.

5. *Facebook and Cambridge Analytica* (March, 2018) was one of the largest this year with severe consequences that are still being felt by the companies and regulators alike. In total, information belonging to up to 87 million users was improperly shared by a developer with Cambridge Analytica for the purpose of voter profiling.

6. *British Airways* (April – July, 2018) Data belonging to hundreds of thousands of customers was leaked who used a credit card to make reward bookings between April and July.

7. *Rail Europe* (May, 2018), a company which sells tickets for trips around the bloc, suffered a three-month-long data breach caused by credit-card skimming malware. Credit card numbers, expiration dates, and CVV card verification codes were all stolen during the covert campaign.

8. *TeenSafe* (May, 2018), a mobile app which touts itself as a "secure" monitoring app for iOS and Android aimed at parents, was responsible for two servers which were publicly exposed, leaking parental email addresses, child Apple IDs, device names, and device identifiers.

9. *Dixons Carphone* (June, 2018) uncovered a data breach of 10 million users where personal and payment card information was compromised.

10. *Ticketfly* (June, 2018) had to pull its website offline on the news that there had been a cyberattack. The company said that information had been leaked which belonged to roughly 27 million customer accounts and included names, email addresses, physical addresses, and phone numbers. A hacker suspected of being responsible sought to extort a single Bitcoin from Ticketfly in order to prevent the data from spreading.

11. *MyHeritage* (June, 2018) revealed the discovery of a file containing 92.2 million account records, including email addresses and scrambled passwords which were made public and published online.

12. *Exactis* (June, 2018), a marketing and data aggregation company, but the firm's name became somewhat well-known following a data breach which exposed 340 million records on a publicly accessible server. Nearly two terabytes of data, including a variety of data about US persons and businesses, were available in the public domain.

13. *SingHealth* (July, 2018): Around 1.5 million healthcare patient records, including one belonging to Prime Minister Lee Hsien Loong, were stolen. Patient names, national identity numbers, addresses, genders, and dates of birth were among the information stolen.

14. *Hackers go old school* (July, 2018): In Yale University, a data breach impacted 119,000 members of Yale. Personal details like names, Social Security numbers, addresses, and dates of birth got exposed.

15. *Timehop* (July, 2018), A social media platform that collects photos from other social media platforms like facebook, and posts them as the past. It revealed a security breach which exposed information in a database of 21 million users. All the personal information was compromised.

16. *Polar Flow* (July, 2018) : A technical flaw in the fitness application permitted anyone to improperly query a developer API which then could be used to track military personnel who made use of the app.

17. *Student medical records* (2018): A data breach affected students of Melbourne high school, in which their confidential medical and other personal records were compromised.

18. *Air Canada* (August, 2018): In a data breach, data of 20,000 customers were exposed. Passport numbers and other personal information was leaked.

19. *T-Mobile* (August, 2018): An unauthorized entry was detected into the network, and the data of three percent of its customers were hacked. Personal information like names, billing ZIP codes, phone numbers, email and account numbers were exposed.

20. *Facebook's network breach* (September, 2018): A loophole in Facebook's code allowed attackers to access the personal information of 30 million users, like names, phone numbers, cities, places of work, and many more were stolen from users.

21. *ISP, web traffic hijacks* (October – November, 2018): Multiple ISP and Internet infrastructure attacks emerged at various places in the world during this time. Cambodian ISPs were impacted by Distributed Denial-of-Service (DDoS) attacks, Google traffic was attacked by an ISP in Nigeria, and Telegram traffic was attacked in Iran.

22. *Canada Post* (November, 2018): A data breach leaked the information of 4,500 users which included names, postcodes, details of delivery like reference numbers and Canada Post tracking numbers.

23. *Amazon* (November, 2018): A "technical error" on the Amazon platform exposed the names and email addresses of some customers. However, there is a lack of concrete information available on the security breach by the company.

24. *Google+* (December, 2018): A bug in the Google+ API permitted attackers to steal data of close to 52.5 million users.

Table 1

User specific security requirements & vulnerable threats on different level of abstraction [34]

Level	**Service level**	**Users**	**Security requirements**	**Threats**
Application level	Software as a Service (SaaS)	End client applies to a user or organization who subscribes to a service offered by a cloud service provider and is accountable for its use	Privacy in multi tenant Environment Data protection from exposure (remnants) Access control Communication protection Software security Service availability	Interception Modification of data at rest and in transit Data interruption (deletion) Privacy breach Impersonation Session hijacking Traffic flow analysis Exposure in network
Virtual level	Platform as a Service (PaaS) Infrastructure as a Service (IaaS)	Developer– moderator applies to a person or organization that deploys software on a cloud infrastructure	Access control Application security Data security, (data in transit, data at rest, remnant) Cloud management control Security Secure images Virtual cloud protection Communication security	Programming flaws Software modification Software interruption (deletion) Impersonation Session hijacking Traffic flow analysis Exposure in network • Defacement • Connection flooding •Impersonation • Disrupting communications
Physical level	Physical datacenter	Owner applies to a person or organization that owns the infrastructure upon which	Legal (not abusive use of cloud Computing) Hardware security Hardware	Network attacks Connection flooding Hardware interruption Hardware theft

		clouds are deployed	reliability Network protection Network resources protection	Hardware modification Misuse of infrastructure Natural disasters

6. Conclusion

One of the common objections to the public cloud is cloud security, in spite of the fact that the main public clouds have proven to be less vulnerable to cyber attacks in comparison to an average business data centre. The biggest concern is related to the integration of security policy and identity management between customers and public cloud providers. Additionally, as per the government regulation customers may be prohibited from allowing sensitive data off premises. Risk of outages, data breach and operational costs are among the other concerns of public cloud services. Nevertheless, cloud computing, public or private, has become the platform of choice for many large applications. More importantly, the major public clouds now lead the way in enterprise technology development, facilitating new advances before they appear anywhere else.

References:

[1] EBook Definitive Guide to Cloud Security. Scribd.com. https://www.scribd.com/document/273458412/eBook-Definitive-Guide-to-Cloud-Security (accessed on June 11, 2021).

[2] A. Chalimov. “The Top Cloud Security Threats for Your Business in 2019 and How to Avoid Them.” Easternpeak.com. https://easternpeak.com/blog/the-top-cloud-security-threats-for-your-business-in-2019-and-how-to-avoid-them/ (accessed on June 9, 2021).

[3] McAfee. “6 Cloud Security Issues That Businesses Experience.” Mcafee.com. https://www.mcafee.com/blogs/enterprise/cloud-security/6-cloud-security-issues-that-businesses-experience/ (accessed on June 11, 2021).

[4] Q. Zhang, L. Cheng and R. Boutaba. “Cloud computing: state-of-the-art and research challenges.” J Internet Serv Appl 1, 7–18 (2010). https://doi.org/10.1007/s13174-010-0007-6.

[5] S. Sengupta, V. Kaulgud and V. S. Sharma. “Cloud Computing Security--Trends and Research Directions.” Proceedings - 2011 IEEE World Congress on Services, SERVICES 2011. 524-531. 10.1109/SERVICES.2011.20.

[6] M. Krigsman. “MediaMax / The Linkup: When the cloud fails.” Znet.com. http://www.zdnet.com/blog/projectfailures/mediamax-the-linkup-when-the-cloud-fails/999 (accessed on June 10, 2021).

[7] Novell Inc. survey on cloud computing. Novell.com. http://www.novell.com/news/press/novell-survey-reveals-widespread-and-accelerating-enterprise-adoption-of-private-clouds.

[8] L. Qian, L. Zhiguo, D. Yujian and G. Leitao. “Cloud Computing: An Overview.” CloudCom (2009).

[9] Air India reports data breach affecting 45 lakh passengers. Thehindu.com. https://www.thehindu.com/news/national/air-india-reports-data-breach-affecting-45-lakh-passengers/article34617628.ece (accessed on June 8, 2021).

[10] N. Alawadhi. “Yet another data leak: One million credit cards of Domino's Pizza customers.” Businessstandard.com. https://www.business-standard.com/article/companies/yet-another-data-leak-one-million-credit-cards-of-domino-s-pizza-customers-121041900731_1.html (accessed on June 8, 2021).

[11] D. Winder. “Zoom Gets Stuffed: Here’s How Hackers Got Hold Of 500,000 Passwords.” Forbes.com.

https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/?sh=3fd000de5cdc (accessed on June 11, 2021).

[12] M. Henriquez. “The top 10 data breaches of 2020.” Securitymagazine.com. https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020 (accessed on June 11, 2021).

[13] C. Cimpanu. “Microsoft discloses security breach of customer support database.” Zdnet.com. https://www.zdnet.com/article/microsoft-discloses-security-breach-of-customer-support-database/ (accessed on June 11, 2021).

[14] L. Abrams. “Wattpad data breach exposes account info for millions of users.” Bleepingcomputer.com. https://www.bleepingcomputer.com/news/security/wattpad-data-breach-exposes-account-info-for-millions-of-users/ (accessed on June 11, 2021).

[15] P. Bischoff. “Broadvoice database of more than 350 million customer records exposed online.” Comparitech.com. https://www.comparitech.com/blog/vpn-privacy/350-million-customer-records-exposed-online/ (accessed on June 11, 2021).

[16] D. Winder. “Estee Lauder Database Exposed; Customer Data Not Involved.” Forbes.com. https://www.forbes.com/sites/daveywinder/2020/02/11/estee-lauder-data-leak-440-million-records-exposed/?sh=4a9acf22590d (accessed on June 11, 2021).

[17] S. Ikeda. “Data of 538 Million Weibo Users Is Available on the Dark Web for Only $250.” Cpomagazine.com. https://www.cpomagazine.com/cyber-security/data-of-538-million-weibo-users-is-available-on-the-dark-web-for-only-250/ (accessed on June 11, 2021).

[18] D. Harwell. “Secret-sharing app Whisper left users’ locations, fetishes exposed on the Web.” Washingtonpost.com. https://www.washingtonpost.com/technology/2020/03/10/secret-sharing-app-whisper-left-users-locations-fetishes-exposed-web/ (accessed on June 11, 2021).

[19] Billions of Records of Web-Tracking Data Exposed by Oracle’s BlueKai. Cyware.com. https://cyware.com/news/billions-of-records-of-web-tracking-data-exposed-by-oracles-bluekai-00629add (accessed on June 11, 2021).

[20] B. Diachenko. “A UK-based Security Company Seemed To Have Inadvertently Exposed Its ‘Leaks Database’ with 5B+ Records.” Securitydiscovery.com. https://securitydiscovery.com/data-breach-database-data-breach/ (accessed on June 11, 2021).

[21] Xxdesmus. “Thai Database Leaks 8.3 Billion Internet Records.” Rainbowtabl.es. https://rainbowtabl.es/2020/05/25/thai-database-leaks-internet-records/ (accessed on June 11, 2021).

[22] Live streaming adult site leaves 7 terabytes of private data exposed. SafetyDetectives.com. https://www.safetydetectives.com/blog/cam-leak-report/ (accessed on June 11, 2021).

[23] Z. Doffman. “Facebook Dark Web Deal: Hackers Just Sold 267 Million User Profiles For $540.” Forbes.com. https://www.forbes.com/sites/zakdoffman/2020/04/20/facebook-users-beware-hackers-just-sold-267-million-of-your-profiles-for-540/?sh=4504e1ce7c85 (accessed on June 11, 2021).

[24] 235 million TikTok, Instagram and YouTube accounts exposed in database breach. Securitymagazine.com. https://www.securitymagazine.com/articles/93141-million-tiktok-instragram-and-youtube-account-exposed-in-database-breach (accessed on June 11, 2021).

[25] T. Hunt. “Inside the Cit0Day Breach Collection.” Troyhunt.com. https://www.troyhunt.com/inside-the-cit0day-breach-collection/ (accessed on June 11, 2021).

[26] P. Bischoff. “US property and demographic database of 200 million records leaked on the web.” Comparitech.com. https://www.comparitech.com/blog/vpn-privacy/200-million-us-database-leaked/ (accessed on June 11, 2021).

[27] E. Montalbano. “Leaked Details of 142 Million MGM Hotel Guests Found for Sale on Dark Web.” Threatpost.com. https://threatpost.com/leaked-details-142-million-mgm-hotel-guests/157402/ (accessed on June 11, 2021).

[28] A. LaVito. “Quest Diagnostics says 11.9 million patients’ financial and medical information

may have been exposed in data breach." Cnbc.com. https://www.cnbc.com/2019/06/03/quest-diagnostics-says-nearly-12-million-patients-may-have-had-data-breached.html (accessed on June 11, 2021).

[29] Houzz Security Update – FAQ. Houzz.com. https://help.houzz.com/s/article/security-update?language=en_US (accessed on June 11, 2021).

[30] T. Franck. "How to tell if you were affected by the Capital One breach." Cnbc.com. https://www.cnbc.com/2019/07/30/how-to-tell-if-you-were-affected-by-the-capital-one-breach.html (accessed on June 11, 2021).

[31] L. Bednar. "How to Check if Your Dubsmash Account Is Compromised." Securedata.com. https://www.securedata.com/blog/dubsmash-accounts-hacked (accessed on June 11, 2021).

[32] S. Ross. "Player Security Announcement." Zynga.com. https://investor.zynga.com/news-releases/news-release-details/player-security-announcement (accessed on June 11, 2021).

[33] C. Osborne. "The worst hacks, cyberattacks, and data breaches of 2018." Zdnet.com. https://www.zdnet.com/pictures/these-are-the-worst-hacks-cyberattacks-and-data-breaches-of-2018/ (accessed on June 10, 2021).

[34] D. Zissis and D. Lekkas. "Addressing cloud computing security issues." Future Gener. Comput. Syst. 28 (2012): 583-592.