JOIV : Int. J. Inform. Visualization, 5(3) - September 2021 298-305

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

# Cloud Computing Issues, Challenges, and Needs: A Survey

Mohammad Aljanabi[a,b], Shams N. Abd-Alwahab[a], RD Rohmat Saedudin[c], Hind Raad Ebraheem[a], Defni[d], Ronal Hadi[d], Mohd Arfian Ismail[e,*]

[a] *Alsalam University College, Baghdad, Iraq*
[b] *Department of Computer Science, College of Education, Aliraqia University, Baghdad, Iraq*
[c] *School of Industrial Engineering, Telkom University, Bandung, West Java, Indonesia*
[d] *Department of Information Technology, Politeknik Negeri Padang, Padang, West Sumatera, Indonesia*
[e] *Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, Malaysia*
*Corresponding author: [*]arfian@ump.edu.my*

***Abstract*— Cloud computing represents a kind of computing that is based on the sharing of computing resources instead of possessing personal devices or local servers for handling several applications and tasks. This kind of computing includes three distinguished kinds of services provided remotely for clients that can be accessed by using the Internet. Typically, clients work on paying annual or monthly service fees for suppliers, in order to gain access to systems that work on delivering infrastructure as a service, platforms as a service, and software as a service for any subscriber. In this paper, the usefulness and the abuse of the cloud computing are briefly discussed and presented by highlighting the influences of cloud computing in different areas. Moreover, this paper also presents the kinds and services of cloud. In addition, the security issues that cover the cloud security solution requirements, and the cloud security issues, which is one of the biggest issues in recent years in cloud computing were presented in this paper. The security requirement that needs by the cloud computing covers privacy, lack of user control, unauthorized secondary usage, and finally data proliferation and data flow. Meanwhile, the security issues cover including ownership of device, the trust issue and legel aspects. To overcome the security issues, this paper also presents the solution at the end of this paper.**

***Keywords*— Cloud computing; security in cloud; challenges; needs of cloud.**

*Manuscript received 29 Sep. 2020; revised 19 Dec. 2020; accepted 1 Apr. 2021. Date of publication 30 Sep. 2021.*
*International Journal on Informatics Visualization is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.*

## I. INTRODUCTION

This section gives an abbreviated review of the model of cloud service and how it has changed the industry and way people use and process digital content. Cloud computing is model which lets a user access various shared services on demand and with minimal management efforts. The cloud service concept is not a new one, it has been in use since the early origins of computing. The idea of cloud computing was supposedly introduced by J. C. R. Licklider whilst evolving the Advanced Research Projects Agency Network (ARPANET) in 1969, to connect people and data anytime anywhere [1]. The earlier versions of computer network had users access the central computer by connecting via terminals, small hardware with limited or no computing capabilities. These early terminals did not do much other than send and receive characters from a mainframe or centralized computer as in a point to point network [2]. Over the period of time these terminals got smarter as they were able to do more processing at the terminals and most of the computing was done at the local site instead of a central Server or computer. As time progressed and with advent of PC, individual computers became the de-facto and widely used across industry. With further revolutions in IT, networking and Internet, a new paradigm of computing has evolved, Cloud Computing. This model does not limit workstation capabilities with its hardware, instead, it allows utilizing the services provided by a shared and much better resources pool. It supplies enterprises and users with different abilities for storing and processing data in a data center of third-party and utilize large, shared resources. The figure 1 shows a cloud architecture with a high-level overview.

Many important organizations define cloud computing in in different definitions. Cloud computing was defined in the IT encyclopedia whatis.com as follows: "A comprehensive concept to anything that includes delivering hosted services

through the Internet". There are three diverse characteristics produced by cloud service distinguished it from conventional hosting. The service is entirely run by the provider (nothing has required from the consumer but internet access and his own computer); selling on request, it may be sold at an hour or a minute, and the users are capable of having abundant or slight of a service up to him in any time which mean it is malleable [3].

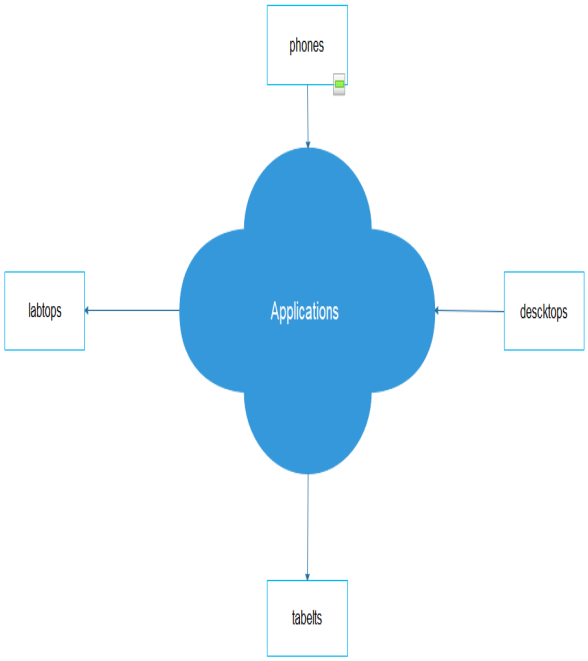


Fig. 1 Cloud Computing

While the cloud computing was defined in the Institute of Electrical and Electronics Engineers (IEEE) as follows: "A model in which information is stored permanently in the internet servers and temporarily cached on clients". And the definition of cloud computing in the Internet Wikipedia and encyclopedia is: "Services of software, computation, access and storage data that don't need the knowledge of the end-user for the configuration and physical position of the system that works on delivering services". Also, the concept of cloud computing was defined by one of the extremely substantial technical universities throughout the world which is the University of Berkeley, "Cloud computing indicates the applications delivered as services through the Internet, and the system's software and hardware in the data centers which supply these services" [4]. Another definition of cloud computing was provided via the firms of the analysts: "A computing style in which the massive scalable IT-related abilities are supplied as services by utilizing the technologies of the Internet for multi-external customers" [4].

Cloud computing was also defined by the NIST which is the National Institute of Standards and Technology, as follows: "Cloud computing is a model which provides appropriate accessing of the on-demand network for a shared group of configurable computing resources such as; applications, network, hardware, storage, etcetera which is capable of being allocated rapidly, scaled, and released with the lower effort of management or service provider intervention [2].

## II. Material and Methods

### A. Data Storage Over Cloud

In order to understand why cloud pose a concerns for your data, it is necessary to understand how it stores the data and what enables it to let the data be available to you anytime and anywhere. The capabilities which allow this flexibility in turn pose risk for the users. Cloud is a made up of many distributed databases but still allows to be treated as one. Among many features of cloud, it is noteworthy to realize that it maintains high tolerance through redundancy and distribution of data. Data which is stored at a server is often duplicated and kept at multiple locations which can be located across geographies coming under different laws and regulations. This can be risky in case of a government agency asking the CSP to reveal the data they have stored in the servers. My research intends to mitigate this problem by encrypting the document so that even if CSP wants to reveal the data at their server, it will be of no use without the key to decrypt the document which is in control of users/ document owners.

### B. Cloud Data Storage Tools

There are many products available in market which provide online storage for your data. This section will give a brief survey of the available products.

*1) Dropbox:* It is a service of file hosting run via Dropbox Inc and the headquarters placed in San Francisco-California [5]. It allows user to create folders in their local system which it synchronizes to the server. Files are accessible from Dropbox website or mobile application.

*2) Google Drive :* It is cloud based file storage and syncing service [6]. It also lets one create, share and collaborate on documents over the Internet. It is available for free unless the data size is less than 15GB.

*3) SkyDrive / OneDrive :* It is a file hosting service soffered by Microsoft which lets one create and store file and later access by web or mobile [7].

### C. Type of Clouds

*1) Public:* In Public cloud, the services are produced by a third side across the Internet in imitative way, and they are apparent for everyone (this shouldn't denote it has to become free). Also renowned as external cloud. Hence the information in the cloud available of many users, however, they still are not capable of accessing this information of the others [8].

*2) Private:* This cloud is specific for the same company mimic a cloud in internet, (private network) which mean for a personal use only. Composed of the computation, hosting of private applications, or storage within the same organization. It can have the same regular way of the coast of infrastructure and maintenance but in better way in scalability and participation [9].

*3) Hybrid:* The hybrid type represents an incorporation of the private and public clouds. This type is a charitable choice if we require of having our application or data in native without the need for excessive investing in infrastructure. Therefore, the organization is capable of

utilizing a portion of its services in its infrastructure and as well in the public cloud. Alternatively, it is capable of utilizing a public only when having peaks of employment [10].

*D. The Services of Cloud*

The cloud providers are capable of providing three fundamental layered services. Every layer can consume the services supplied via the layer under it [11].

*1) Software as a Service (SaaS):* The whole kinds of software involving Sales, financial, HR, CRM, and office assistants are capable of delivering as a service. Google Docs, Zoho Docs, and Salesforce.com are instances for the services of SaaS. SaaS services consumers (generally, software-administrators, and end-users of the applications) can reach these kinds of software via mobile applications and web browsers [12].

*2) Platform as a Service (PaaS):* Integration bus, middleware, and databases are instances supplied via the providers of PaaS as a service. The services of PaaS are usually consuming via the testers, application administrators, integration engineers/middleware and developers. An example for the common PaaS is the Engine of Google App.

*3) Infrastructure as a Service (IaaS): Clouds* of IaaS works on providing resources of low-level infrastructure for the consumers like computational power, storage, recovery & backup, networks, and content delivery networks as a service. Typically, the consumers of IaaS include the developers of systems, the engineers of networks, the administrators of systems, the managers of IT, and the engineers of monitoring [13].

*E. Cloud Computing Advantages*

There are many usefulness of using cloud computing, some of these advantages are presented in this section:

*1) Save Hardware Cost:* By using cloud computing, Companies can diminish on hardware employment because they will not be forced on purchase extra server, peripherals, and other network equipment.

*2) The easy of Backup & Recover:* Within a virtual machine, the servers can be kept in one image file including the whole system settings and configuration. When a server shattering, there is no requirement for starting from beginning to proceed reinstallation and reconfiguration. You can keep time, effort and resources, by no more of taking a copy of the saved image, restoring data from final back up, and the server will be backup and working another time [14].

*3) Easy to Deploy*. the workload and efforts of IT staff can be diminished and accelerating the work because it is wherever possible to clone the servers, as well as, to perform on other machines with no need to alter the configuration [15].

*4) Energy Bills Saving.* The usage of cloud computing works on reducing the requirement of preserving room temperature to cool down the server, hence, the electricity usage cost will be minimized. additionally, space will be reduced, the fewer servers, the less space to store the equipment of the network. In cloud computing, hardware virtualization and standardization include imitation and encapsulation in order that the presentation and elimination process of specific hardware can be performed easily [16].

*5) Easier in supersede and improve.* By utilizing cloud computing the substituting or promotion a server specification will be simpler to implement, also, we can simply rise the specialization or shift virtual machines to others, more robust server in the case the origin server is overstrain and specifications are not adequate anymore [17].

*6) Remote Accessibility.* With cloud computing, you can access the services from anywhere which means your business is not bounded to a certain position. To achieve that you must have your password and identification (ID). Sometimes there is an additional security request however since they also are mobile, so the cloud services can be reached at any place over the world.

*7) The Easily of Expanding.* In cloud computing, one of the most attractive advantages is represented in pliability, if we need to extend our business, we can access more resources quickly. We will never need to purchase further infrastructure. The only one thing we need is to report the cloud supplier about the desire resources and they will be assigned it to us. In most cases, expanding requires only a few minutes. A similar process can happen when we need to utilize lesser resources [18].

*8) Security.* Clouds head to be very secure comparing with the conventional models of business. The real-time back up presented by the cloud provides a lower loss of data. In the outage case, the backup servers can utilize that sync with the major ones instantly they are up. Our business acquire superior uptime with no data loss [19].

*9) Friendly of Environmentally.* The utilization of ready-made resources designed for us requires reducing the expenses of electricity. Whilst we are saving on electricity, additionally, we are saving on resources needed for cooling off the computer and another component. This led to reducing the risk of emissions to the surrounding [20].

*F. Cloud Computing Disadvantages*

Cloud computing needs a stabilized connection of the internet, and if the connection of the internet is not reliable, then we can't obtain it. Particularly, this case represents an obstacle for the people who are living in distant places with no reliable accessing of connection. The main notable cloud computing abuse is the affecting of the whole virtual machines (VMs) if the center of data is crashed. This disadvantage is stopped via making a regularly back up for our data and utilizing clustering or failover [21].

One of the other bad scenarios is when an origin server be a goal of a hacking attack, so, perhaps, the intruder is capable of accessing virtual servers utilizing the data that are stored on the origin server. These are the cloud computing advantages that we must be taking it in our considerations prior to jump on the virtualization and cloud computing wagon. In spite of cost and facility of use are two considerable benefits of cloud computing, but there are substantial security attentions that must be processed when needing to convert ticklish applications and sensitive data to generic and participate cloud environments. To address these

attentions, the level of the security would be the same or greater of security than the organization would have if the cloud were not utilized, this achieves by the cloud supplier which must improve adequate controls. When considering cloud computing ten points below should be review [22].

1. Where's the data? Diverse countries have diverse requirements and controls placed on access. Your data is in the cloud, this led to that the data must reside in a physical location. Your cloud supplier should agree in writing to prepare the level of security desired for your customers.

2. Who has access? It is a major concern "access domination", the insider offense are a tremendous risk. These attacks may come from a person who has been dependent with confirmed reach to the cloud" A probable hacker ". If anyone doubts this, consider that in early 2009 an insider was accused of implantation a logic bomb on Fanny Mae servers that, colossal injury would have occasion if launched. The main interest to anyone considering utilizing the cloud must to look at the person who is managing their data and what types of controls are applied to these individuals.

3. What are your regulatory requirements? In the US, Canada, or the European Union Organizations operating have plentiful regulatory demands that they must abide by (e.g., ISO 27002, Safe Harbor, ITIL, and COBIT). These requirements must be met by the cloud supplier and is willing to undergo certification, accreditation, and review [23].

4. Do you have the truth to auditing? This appointed item is a wide issue; the cloud supplier must accept in writing to the conditions of audit.

5. What kind of training does the supplier submit their employees? The really a rather significant thing, the reason is people will always be the enervate link in security. It's an important item to Knowing how your supplier practice their employees.

6. What kind of data classification system does the supplier utilize? We must be observant of questions which involve: Is the data classified? How is our data separate from other users? Additionally, ciphering should be argued. Is it being utilized whereas the data is in transit and at rest? What kind of ciphering is being utilized? For instance, there is a large variation between WPA2 and WEP [24].

7. What are the terms of service level agreement (SLA)? The services level should be supplied is defined in the serves of SLA with a contract level of ensured service which conducted between the cloud supplier and the client.

8. What is the long-term survival of the provider? In the case of the cloud provider exit the business, what about your data? Can you retrieval your data, and if so, in what format? What is the period that cloud supplier been in business and what is their channel record be? For instance, in 2007, Media Max of on-line storage service left the business because of an error in the system administration which led to delete active customer data. This unsuccessful company was concentrated on reliability concerns of cloud computing and left unhappy users behind it.

9. What is a procedure in a security violation case? If a security incident occurs, how the cloud provider will support you? Whilst several providers want their services to become not hackable. The main goal for hackers is cloud-based services [25].

10. What is the plan of business continuity/disaster recovery (BC/DR)? Whilst we mightn't realize the actual place of our services, physically, it is placed someplace. The whole physical places face threating events like storms, fire, power loss, and natural disasters. When one or more of these threats are happening, the question is how the provider of the cloud can respond, and what is the promising warranty of services continuing that is provided by the provider? for instance, in February of 2009, the contacts of Nokia's on Ovi-servers are destroyed.

### *G. Applications of Cloud Computing*

*1) Communication:* Through cloud the users can entertain network-based access for connecting apparatus such as calendars and emails. Many apps like Skype and WhatsApp which are specified for calling and messaging are also based on the infrastructure of the cloud. Instead of stored all information and messages on the personal device, they can be stored on the hardware of the service provider. This will offer you accessibility to your information across the internet from anywhere [26]

*2) Productivity:* Also, the Office materials utilize cloud computing like Microsoft Office 365 and Google Docs, across the internet making us use our more productive tools. We are capable of working our spreadsheets, presentations, and documents at any time and from anywhere. Because our data is stored in the cloud, when our device is stolen, we do not require to concern about losing or spoiling data. The sharing of documents also offered by the cloud which make different individuals working at the same time on the same document.

*3) The Process of Business:* Several applications of business management such as enterprise resource planning (ERP) and customer relationship management (CRM) are dependent on the provider of cloud service as well. SAAS becomes a widespread method to deploy software of enterprise-level. Marketo, Hubspot, Salesforce, and etcetera are regarded as widespread instances for this method. SAAS represents an efficient and cost-effective method for service customers and providers. This method guarantees hassle-free maintenance, management, and security of our organization's critical business resources and permits us for accessing these applications easily by a web browser [27].

*4) The Backup and Recovery:* If we select a cloud for storing the data, then the service provider is becoming responsible for our information by providing secure data and legal requirements, and this will help us to avoid capital spending to build and maintain infrastructure. Additionally, the cloud is capable of providing high flexibility of large storing and backup on-demand. The process of recovering data in the cloud is accomplished in a fast way since the stored data is on physical servers rather than on data site center. Dropbox, Amazon S3 and Google Drive are common instances for the solutions of cloud back up.

*5) The development of Application:* Cloud platforms are considered as a reliable solution to develop different applications such as mobile, web, or games. Therefore, it can

be very easy to make scalable experiences of cross-platform to our users, when utilizing the cloud. These platforms involve various pre-coded libraries and tools which led to speed up and simplify the development process such as services of the directory, security, and search. One of the common tool for developing a mobile game utilized in the cloud is the Amazon Lumberyard.

*6) Testing & developing:* The cloud environment is capable of reducing spending and launching our applications in the markets fast. The developers are able to utilize the cloud for setting up and dismantling the testing and developing of environments instead of setting up physical environments. Therefore, the technical team will reduce the need for guaranteeing budgets and outlying crucial project resources and time. The environments of developed testing are also capable of scaling up or scaling down depending on their needs. The common tools of testing are Blaze Meter and Load Storm.

*7) The Analytics of Big Data:* Cloud computing allows the scientists of data to benefit from any organized data for analyzing it for insights and patterns, get relations to obtain predictions, predict future disaster and assist in making a decision in data backed. The services of cloud work on mining a huge amount of data via utilizing sophisticated tools and high power of processing. Lots of open-source big data tools are available which are depending on clouds, such as Cassandra, HPCC, Hadoop, etc. In small companies, with no cloud, it is not hard for collecting and analyzing data in real-time.

*8) Sits of Social Networking:* One of the common and usually forgotten applications in cloud computing is social media. There are several sites of social media networking that utilize cloud computing such as; LinkedIn, Facebook, Twitter, MySpace, etc. These sites are created for finding persons we want to know or formerly know. In the process of finding persons, we share various private information. When a person shares information on social media, then this person shares information not only with his friends but with the platform makers as well. Therefore, the platform needs a robust solution for real-time data managing and storing which makes the utilization of cloud crucial. Cloud has presented advanced solutions for individuals and companies. When we are searching for a provider of service for helping us leverage the cloud, then, New Gen Apps can become a partner of selection. Today, there are several widespread cloud platforms to be worked with such as GCP, Azure, and AWS.

*9) The Usage of Scalable:* Cloud computing is capable of offering scalable resources via different models of subscription, i.e., we will just require paying to the computing resources we utilize. This assists in managing the rise in requests with no requirement for permanent investing in the hardware of computers. As an example, Netflix is leveraging the possibility of cloud computing to its usefulness. It countenances considerable surges in server load at times of peak, owing to its service of on-demand streaming. The moving from in house data centers to cloud permits the company to considerably extend its base of the customer with no need for investment in the setting up or maintaining the expensive infrastructure.

*10) The bots of Chat:* The cloud capacity and the expanding of computing power provides us with the capability of storing information about the preferences of the user. This can be utilized for providing customized solutions, products, and messages depending on the user's preferences and behavior. Google Assistant, Alexa, and Siri are cloud-based natural language smart bots. The chat bots benefit from the computing abilities in the cloud for providing personalized experiences of the context-relevant customers. Therefore, remember that, when we say hi to Siri, there is a cloud-based artificial intelligent solution beyond it.

### *H. Security Concern*

With user data stored on a third-party resource many security issues arise. Below are short description of issues as enumerated in Benameur, et al [28] [22].

*1) Privacy*: Privacy at a coarse level refer to users control of their data and reserving the right to expose it to others. For organizations, it entails the way they store and manage personal identifiable information. Public cloud access is the most widespread way of accessing the cloud as service (that can be accessed over Internet and intranet) but relying on the provider of cloud service to handle the confidentiality of the data raises many concerns [29].

*2) Lack of User control:* While accessing cloud service it is not expected from service provider to cater to users demand of restricting storage of their data and duplicating it. Data is stored over machines where users do not have any control and places where the laws can be different from the place of origin.

*3) Unauthorized Secondary Usage:* Data over cloud is a great source of revenue of the service provider as it provides a resource for mining interesting patterns and target ads. Moreover, there is no guarantee if the service provider goes bankrupt and the sells the data to gain more revenue. These unauthorized data usages pose a great risk to the user and organizations using the cloud service [30].

*4) Data Proliferation and Trans border Data Flow:* Data in cloud involves multi-parties and multi storage sites. User, who is the data owner, has no control over the sites and parties involved in the processing of his/her data. When data in cloud is moved across sites falling under different legal jurisdiction increases risk and factor and legal complexities [31].

## III. Results and Discussion

### *A. Security Issues*

Traditional security measures considered a secured perimeter with a trusted boundary within which information is stored and processed, to be secure. But this has changed a lot within few years with increased access to cloud and distributed computing. People and data have been more dynamic and information exchange has been increasing. With data being freely shared and distributed, It poses danger of information leak and it is more severe for enterprises who use cloud services. It endangers their

Intellectual property and business secrets. Traditionally, enterprises enforce IT policies and security constraints to restrict the flow of data outside their organization. With more and more employees using cloud for their day to day work, business now face a risk of losing or leaking out information. A document once uploaded over cloud may not fall under the owners jurisdiction and is susceptible for copying or any malicious usage.

*1) Bring your own device (BYOD)*: This issue knows as ownership issues. It is becoming very popular these days among employees, as it gives the much-needed flexibility to the employees and increase productivity. It is a growing trend among the users for utilizing their personal devices for work purposes. According to a survey done by security intelligence which provides analysis and insight for information security professionals, almost 60 percent of the enterprises allow their users for bringing their own devices to be worked [25]. This shows how popular usage of non-IT systems is. This increases the risk of information leakage manifold as now not all the personal laptops and devices are enabled with IT policies of the organization and not as secure as an on-premises computer. Another report by Gartner [10] guesses that about 2017, almost half of the users would need to utilize their devices for purposes of work. BYOD does increase productivity and helps get things done virtually from anywhere, but a certain solution is needed to compensate the risk factors involved [32].

*2) Trust Issues:* With the presence of multiple vendors offering distributed computing and cloud storage, there has been a race to get to cloud. Business now has many options to choose from. However, the dynamically changing industry and the sensitivity of data may be inhibiting factors against choosing for cloud. Trust is a main concern with many industries, mainly health and financial due to the sensitivity of the data being stored. Since user does not have control over his/her data over cloud, they may not completely trust the cloud service provider specially if the data is related to their health and finances. Recent reports in media hint at government agencies like NSA being able to mine the data stored over cloud without any prior permission. NSA PRISM program in collaboration with large tech companies intends to do so. Media articles even suggest that Microsoft gave NSA permission to record Skype calls and go mine user data store over cloud [28].

*3) Legal Aspects:* Since data in cloud is stored at multiple places across geographies, laws of the land could be different and may not be strict enough to protect user data. Moreover, cloud service provider always get request from government and securities agencies to disclose the data they have stored and are bound by law to disclose it. The USA Patriot Act signed by Bush on Oct 26, 2001, assigned the US government unrestricted capability of accessing data stored outside the US via U.S. providers of cloud service or their foreign subsidiaries [12].

### *B. Recent Attack*

This section will briefly enlist some recent attacks to give an idea of the impact of data breaches on corporation. The intent of this section is not to enlist every attack but only to give an idea of the importance of protecting data over cloud. The recent cyber-attack on Sony Pictures Entertainment [13], allegedly due to the release of the motion picture The Interview" can be a lesson for businesses to put in more efforts in protecting the data in cloud [11], [16], [18]. Analysts are predicting that the data breach could have cost Sony as much as 100 million USD notwithstanding the lost goodwill and brand image of the company. Recently IDC, International data center, expected that more than 1.5 billion persons in 2020 will be influenced via the breaches of data, that is almost a quarter of world population [14], [33]. There is a growing need for a hardened security feature for enterprises whichtoday face attacks from hackers. The emphasis of this thesis is to provide a hardened security by using Intel's latest technology which would help prevent data breaches. The analyst of the industry in Moor Insights and Strategy, Patrick Moorhead pointed out that when Target and Sony [8] possessed that hardware-based, multiple-factor authentication, they would not be successfully hacked [15].

### *C. Cloud Security Solution*

Information Security is not very black and white to implement. The data one wants to protect may not always be static or restricted to one person. Information is created to be shared among many stake holders. Information is not monolithic, various access levels for users are required according to their privilege levels. Information right management solves this to some extent where user have different permissions for any given document. However, this does not protects the data from the cloud. Given the popularity and various advantages of cloud services usage of cloud is very difficult to avoid. A general security solution in enterprise is either very restrictive or very open. Traditional security measures assumed that information consumption in a secured and bounded environment is secure enough. But both the solutions have their faults, the complete and unshared security limits the users from being productive and makes it hard to share even with an intended recipient. Using an enterprise cordoned off environment does not restrict users to upload on cloud and is susceptible to cloud services [34], [35].

### *D. Cloud Security Solution Requirement*

A Cloud security solution must have the following features which would solve the purpose of security and allow the flexibility of cloud.

*1) Selective Security:* It should allow Users to mark any folder as secure. Users must have flexibility to protect specific documents they want. A complete system-level security hampers the performance and is very user intrusive which may lead to users finding a way around and defeating the purpose of information protection [32].

*2) Cloud Access:* Even though uploading data on cloud in plain text is risky, the requirement here is to allow users to upload the data to cloud in a secure fashion. The solution meet the corporate IT standards and cloud provider should have no visibility into the data.

*3) Sharing:* The users should be able to share the documents with any authorized users. To provide a hassle-

free sharing, the users should be able to use a single click UX to share data [36], [37].

## IV. CONCLUSION

We can keep time, effort and resources, by no more of taking a copy of the saved image, restoring data from final back up, and the server will be backup and working another time. The real-time back up presented by the cloud provides a lower loss of data. The main notable cloud computing abuse is the affecting of the whole virtual machines if the center of data is crashed. This disadvantage is stopped via making a regularly back up for our data and utilizing clustering or failover. One of the other bad scenarios is when an origin server be a goal of a hacking attack, so, perhaps, the intruder is capable of accessing virtual servers utilizing the data that are stored on the origin server. In spite of cost and facility of use are two considerable benefits of cloud computing, but there are substantial security attentions that must be processed when needing to convert ticklish applications and sensitive data to generic and participate cloud environments. Your data is in the cloud, this led to that the data must reside in a physical location. The main interest to anyone considering utilizing the cloud must to look at the person who is managing their data and what types of controls are applied to these individuals.

With data being freely shared and distributed, It poses danger of information leak and it is more severe for enterprises who use cloud services. Trust is a main concern with many industries, mainly health and financial due to the sensitivity of the data being stored. Since user does not have control over his/her data over cloud, they may not completely trust the cloud service provider specially if the data is related to their health and finances. Recent reports in media hint at government agencies like NSA being able to mine the data stored over cloud without any prior permission.


## ACKNOWLEDGEMENTS

The authors would like to thank Universiti Malaysia Pahang for the financial sponsorship under Postgraduate Research Grants Scheme (PGRS) with grant No. PGRS190360.


## REFERENCES


[1] C. Sumner, A. Byers, and M. Shearing, "Determining personality traits & privacy concerns from facebook activity," *Black Hat Briefings,* vol. 11, pp. 197-221, 2011.

[2] T. Alakurt, "Adaptation of online privacy concern scale into turkish culture," 2017.

[3] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," *International journal of engineering research and applications,* vol. 3, no. 4, pp. 1922-1926, 2013.

[4] O. Kocabas and T. Soyata, "Towards privacy-preserving medical cloud computing using homomorphic encryption," in *Virtual and Mobile Healthcare: Breakthroughs in Research and Practice*: IGI Global, 2020, pp. 93-125.

[5] 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.

[6] S. N. Kumar and A. Vajpayee, "A survey on secure cloud: security and privacy in cloud computing," *American Journal of Systems and Software,* vol. 4, no. 1, pp. 14-26, 2016.

[7] Z. Shen and Q. Tong, "The security of cloud computing system enabled by trusted computing technology," in *Signal Processing Systems (ICSPS), 2010 2nd International Conference on*, 2010, vol. 2, pp. V2-11-V2-15: IEEE.

[8] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for cloud exchange: A survey," *Computers & Electrical Engineering,* vol. 81, p. 106526, 2020.

[9] T. Wang, Y. Mei, W. Jia, X. Zheng, G. Wang, and M. Xie, "Edge-based differential privacy computing for sensor–cloud systems," *Journal of Parallel and Distributed Computing,* vol. 136, pp. 75-85, 2020.

[10] S. A. Osia *et al.*, "A hybrid deep learning architecture for privacy-preserving mobile analytics," *IEEE Internet of Things Journal,* 2020.

[11] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Communications Magazine,* vol. 55, no. 1, pp. 26-33, 2017.

[12] P. Li *et al.*, "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems,* vol. 74, pp. 76-85, 2017.

[13] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *Journal of Network and Computer Applications,* vol. 84, pp. 38-54, 2017.

[14] S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Computing,* vol. 22, no. 2, pp. 42-51, 2018.

[15] M. Alsajri, M. A. Ismail, and S. Abdul-Baqi, "A review on the recent application of Jaya optimization algorithm," in *2018 1st Annual International Conference on Information and Sciences (AiCIS)*, 2018, pp. 129-132: IEEE.

[16] S. A.-b. Salman, A.-H. A. Salih, A. H. Ali, M. K. Khaleel, and M. A. Mohammed, "A New Model for Iris Classification Based on Naïve Bayes Grid Parameters Optimization." International Journal of Sciences: Basic and Applied Research (IJSBAR) (2018) Volume 40, No 2, pp 150-155.

[17] M. K. Khaleel, M. A. Ismail, U. Yunan, and S. Kasim, "Review on Intrusion Detection System Based on The Goal of The Detection System," *International Journal of Integrated Engineering,* vol. 10, no. 6, 2018.

[18] Z. F. Hussain *et al.*, "A new model for iris data set classification based on linear support vector machine parameter's optimization," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 10, 2020.

[19] B. Q. Elias, M. Alsajri, P. J. Soh, and A. A. Al-hadi, "Design of Flexible Planar Antennas Using Substrate Gap Structure for Surface Wave Reduction," in *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*, 2019, pp. 453-458: IEEE.

[20] M. A. Mohammed *et al.*, "A Focal load balancer based algorithm for task assignment in cloud environment," in *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2018, pp. 1-4: IEEE.

[21] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *2012 International Conference on Computer Science and Electronics Engineering*, 2012, vol. 1, pp. 647-651: IEEE.

[22] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[23] E. Knorr and G. Gruman, "What cloud computing really means," *InfoWorld,* vol. 7, pp. 20-20, 2008.

[24] J. Brodkin, "Gartner: Seven cloud-computing security risks," *Infoworld,* vol. 2008, pp. 1-3, 2008.

[25] R. Chow *et al.*, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, pp. 85-90: ACM.

[26] F. Zafar *et al.*, "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends," *Computers & Security,* vol. 65, pp. 29-49, 2017.

[27] M. Ahmadian, F. Plochan, Z. Roessler, and D. C. Marinescu, "SecureNoSQL: An approach for secure search of encrypted NoSQL databases in the public cloud," *International Journal of Information Management,* vol. 37, no. 2, pp. 63-74, 2017.

[28] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation computer systems,* vol. 28, no. 3, pp. 583-592, 2012.

[29] T. Wang *et al.*, "Fog-based storage technology to fight with cyber threat," *Future Generation Computer Systems,* vol. 83, pp. 208-218, 2018.

[30] O. Razi, S. Sanyal, M. Raza, S. Sourav, and R. Somkunwar, "A survey paper on improving performance and enhancing security by using division and replication of data in cloud," *International Journal of Advanced Research in Computer Science,* vol. 9, no. 2, 2018.
[31] K. Patel and A. Alabisi, "Cloud Computing Security Risks: Identification and Assessment," *The Journal of New Business Ideas & Trends,* vol. 17, no. 2, pp. 11-19, 2019.
[32] W. I. Yudhistyra, E. M. Risal, I.-s. Raungratanaamporn, and V. Ratanavaraha, "Using Big Data Analytics for Decision Making: Analyzing Customer Behavior using Association Rule Mining in a Gold, Silver, and Precious Metal Trading Company in Indonesia," *International Journal of Data Science,* vol. 1, no. 2, pp. 57-71, 2020.
[33] A. H. Ali, "Fuzzy generalized Hebbian algorithm for large-scale intrusion detection system," *International Journal of Integrated Engineering,* vol. 12, no. 1, pp. 81-90, 2020.
[34] M. Ahmad Dar, "Security Architecture for Low Resource Devices in Smart City using Cloud," *2020,* smartphone; elliptic curve; smart city; cloud vol. 4, no. 3, p. 4, 2020-09-30 2020.
[35] N. R. Zaynalov, U. K. Narzullaev, A. N. Muhamadiev, I. R. Rahmatullaev, and R. K. Buranov, "Combining Invisible Unicode Characters To Hide Information In A Text Document," *2020,* vol. 4, no. 3, p. 6, 2020-09-30 2020.
[36] P. Khandare, S. Deokar, and A. Dixit, "Improvement of Traditional Protection System in the Existing Hybrid Microgrid with Advanced Intelligent Method," *International Journal on Data Science,* vol. 1, no. 2, pp. 72-81, 2020.
[37] I. M. Al-Joboury and E. H. Al-Hemiary, "Virtualized Fog Network with Load Balancing for IoT based Fog-to-Cloud," JOIV : International Journal on Informatics Visualization, vol. 4, no. 3, Jul. 2020.