CSPM: A Secure Cloud Computing Performance Management Model

Abeer F Alotaibi[a], Mohammed A. AlZain[a], Mehedi Masud[a] and NZ Jhanjhi[b]

[a]College of Computers and Information Technology,Taif University, Al-Hawiya, 21974, KSA
[b]School of Computer Science and Engineering, SCE, Taylor's University, Malaysia

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: Cloud computing offers an innovative organization and user ability share, store and retrieve data anytime and from anywhere. The critical aspect in cloud computing is security due to privacy and sensitive information. As a lot of companies and users share confidential and critical data on a cloud so the important part is how the data be secured. The worried question about confidentiality, availability and integrity of data in the cloud from attacks and damage of cloud services. This paper discusses the concerns associated to the data security, performance and management sides in cloud computing. The worry side in security such as CIA security which is data Confidentiality, data integrity, and service availability will be given. This paper proposes a cloud security performance management (CSPM) model which ensures different aspect such as, cloud computing security, cloud performance, cloud management. In addition, it discusses the construction of the proposed CSPM model. It defines the factors and layers of CSPM model. Gets the outcome of the new proposed model and then implementation that's to illustrate the factors of security in cloud computing, such as data confidentiality, data integrity, and service availability. Data management and time performance will be discussed during experimentation part of this work.

Keywords: Cloud computing, cloud security, data management, time performance, data integrity, data confidentiality, service availability.

1. Introduction

Recently, cloud computing has attracted interest in all aspects and issues however it is as yet growing model. Certain people see the cloud computing as a new uprising technology, while others consider it as a natural development of technology, economy and culture (Zhang, X ,2010). Cloud computing is an essential part, as with cloud computing the possibility of considerably reducing budgets through improvement and also increasing operational and economic productivities. The rapid advancement of cloud technology is due to its ability to access the hardware, the software and the infrastructure that can be arranged at user need. Thus, it led to increasing in the number of users in all areas and fields of cloud computing(Ratten, V, 2020).With the increase and availability of cloud services for consumers and the usage of tablet devices and mobile, this has led to a large and growing turnout of companies, increasing the consumers' need to access more information services. Cloud computing provides flexible access to data over the Internet. Therefore, referring to travelling or working online from anywhere, it has become important to access information across different computing devices. a lot of organizations both small and medium has rapidly increased the use of cloud computing due to the reduction in cost, availability of data and ease of access (Subashini, S, 2011),(AlZain, M.A.,2012). Cloud computing carries these benefits more attractive than ever whereas it presents security threats because Cloud Service Providers (CSPs) are isolated administrative entities. Without security and confidentiality clarifications for the cloud, the potential revolutionary computing model could become unusable and unreliable. Some surveys and studies of cloud computing users clarify that the security and privacy are the main concerns which promote to cloud adoption (Wang, C.,2010). Security factors are considered as challenges and hardships in cloud computing environment. Confidentiality, integrity and availability are the security factors. Thus, the security factors which are confidentiality, integrity and availability will be examined in the proposed model.

The remainder of this paper is organized as follows.

Second section presents in brief an introduction of cloud computing environment. Third section discusses cloud computing performance concerns. Fourth section presents management issues in cloud computing. Fifth section discusses the newly proposed model which is called CSPM model with the explanation of its component. Sixthly, the experimentation and the evaluation of the newly proposed model will be given. Finally, section seven will conclude the paper.

2. Cloud Computing: primarily

The idea of cloud computing is ability to stored data centrally, and could accessed to data anywhere and time (Ryan, M.D,2013). The National Institute of Standards and Technology (NIST) defines cloud computing as a model to enable access to the network anywhere and anytime(Basu, S,2018). In addition, NIST describes cloud computing as a request to a common configurable group of computing supplies, such as applications, networks, services, storage and servers that can be provided quickly and minimize the administrative effort(Hogan, M,2011). Cloud computing is one of the fastest evolving technologies, while everyone in various fields use cloud computing on a daily basis, such as Microsoft Office 365, Gmail Dropbox, Gmail, etc(Kumar, P.R,2018).

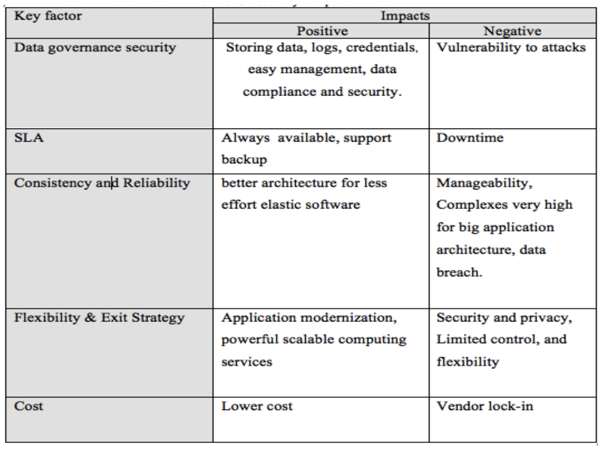
3. Cloud computing performance

The cloud works with a huge user that’s according different requirements. So, the clouds have the ability to provide venders with many profits in terms of cost, software, service, performance and also at the same time. Researchers in (Iosup, A,2011) Select four clouds and Infrastructure as a Service, the four clouds are Amazon EC2, GoGrid, ElasticHosts, and Mosso. Also, authors focused only on IaaS service providers. The reason for that focus on IaaS is due to the survey conducted for cloud computing providers(Prodan, R,2009) . FlexiScale sets new clients on the waiting list for a period of up to more than two weeks due to the overload of the system. Amazon Elastic Compute Cloud (EC2) is infrastructure as a Service of cloud computing that allow access of amazon’s infrastructure for clients. The service is flexible as the user can expand or reduce their infrastructure by launching or terminating new virtual machines.

3.1 Five Performance Factors

Several inquiries about cloud computing and services provided to companies from medium and small enterprises have been studied and analyzed. Also, what are the factors and causes affect the performance in providing the service and its impact on those companies. According these questions, "What are essential factors that required special management attention to develop the adoption of cloud computing and corporate performance?" This question was analyzed using a performance map (IPMA)(Khayer, A, 2020) The results and the answer of this question emerged from several factors, including as following: The comparative advantage in using cloud computing enables the reduction of cost, save work time that it's enhances productivity and increases sales in addition to providing opportunity and enables the use of common resources (Alkhater, N, 2018),(Armbrust, M, 2010). In addition to the fact that cloud computing provides medium and small businesses with several advantages that cannot be possible in the past, one of these advantages is a pay-per-use option. Moreover, scalability and flexibility. So, the relative advantage of the impact on cloud computing adoption is positive. The second factor affecting the adoption of cloud computing is the quality of the service, as services are provided to end users. Services are through multiple technologies anytime and anywhere, so the service must be fast, uninterrupted and responsive(Alkhater, N,2018). There are issues that could harmfully the adoption of cloud computing, and they are the risks associated with this service that may negatively affect the company, which is what most worries companies’ dealings over the Internet or the network. As there are previous studies that estimated the direct negative impact of the potential risks (Liao, C.,2011); (Gupta, P,2013) Companies are focus on partners of technology rather than suppliers of technology. So they can provide support and knowledge from partners(Maqueira-Marín, J.M.,2017). In the field of cloud computing, an increasing number of advanced companies, led by Amazon, are developing many gigantic servers and striving to provide various cloud-based service and business models to their client companies. based on major of cloud providers such as Apache, EMC, and Cisco facilitate customer companies' access to the cloud (Maqueira-Marín, J.M.,2017).Where they enjoy providing, developing, adopting the cloud and providing services, one of these cloud service providers is IBM Google Salesforce. Hence, we conclude that cloud providers may positively influence cloud computing adoption. At this moment, there are no global laws to ensure the safety of data and cloud resources (Faragallah, O.S.,2021). Therefore, the server’s location is an important factor in adopting the cloud, in addition to that some service providers may have the actual location of the server located anywhere in the world. Store data with laws. For that cloud storage location may affect cloud adoption. Cloud computing provides access to technology resources that provided by third party and this led reduces the cost on the company and the cost of developing the internal IT infrastructure (Yeboah-Boateng, E.O.,2014);(Maqueira-Marín, J.M.,2017). Table 2.2 summaries benefit and drawbacks on security and performance.

Table 1: Benefit and Drawbacks: On security and performance



Key factor	Impacts	
	Positive	Negative
Data governance security	Storing data, logs, credentials, easy management, data compliance and security.	Vulnerability to attacks
SLA	Always available, support backup	Downtime
Consistency and Reliability	better architecture for less effort elastic software	Manageability, Complexes very high for big application architecture, data breach.
Flexibility & Exit Strategy	Application modernization, powerful scalable computing services	Security and privacy, Limited control, and flexibility
Cost	Lower cost	Vendor lock-in

3.2 Four technological characteristics decision influence performance

This section describes four technological characteristics decision influencing performance which are relative advantage, trialability, complexity and compatibility according to(Morgan, L,2013). The relative advantage in terms of cost savings as users can pay as they need, rather than paying on an ongoing basis for the extra capacity. Moreover, the transition from permanent capital expenditures to operating expenses as a cost benefit. As the licensing costs, maintenance costs, tape support costs, electricity bills and air conditioning bills are saved. The compatibility Bandwidth and cloud connectivity are a major concern as are the actual performance and amenities available from the cloud provider. The complexity that's mean the system still needs more work in terms of related features, which is how employees consume or interact with the workflow in terms of retrieving summary data. However, this does take time, especially for small and medium-sized service providers. the trialability and analysis reveals that trialability is also the important factor impacting cloud adoption(Morgan, L,2013); (Seethamraju, R,2015).

4. Cloud computing management

There are many types of cloud computing services, allows Communication-as-a-Service (CaaS) by using some tools. For example, od these tools is Voice over IP (VoIP) and video conferencing also Instant Message. IaaS is a computer-as-a-service delivery so that allows customer to maintain the owner also manage applications that's during offloading infrastructure administration to the IaaS provider. MaaS (Monitoring as a Service) is dealing with external sources and third-party security services for a security team. PaaS is sending application model that is completely independent of the specific operating system is running on and dealing with. This means that it is only a web-based development infrastructure. SaaS typical vendor provides software over a network rather than being distributed for installation on individual computers. IT professionals uses several protocols and techniques to create cloud networks (Rittinghouse,2016). As of security over the network can talk about issues by beginning of this year 2020, everyone was using it, and know that zoom used VoIP protocols over the cloud computing power process, then there was some flaw inside the network which zoom let people let enter without any security checks, then there was some files vulnerability which zoom didn't check if it is genuine file or a worm, all this factor give zoom a very vulnerable position, which is a must have on SaaS layer and the protection data of user(Rittinghouse,2016).

5. The Proposed Model

This section focused on the concerns associated to the data security aspect, in cloud computing, such as data Confidentiality, data integrity and service availability. It's called a cloud security performance management model (CSPM) which ensures different aspect such as, cloud computing security, cloud performance, cloud management. Moreover, its present and describe the architecture of the suggested CSPM model. Then it will be defining the components and layers of CSPM model. The outcome and execution of the new proposed model will be examined, in appropriate way to present the security elements in the cloud computing, for example data confidentiality, data integrity and service availability. CSPM model permits users with different forms of queries for example, the exact match and the aggregation and the range query with the capability for storing verity kinds of data such as documents, pictures, file, video or audio. The main aims of the suggested new model are to increase security, avoiding the risks of hackers and intruder in the cloud. The security risks like data confidentiality, the data integrity and service availability and authentication will be studied in the model.

5.1 Overview of Cloud Model

Figure3.1. clarifies the overview of general cloud computing model. section A, illustrate the user sideways, which shows the user directs data inquiries to the server for example in Amazon Elastic File System (Amazon EFS) in section B. In section B the cloud is supposed to be confidential and secure so, the data source is stored on the cloud side, in order to ensure the reliability of privacy and security of query. A problem could occur when a cloud service loses its reliability.

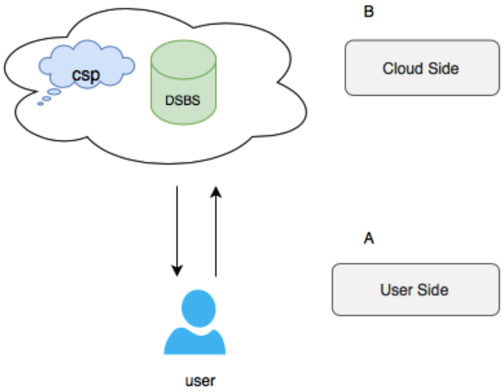


Figure1. overview in general cloud/user

5.2 The Proposed CSPM Model

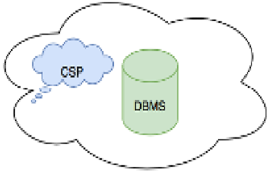
CSPM model provides cloud with database storage by Asymmetric encryption service provider and the use of a combined authentication process which distinguishes it from Amazon cloud service. CSPM model does not ensure and maintain the security with one authentication step.

It avoids the disadvantage effects of traditional authentication and send data in plain text. It reduced security risks against malicious and intruder insider in environment of cloud computing and decreases the disadvantage effect using encryption techniques(Faragallah, O.S.,2021);(Faragallah, O.S.,2020)CSPM model maintain the privacy and security of client's data using Asymmetric key approach. CSPM model handle processes run and managed by database management system DBMS with users and the cloud service providers (CSP). Table3.1 illustrates CSPM component in detail in our proposed model.

5.3 CSPM Component

It's clear from Table3.1 that CSPM model consist of several components such as user endpoint, cloud broker, standby cloud broker, DBMS in CSPM. Firstly, in the user component web browser display user interface for end user, secondly the endpoint manage communication between the system and the browser, thirdly the cloud broker handles queries between users and CSP and also retrieve responses that's from CSP to user's machines. Fourthly, the standby cloud broker is another cloud broker, if there is something happened for cloud broker, the endpoint recommunicates to the standby cloud broker. Finally, DMBS in CSPM, the CSP is responsible for storing the data in the cloud storage (for example Elastic File System (EFS) in Amazon that return the relevant to the DBMS that contains result of the user's query.

Table2: CSPM model's components

CSPM Component	Description
user	Web browser display user interface for end user
Endpoint	Endpoint accountable for dealing the communication with the browser and the system. generated interface of user that's using the implementation from the system to the server-side logic
Cloud Broker	The cloud broker mange the communication between user's machines and CSP.it handles queries between users and CSP and retrieve responses from CSP to user's machines
Standby Cloud Broker	Alternative component of cloud broker
 CSP DBMS	DBMS receives the rewritten user's query for CSP from cloud broker. CSP is accountable of storing data in cloud storage (such as Elastic File System (EFS) in Amazon, that return the relevant response that contains of the clint's query result to the cloud broker.
combined Authentication1	CAP1 user calls endpoint by token generated before the user login authentication then endpoint check if the user is valid and the payloads.
combined Authentication2	CAP2 occur on cloud broker handle the encryption query to the DBMS. so, in the cloud broker there is a checking point to do the query.

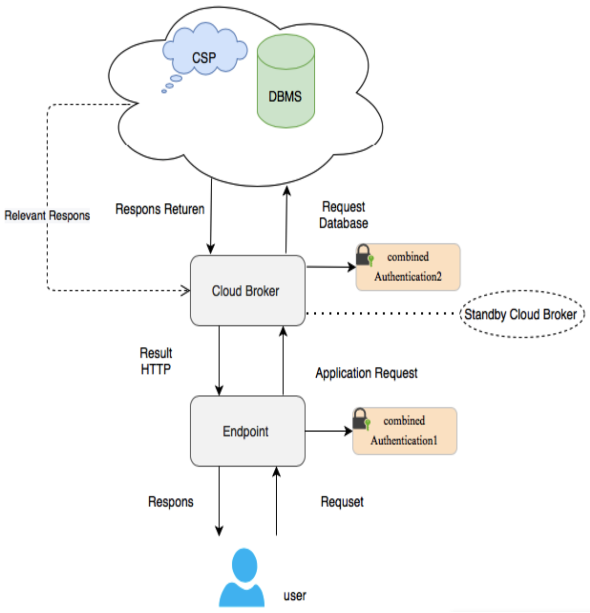


Figure 2. Overview CSPM model: combined Authentication1, combined Authentication2 will be explained in section combined Authentication prosses

5.4 CSPM Model Data Flow

This part shows the flowing of data in the CSPM model and shows the process of sending data to the DBMS then show how user executes queries via CSPM model in private and protected way to the could. Moreover, it describes how combined authentication methods proceed. CSPM combined authentication proses is more secure than traditional authentication techniques such as username and password.

- Sending data Procedure

As it is clear in Figure3.3, the user side send the query by the interface of the user and browser via HTTP request. The endpoint shows the main part of the connection in web browser and with the application. Then the query of user sent from the endpoint to cloud broker engine via an application request. The user's query encrypted by asymmetric-key algorithms. Which supposed to be secured and means to ensure the privacy of any user queries. So, when the query arrives to data source, the DBMS is responsible to survive the query then decrypt it and direct it to the CSP. Then, the outcome of the query backed to the DBMS, after that DBMS proceeds the query outcome to the cloud broker Engine and then the endpoint takings the outcome of the user's query to return it to the user interface.

The advantage of endpoint is the communication between the user browser and the cloud broker.

- Data Retrieval Procedure

This section describes data flow from DBMS to CSP. The user query arrives to DBMS in secure communication then users query will be sent from DBMS to CSP. The query always encrypted by asymmetric algorithm. After that, the appropriate result will be retrieved from CSP.

For example, the rewritten query was for CSP is to retrieve the range of all workers age from (20-50) and the confidential result is 20 in CSP. So upon receiving the query [fk(20), fk(50)], cloud provider process the query on the n data items (d1)k, · · · , (dn)k that's by checking which are fk(dj) (20 ≤ j ≤ 50) satisfies the condition fk(20) ≤ fk(dj) ≤ fk(50). Based on achieve maintaining property of the function fk, dj ∈ [20,50] if and only if fk (20) ≤ fk(dj) ≤ fk (50). Thus, the cloud provider just essentials to return all the encrypted data elements who's the hash values fk are in the range [fk (20), fk (50)]. Another example is the aggregation queries that's means calculates aggregations such as SUM, COUNT, MAX, MIN, and AVG, the rewritten query for CSP is to retrieve COUNT (number) of products whose price is greater than 500.

After retrieving the relevant set from the CSP, the database calculates the confidential result of sending the public key to the user over the private and protected network. The public key using way can be applied to implement the varieties type of queries for example the aggregation, the exact match, and the range query.

5.5 Combined Authentication process

This section shows the combined authentication process for the CSPM model. CSPM model consists of combined authentication prosses1 (CAP1) as it is clear in figure3.3. And combined authentication proses 2(CAP2) as it is clear in figure3.4. The combined authentication process in CSPM model is more secure than traditional authentication techniques such as username and password. In CAP1, the user calls the endpoint with a token generated before by the user login authentication then endpoint check if the user is valid and the payloads.

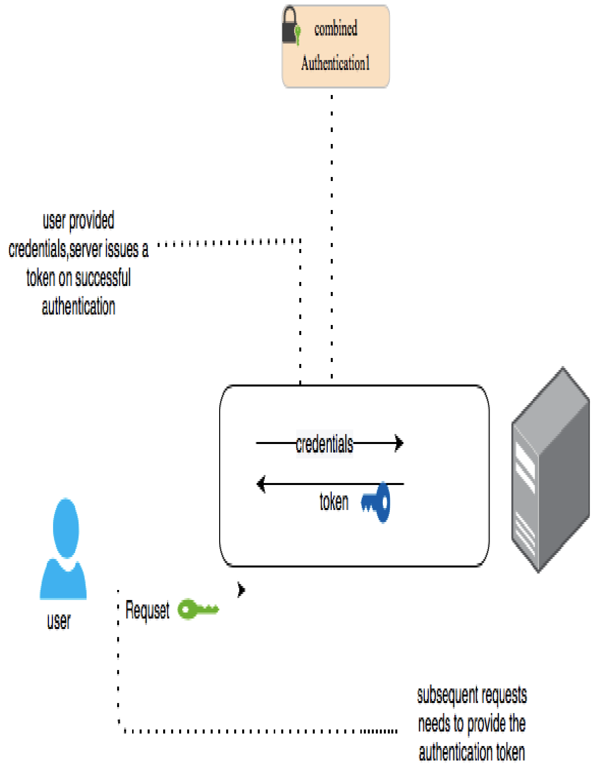

combined
Authentication1
user provided credentials,server issues a token on successful authentication
credentials
token
user
Requset
subsequent requests needs to provide the authentication token

Figure3. Combined authentication proses 1

CAP2 occurs on cloud broker layer which handle the encryption query to the DBMS. therefore, in the cloud broker there is an extra checking point, to do the user query in asymmetric encryption algorithm which uses the private key and public key to ensure the transfer security layer. Finally, the creation and saving of fingerprint are evaluated by user authentication which verify the file fingerprint checksums, which allow later to check if all files are retrieves correctly or missing, for the fingerprint in our case we use sha512 digest checksum.

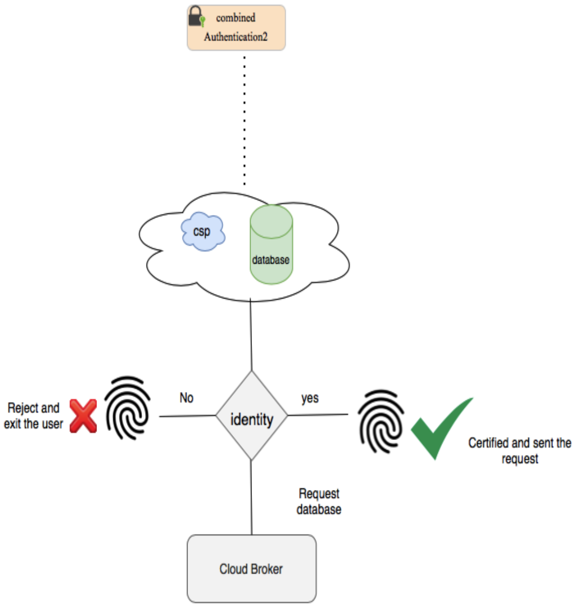


Figure 4. Combined authentication proses 2

6. Analysis and Experimentation

This section presents the CSPM model in practical way. The goal of this experiment is to address cloud security, cloud performance and cloud management. Firstly, this section explains CSPM scenario with its components works. Secondly, in relation to cloud security, this section examines and compare CSPM model with amazon cloud service model in the data confidentiality, data integrity, and the service availability. Thirdly, in relation to cloud performance, this section summaries the experimentation of our new suggested model. The experiment for studying efficiency and performance of the CSPM model and to show the procedures of storing data and retrieving data.

6.1 CSPM Scenario

In our proposed model, CSPM stores data in single cloud provider. The user send query (assuming the data encrypted by asymmetric key). We assuming to store data encrypted with the asymmetric encryption technique using RSA algorithm. Which means that there are two keys will be generated to the file. So, encryption is executed to the file to be ready for uploading on the cloud servers. Then after data uploaded, the holder gets overall detail such as time of uploading, the date, and the hash that generated of the file and certification. User catch the file in encrypted shape then decrypted using private key. The public and private key was generated on the time of encryption.

For the queries, we can use combined authentication for example fingerprint digest, if fk(age) => sha1 digest, use that digest in return compare the user input to verify the exact query as if the sha1 of fk(age) == sha1. The digest fingerprint checking could be like this, fk (age, uniqueID), the age will be saved as sha1 fingerprint on the database with the uniqueID can be anything else where need to be a fixed value. We argue our CSPM model more secure than traditional such as username and password.

6.2 Data Security Analysis

This section describes data security analysis in our proposed model. Also, a comparison of our proposed CSPM model with Amazon cloud service will be given as following:

- **Data confidentiality**

Data confidentiality is one of the security risks that can occur with a cloud provider, for example Amazon cloud service password hacked (Garfinkel, S.,2007); (AlZain, M.A.,2011). CSPM model based on asymmetric encryption with public and private key that is implemented to ensure data confidentiality. Firstly, the encrypted data with asymmetric encryption key which is creation of public and private key. Then stored data encrypted on cloud servers. So, even if there is any, malware or viruses acquire the data they are not capable to access the data because they cannot get key. So, this way keeps the data confidential and secure with other clients. Moreover, what distinguishes the proposed model than amazon is that it uses combined authentication techniques that's makes attack more difficult to occur. As some of the service providers in Amazon are still using the traditional method of authentication, which is a username and a password. And it is easy for hackers to crack password and access data.

- **Data integrity**

Data integrity considers as a factor associated critical issues of cloud security threats. The stored data could expose damage during transfers to or from the cloud storage provider Attack risks must be taken into consideration both from inside and outside the cloud provider. So, the most main approach of the data cannot be modified by any other even users or intruder. As explained before, the comparison between our proposed CSPM model and Amazon cloud service used the asymmetric encryption. Moreover, the use of combined authentication may take time but we arguers it's more secure than traditional authentication such as username and password or single authentication. So, by this way CSPM model can ensure the integrity of the data is maintained. See figure 3.3 and figure 3.4 for CAP1 and CAP2.

- **Service Availability**

Availability is considering a reoccurring and a growing concern in cloud. Fundamentally, the role of availability is to determine the time that the system running correctly so, the period of time needs to be analyzed. The licensing agreement of Amazon mentions the unreachability of the service could occur in the Amazon

Company(Garfinkel, S.,2007). Whereas Amazon in the event of any damage to any Amazon web service there will be no compensation from Amazon.

According to the result of data security which are data confidentiality, data integrity, and service availability, our newly suggested CSPM model enhance the CIA security elements more than in the Amazon cloud service provider. Moreover, it's ensured confidential and protect user's data from unauthorized access with combined authentication technique and encrypt the stored user's data in the cloud. Amazon cloud service request the clients to encrypt their data before storing procedure, whereas CSPM model take care of this task.

6.3 Experiment and Evaluation

This part clarifies the experimentation to study the CSPM model. The experiment done by Java language to show and describe storing of data and data retrieval. The experiment provides evaluation of different kinds of queries, such as exact match, range and aggregate query.

- **Data storing procedure**

Data storing in CSPM model includes deliver data from the source to cloud service providers. Amazon cloud service requests the company to encrypt before storing data. The difference with Amazon and CSPM in time of storing data, obviously combined authentication will affect in the cost and time. But this never contradict our contribution to ensure the privacy and integrity of clints' query through process of the data retrieval. We implement experimentation for data storing procedure in CSPM model using constant data size 1MB, 5MB, 10MB. Figure 4.1, 4.2 and 4.3 illustrate the time cost for the data storing procedure for each data size and Figure 4.4 illustrate comparison of time cost for the data storing procedure of three size 1MB, 5MB, and 10MB altogether.
If the cloud operations considered the load balancing, SLA and Virtual Machine (VM) migration intact resulting the service availability will be better.

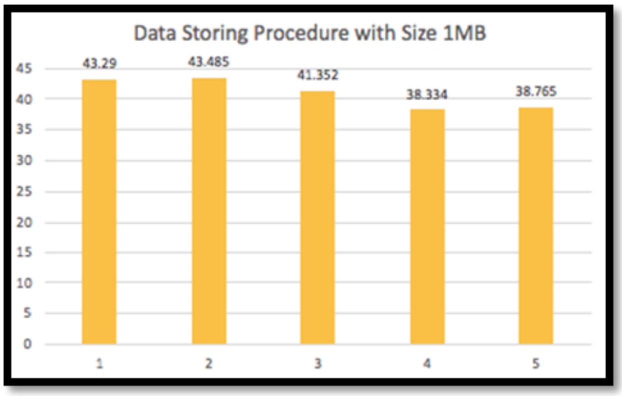


Figure5. Data storing with size 1MB.

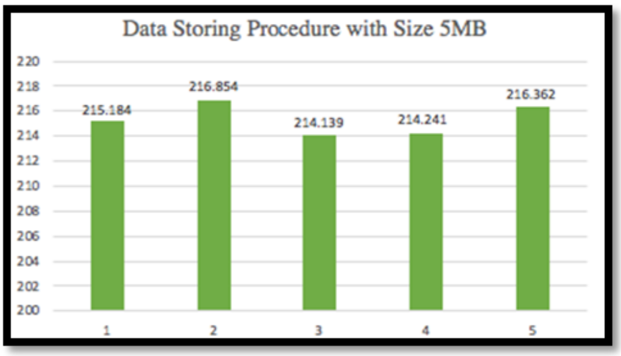


Figure 6. Data storing with size 5MB.

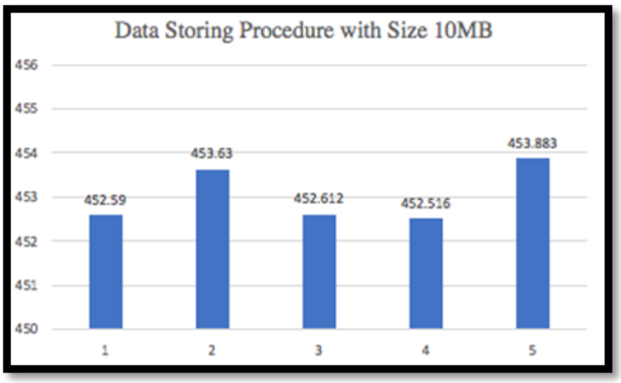


Figure7. Data storing with size 10MB.

Figure 4.4. demonstrates that the cost of time for performing data storing procedure increases as the size of data increases and decreases if the size is reduced.

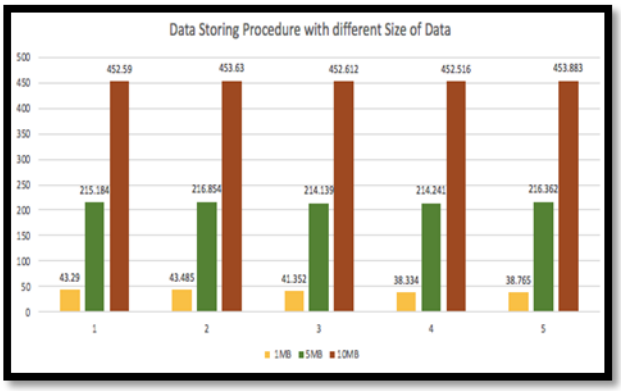


Figure8. Data storing procedure compression between three size 1,5 and 10MB.

- **Data retrieval procedure**

In the side of data retrieval, we perform varies forms of queries like the aggregation, the exact match, and the range query in CSPM model which is different with Amazon cloud service provider. These varies forms of queries distinguish the CSPM model with Amazon cloud service. The procedure of data retrieval in the CSPM model begin with rewriting the clint's query in the DBMS and then send this query to CSP after decryption retrieval to user. In Figure 4.5 example, evaluate time in aggregation type of query inside CSPM model with three size of data 1MB, 5MB and10MB. The cost of time for the aggregation query procedure increases with the size of data increase and reduce if the size reduced.

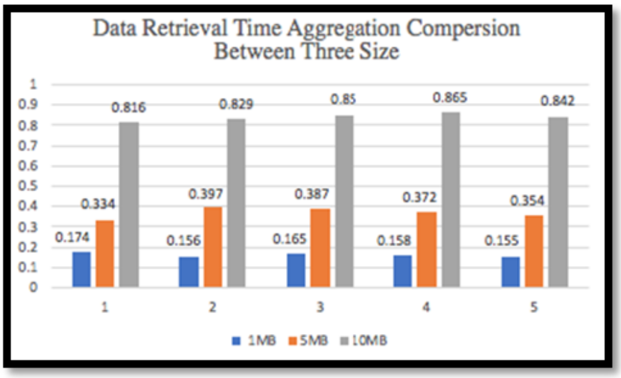


Figure 9. Aggregation comparison between three size (1MB,5MB,10MB)

In Figure4.6 example, it evaluates time in exact match type of query inside CSPM model. The time cost for the exact match type procedure at a speed of varying and converging, except in the case of a very large size it rises with the size of data.

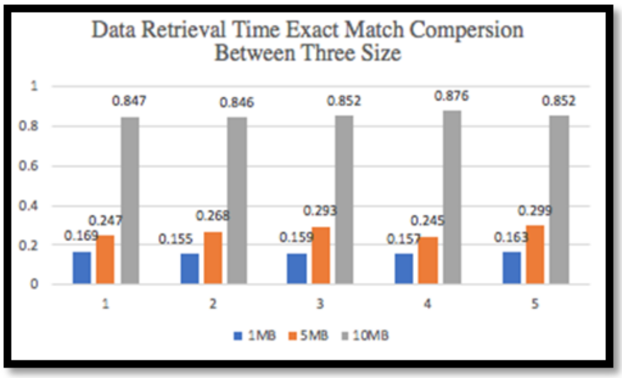


Figure10. Exact Match comparison between three size (1MB,5MB,10MB)

In Figure4.7example, evaluate time in range type of query inside CSPM model in different type of size which are 1MB,5MB and 10MB. The cost of time for the range query procedure increases with the size of data increase and reduce if the size reduced.

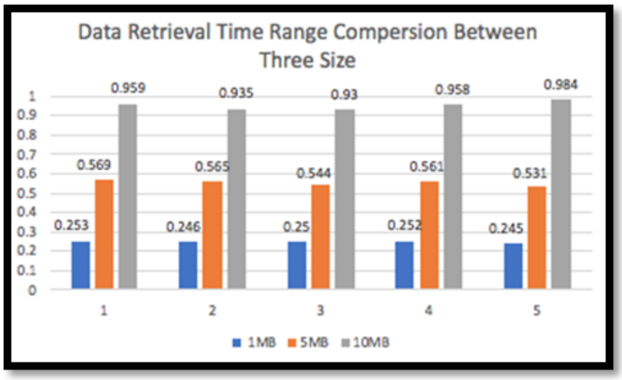


Figure11. Range comparison between three size (1MB, 5MB, 10MB)

In Figure4.8example, evaluate time in three types of query which are the aggregation, exact match, and range query inside CSPM model with size 1MB data. The time cost for the three type of queries procedure shown the highest period in range query.

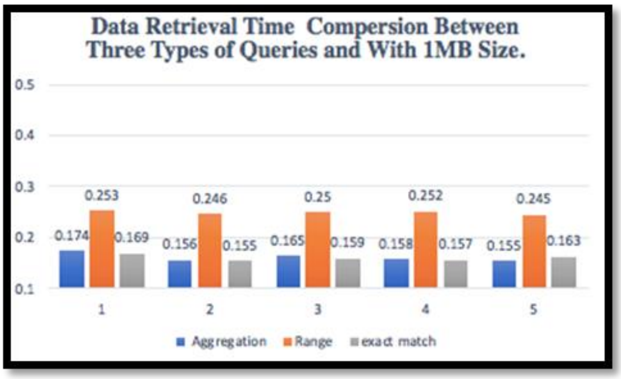


Figure12. comparison between three types of queries with 1MBsize of data.

In Figure4.9example, evaluate time in three types of query which are the aggregation, exact match, and range query inside CSPM model with size 5MB data. The time cost for the three type of queries procedure increase when size of data increase so, the cost of time shown the highest period in range query. But in aggregation type we found it query outperform the exact match as it is clear in Figure4.9.

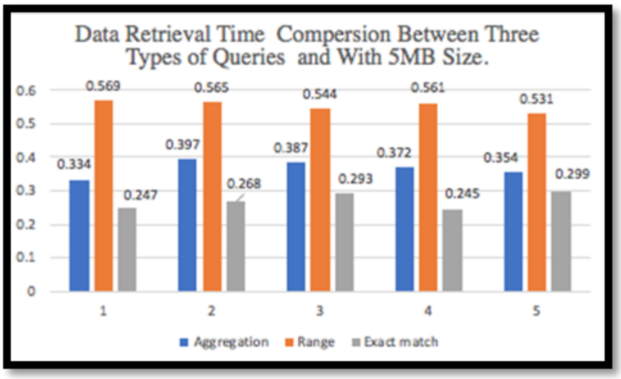


Figure13. comparison between three types of queries with 5MBsize of data.

In Figure4.10example, evaluate time in three types of query which are the aggregation, exact match, and range query inside CSPM model with size 1MB data. The time cost for the three type of queries procedure increase when size of data increase so, the cost of time shown the highest period in range query. But in aggregation type we found it query outperform the exact match and range as it is clear in Figure 4.10.

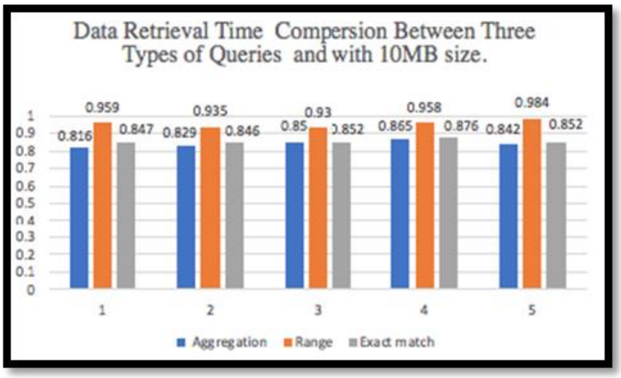


Figure14. Comparison between three types of queries with 10MB Size of Data.

Based on what analyzed, we found that when the data increased the time in inquiries also increased, as we also found the fastest query is exact much query. Figure 4.11. illustrate the comparison average between three type of queries the aggregation, the exact match, and the range query inside CSPM model with size 1MB,5MB,10MB.

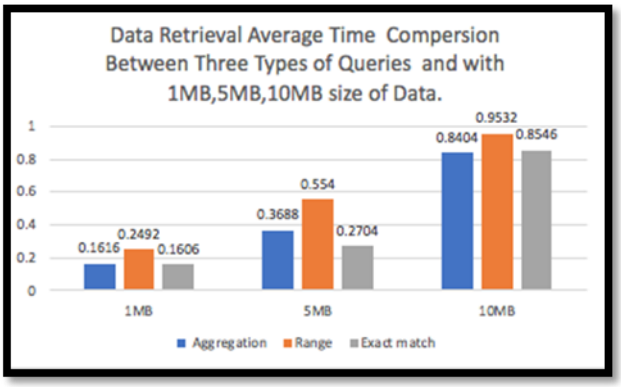


Figure 15. Comparison average time of three type of queries with size 1MB,5MB,10MB

7. **Conclusion and future work**

Cloud computing offers great potential for improving productivity and reducing costs. Cloud computing is subject to continuous development to provide different levels of services on demand to customers. As customers enjoy the services and benefits of cloud computing, cloud security is a major challenge. As there are still many security holes in the clouds, the hackers continue to exploit these vulnerabilities. The point of this research is proposed new model namely CSPM model which use asymmetric algorithm encryption and combined authentication prosses. Furthermore, it is examined the architecture and discussed components of CSPM model and layers. The goal of CSPM model is to decrease the risk of security that's happens in cloud computing and adopts the issues that associated with CIA security. At this phase we compared our combined authentication proses in our suggested model with Amazon cloud service as traditional authentication cloud model. And some experiment of store and retrieval data with varieties of size of data. In the future work we scheme and proposal to compare our suggested model with other models, systems, and cryptography algorithms to go extra in our evaluation until become the better and developed our model. So, we will in line to provide to the efforts in examining risks of cloud security and the countermeasures to cloud security breaks.

References

1. Alkhater, N., R. Walters, and G. Wills, *An empirical study of factors influencing cloud adoption among private sector organisations.* Telematics and Informatics, 2018. **35**(1): p. 38-54.
2. AlZain, M.A., B. Soh, and E. Pardede. *Mcdb: using multi-clouds to ensure security in cloud computing*. in *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*. 2011: IEEE.
3. AlZain, M.A., et al. *Cloud computing security: from single to multi-clouds*. in *2012 45th Hawaii International Conference on System Sciences*. 2012: IEEE.
4. Armbrust, M., et al., *A view of cloud computing.* Communications of the ACM, 2010. **53**(4): p. 50-58.
5. Basu, S., et al. *Cloud computing security challenges & solutions-A survey*. in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*. 2018: IEEE.
6. Basu, S., et al. *Cloud computing security challenges & solutions-A survey*. in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*. 2018: IEEE.
7. Bhasha, A.C., Balamurugan, K. End mill studies on Al6061 hybrid composite prepared by ultrasonic-assisted stir casting. Multiscale and Multidiscip. Model. Exp. and Des. (2020). https://doi.org/10.1007/s41939-020-00083-1
8. ChinnamahammadBhasha, A., Balamurugan, K. Studies on Al6061nanohybrid Composites Reinforced with SiO_2/3x% of TiC -a Agro-Waste. Silicon (2020). https://doi.org/10.1007/s12633-020-00758-x
9. D. A. Shafiq, N. Jhanjhi and A. Abdullah, "Proposing A Load Balancing Algorithm For The Optimization Of Cloud Computing Applications," 2019 13th International Conference on Mathematics, Actuarial

Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-6, doi: 10.1109/MACS48846.2019.9024785.

10. D. A. Shafiq, N. Z. Jhanjhi, A. Abdullah and M. A. Alzain, "A Load Balancing Algorithm for the Data Centres to Optimize Cloud Computing Applications," in IEEE Access, vol. 9, pp. 41731-41744, 2021, doi: 10.1109/ACCESS.2021.3065308.
11. Faragallah, O.S., et al., *Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication.* Journal of Ambient Intelligence and Humanized Computing, 2021: p. 1-25.
12. Faragallah, O.S., et al., *Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications.* IEEE Access, 2020.
13. Garfinkel, S., *An evaluation of Amazon's grid computing services: EC2, S3, and SQS.* 2007.
14. Gupta, P., A. Seetharaman, and J.R. Raj, *The usage and adoption of cloud computing by small and medium businesses.* International Journal of Information Management, 2013. **33**(5): p. 861-874.
15. Hogan, M., et al., *Nist cloud computing standards roadmap.* NIST Special Publication, 2011. **35**: p. 6-11.
16. Iosup, A., et al., *Performance analysis of cloud computing services for many-tasks scientific computing.* IEEE Transactions on Parallel and Distributed systems, 2011. **22**(6): p. 931-945.
17. Khayer, A., et al., *Cloud computing adoption and its impact on SMEs' performance for cloud supported operations: A dual-stage analytical approach.* Technology in Society, 2020. **60**: p. 101225.
18. Kumar, P.R., P.H. Raj, and P. Jelciana, *Exploring data security issues and solutions in cloud computing.* Procedia Computer Science, 2018. **125**: p. 691-697.
19. Latchoumi, T.P. and Kannan, V.V., 2013. Synthetic Identity of Crime Detection. International Journal, 3(7), pp.124-129
20. Liao, C., C.-C. Liu, and K. Chen, *Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model.* Electronic Commerce Research and Applications, 2011. **10**(6): p. 702-715.
21. Loganathan, J., Latchoumi, T.P., Janakiraman, S. and parthiban, L., 2016, August. A novel multi-criteria channel decision in co-operative cognitive radio network using E-TOPSIS. In *Proceedings of the International Conference on Informatics and Analytics* (pp. 1-6). https://doi.org/10.1145/2980258.2982107
22. Maqueira-Marín, J.M., S. Bruque-Cámara, and B. Minguela-Rata, *Environment determinants in business adoption of Cloud Computing.* Industrial Management & Data Systems, 2017.
23. Morgan, L. and K. Conboy, *Factors affecting the adoption of cloud computing: an exploratory study.* 2013.
24. Prodan, R. and S. Ostermann. *A survey and taxonomy of infrastructure as a service and web hosting cloud providers*. in *2009 10th IEEE/ACM International Conference on Grid Computing*. 2009: IEEE.
25. Ratten, V., *Cloud computing technology innovation advances: a set of research propositions*, in *Disruptive Technology: Concepts, Methodologies, Tools, and Applications*. 2020, IGI Global. p. 693-703.
26. Rittinghouse, J.W. and J.F. Ransome, *Cloud computing: implementation, management, and security*. 2016: CRC press.
27. Ryan, M.D., *Cloud computing security: The scientific challenge, and a survey of solutions.* Journal of Systems and Software, 2013. **86**(9): p. 2263-2268.
28. S. K. Pande, S. K. Panda, S. Das, K. S. Sahoo, A. K. Luhach et al., "A resource management algorithm for virtual machine migration in vehicular cloud computing," Computers, Materials & Continua, vol. 67, no.2, pp. 2647–2663, 2021.
29. Seethamraju, R., *Adoption of software as a service (SaaS) enterprise resource planning (ERP) systems in small and medium sized enterprises (SMEs).* Information systems frontiers, 2015. **17**(3): p. 475-492.
30. Subashini, S. and V. Kavitha, *A survey on security issues in service delivery models of cloud computing.* Journal of network and computer applications, 2011. **34**(1): p. 1-11.
31. Wang, C., et al. *Privacy-preserving public auditing for data storage security in cloud computing*. in *2010 proceedings ieee infocom*. 2010: Ieee.
32. Yeboah-Boateng, E.O. and K.A. Essandoh, *Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies.* International Journal of Emerging Science and Engineering, 2014. **2**(4): p. 13-20.
33. Zhang, X., et al. *Information security risk management framework for the cloud computing environments*. in *2010 10th IEEE international conference on computer and information technology*. 2010: IEEE.