Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume12, Issue 5, July 2021: 3288-3306

Research Article

Performance Evaluation and Analysis of CSPM: a Secure cloud Computing Model

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

Abstract

Cloud computing offers an innovative organization and user ability share, store and retrieve data anytime and from anywhere. Recently companies have increases to adopting cloud computing. The main concerns in adopting cloud computing about the security issues. The critical aspect in cloud computing is security due to privacy and sensitive information. As a lot of users in the company share confidential and critical data on a cloud so the important part is how the data be secured. This paper discusses overview of the cloud computing and presents proposes a cloud security performance management (CSPM) model. Presents experimentation and evolution based in performance in different data size. Applying asymmetric encryption by using RSA and ECC algorithm. Show scenarios between RSA vs ECC in storing and retrieval data inside proposed CSPM model. Presents CSPM Model-Store algorithm and CSPM Model-Retrieve algorithm.

Keywords: Cloud computing, cloud security, asymmetric encryption data, RSA algorithm, ECC algorithm.

1. Introduction

The definition of cloud computing is presented by the most popular definition by NIST: defined as a model enabling access to network for request to a common configurable group of computing supplies such as storing, applications and servers any time[1], [2],[3].

The cloud computing motivated the companies for adopting the cloud computing. Recently, companies around the world are increasingly using cloud computing[1]. The main benefit of using cloud computing is reducing the IT costs and increase the capabilities also reachability for delivered services[4],[5]. The concerns in adopting cloud computing about the security issues[6],[7],[8]. As a result of the essential of continues need for data security in the cloud computing. So, critical aspect in the cloud computing is security due to privacy and sensitive information[9]. A lot of companies share confidential and critical data on the cloud computing so the important is focus in the part of how the data be secured[10],[11],[12].

This paper focuses on issues relating to storing and retrieval data in secure cloud[1]. The worried side about CIA which are confidentiality, availability and integrity of data in the cloud from attacks and damage of cloud services[13],[14].

[1][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
Email: [abeer.fahad.alotaibi@hotmail.com, m.alzain@tu.edu.sa, mmasud@tu.edu.sa, noorzaman.jhanjhi@taylors.edu.my]

The remainder of this paper is organized as follows. Section 2 presents overview of cloud computing. Section 3 discussed CSPM model. Section 4 presents experiment and evaluation of CSPM mode. Section 5 discussed scenarios of CSPM model. Section 6 discussed Algorithms of CSPM model in data storing and retrieval. Section 7 will conclude the paper.

2. Overview of cloud computing

Cloud computing considered as next generation in various fields everyone from anywhere using cloud computing on a daily basis, such as Microsoft Office 365, Gmail Dropbox, Gmail, etc[15] . The main concept of the cloud computing is to reduce the continuous essential to maintain an internal data center. In addition to relocation the company or organization data to a remote site on the provide cloud site [16] , [7].

Cloud computing divided into three layers as it includes the first layer cloud computing deployment models which contains public cloud, private cloud, community cloud and hybrid cloud [13]. The second layer cloud computing characteristics which are on-demand self-service. After that broad network access, resource pooling which are establish resources that could be infrastructure, storage, platform, or data. The rapid elasticity that's provide the flexible provisioned[10]. The measure service and finally cloud computing delivery models which it's are software as a Service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Figure1. shows the cloud environment layers[13],[16],[17].

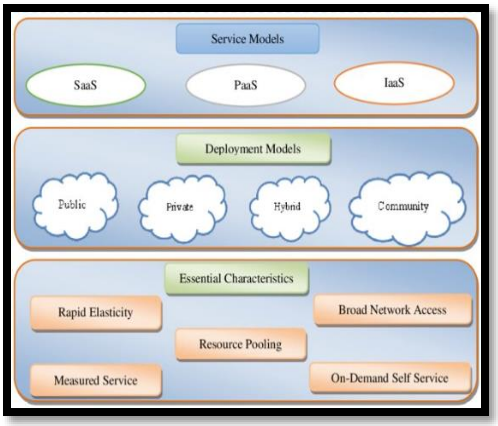

Figure1. Cloud Environment layers adopt from NIST [18]

3. CSPM Model

This section presents a secure model called CSPM model. It provides storing and retrieval data in secure cloud. This model store data by using asymmetric encryption algorithm which have public and privet key and using combined authentication process in two stages which distinguishes it from traditional process.

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 intruder insider in environment of cloud computing and decreases the disadvantage effect using encryption techniques[19],[20],[21]. CSPM model contain of several components which are user, endpoint, cloud broker, standby cloud broker, DBMS in CSPM as clear. Two stages the first stage combined authentication process in endpoint side. Second stage combined authentication process 2 in cloud broker side. Figure2. illustrates CSPM model. Figure3. illustrates the CAP 1 in stage 1 and Figure4. illustrates CAP 2 in stage 2. More details regarding CSPM model can be found in our previous research[22].

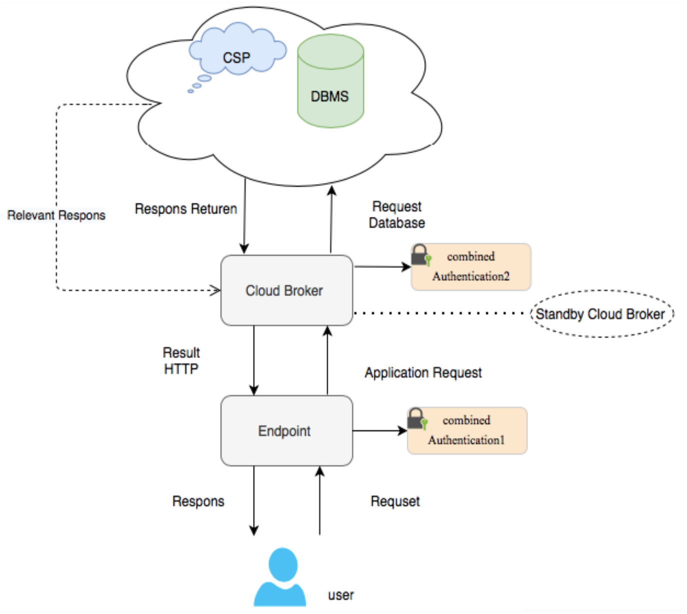

Figure2. Proposed CSPM model

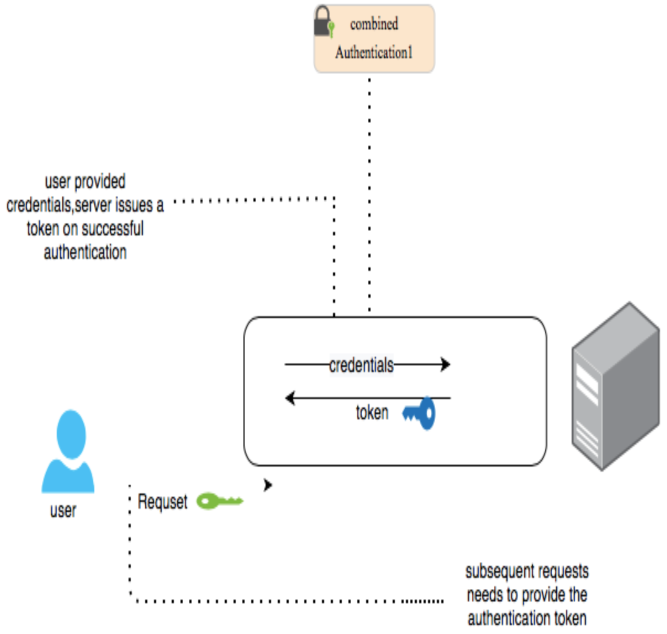

Figure3. Combined authentication proses 1

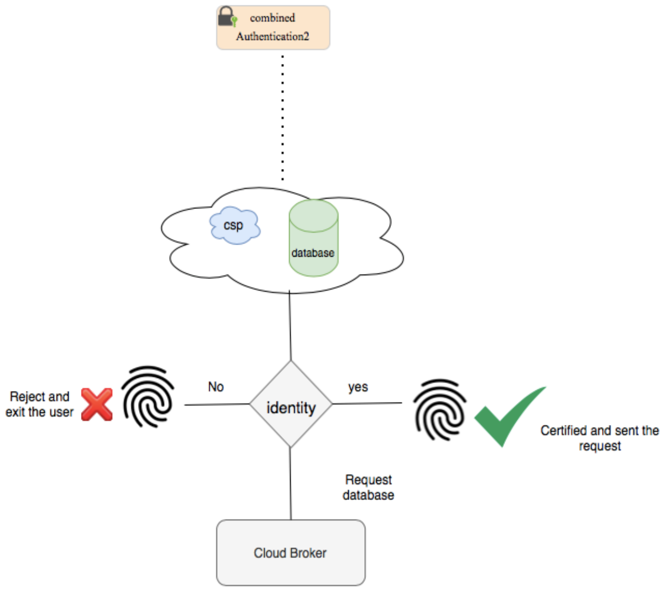

Figure4. Combined authentication proses 2

4. Experiment and Evaluation

This section describe experimentation between two techniques which are RSA asymmetric encryption and ECC encryption in different data size to make comparison based their performance. The experiment done by Java language to show and describe storing of data and data retrieval procedure. The experiment provides evaluation of different kinds of queries, such as exact match, range and aggregate query.

4.1 Data storing procedure

This section presents data storing procedure in CSPM model. The procedure begin from user sends data to store in cloud. we implement experimentation for data storing procedure in CSPM model using constant data size 1MB and 5MB by RSA and ECC asymmetric encryption.

Figure 5. and 6. illustrate the performance of the RSA data storing procedure for each data size and ECC data storing procedure for each data size as well.

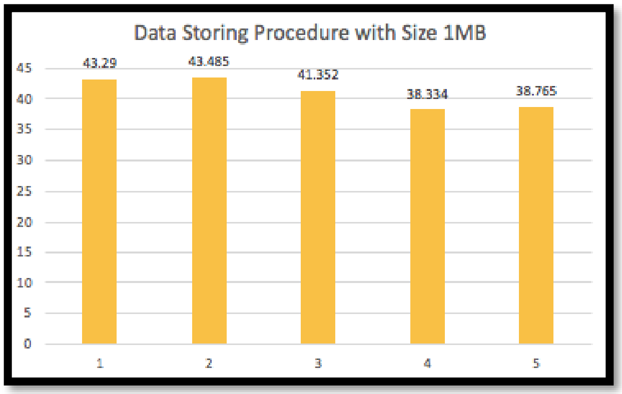

Figure5. RSA data Storing with Size 1MB.

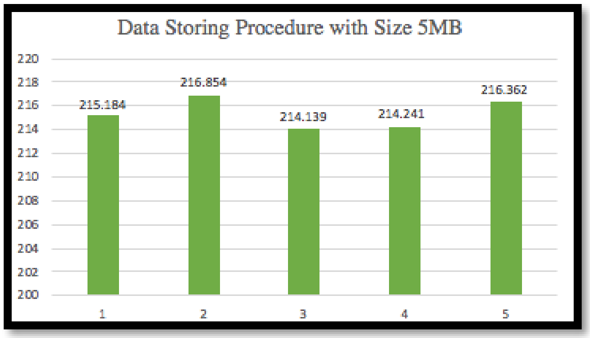

Figure6. RSA data Storing with Size 5MB.

The performing data storing procedure in RSA asymmetric encryption increases as the size of data increases and decreases if the size is reduced. Although the cost of time increases along with the increase in size of data, the increase will lead to improved level of security.

In Figure 7. and Figure 8. illustrate the performance for the ECC data storing procedure for each data size.

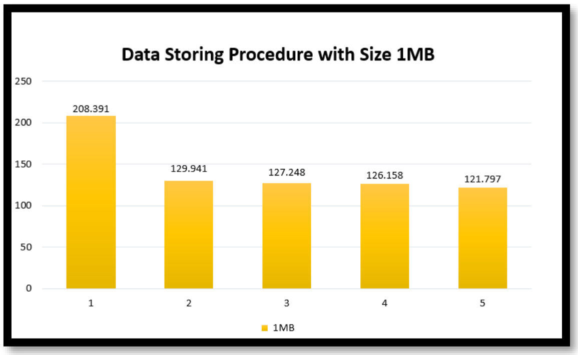

Figure7. ECC. Data Storing with Size 1MB.

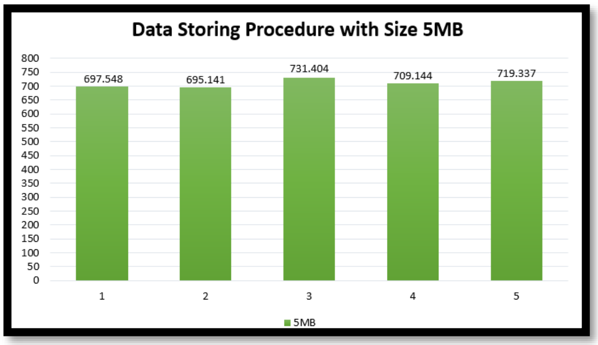

Figure8. ECC. Data Storing with Size 5MB.

Based in result we found in storing procedure
we found the RSA asymmetric encryption cost time faster than ECC asymmetric encryption.

4.2 Data retrieval procedure

This section presents data retrieval varies forms of queries such as the aggregation, the exact match, and the range query inside proposed CSPM model. The procedure of data retrieval in the CSPM model begin with user's query rewriting in the DBMS and then send this query to CSP after decryption retrieval to user. We perform the procedure of data retrieval by using RSA asymmetric encryption and ECC asymmetric encryption. Figure9. and Figure10. evaluate time in RSA aggregation type of query inside CSPM model with two size of data 1MB, 5MB. The cost of time for the aggregation query procedure increases with the size of data increase and reduce if the size reduced.

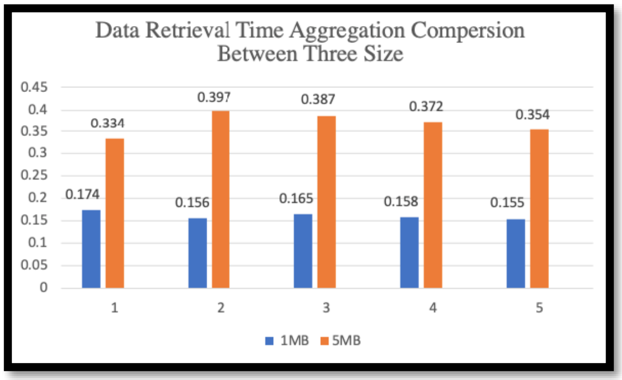

Figure9.RSA aggregation comparison between three size (1MB,5MB).

Figure10. evaluates time in RSA exact match type of query inside CSPM model.

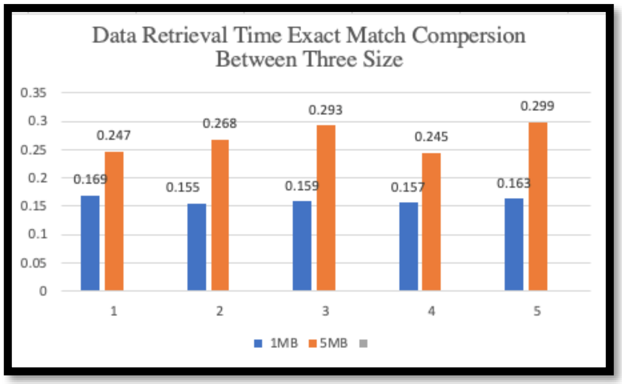

Figure10.RSA exact match comparison between three size (1MB,5MB).

Figure11. evaluates time in RSA range type of query inside CSPM model in different type of size which are 1MB, and 5MB. The cost of time for the range query procedure increases with the size of data increase and reduce if the size reduced.

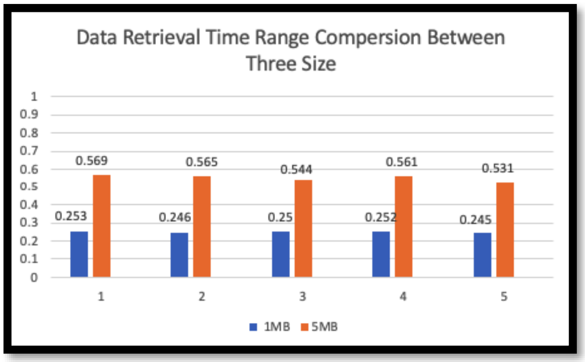

Figure11. RSA range comparison between three size (1MB,5MB).

In Figure12., time evaluation of three types of query in RSA which are the aggregation, exact match, and range query inside CSPM model with size 1MB data will be given. The time cost for the three type of queries procedure shown the highest period in range query.

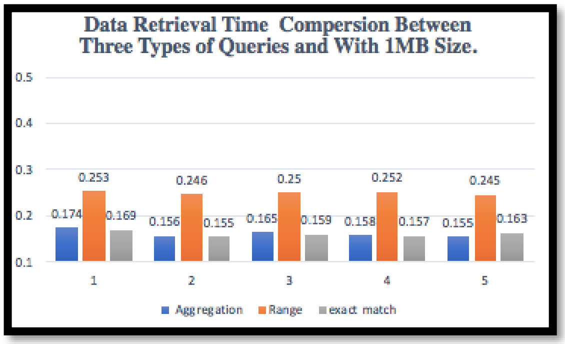

Figure12. Comparison between three types of queries in RSA with 1MBsize of data.

Figure13. evaluates time performance in three types of query in RSA 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 increases 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 Figure13.

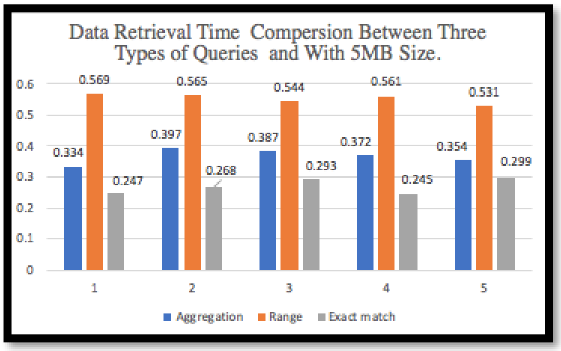

Figure13. Comparison between three types of queries with 5MBsize of data.

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 RSA exact much query.

Figure14. and Figure15, evaluate time performance in ECC exact match, aggregation and type of query inside CSPM model with two size of data 1MB and 5MB. The cost of time for the aggregation query procedure increases if the size of data increased and reduce if the size reduced.

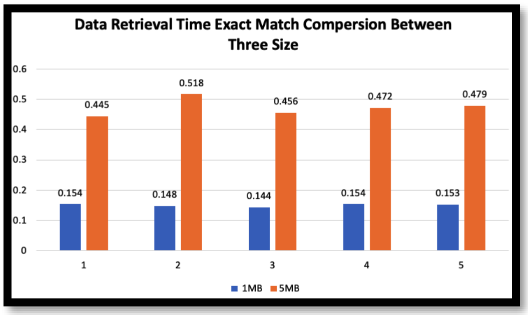

Figure14.ECC exact match comparison between three size (1MB,5MB).

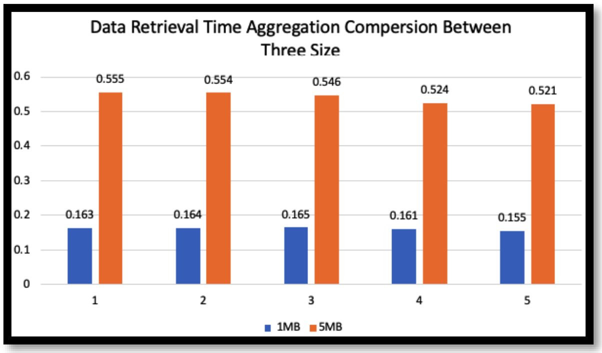

Figure15.ECC aggregation comparison between three size (1MB,5MB)

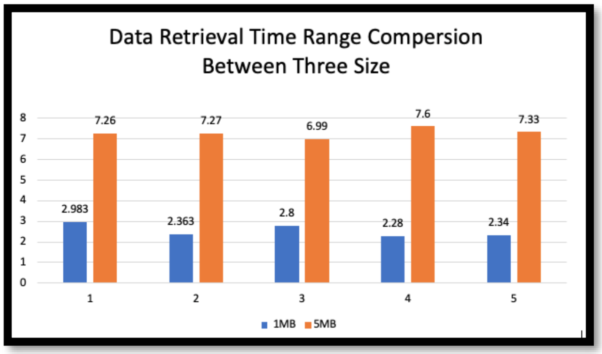

Figure16. ECC range comparison between three size (1MB,5MB)

In Figure17., it evaluate time performance in three types of query in ECC 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.

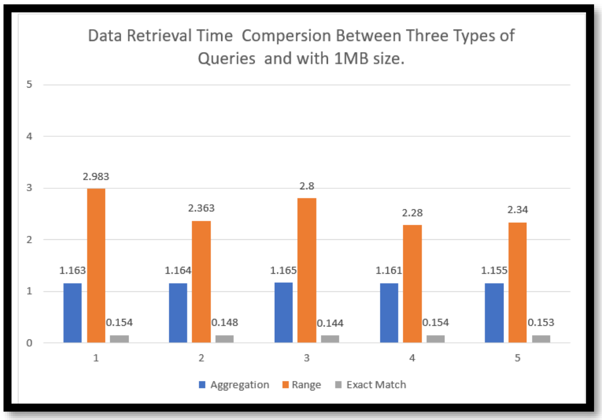

Figure17. Comparison between three types of queries in ECC with 1MB size of data.

In Figure18. example, it evaluate time in three types of query in ECC 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 increases when size of data increase so, the cost of time shown the highest period in range query.

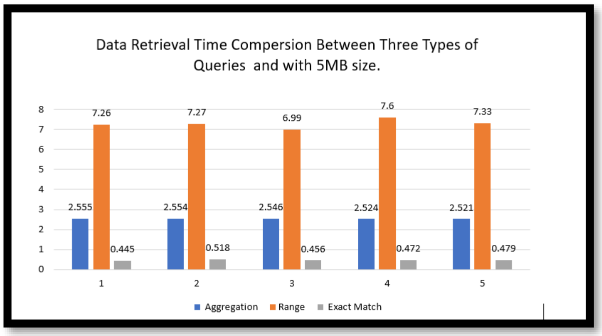

Figure18. Comparison between three types of queries in ECC with 5MB size of data.

5 CSPM Scenarios

This section presents several scenarios of CSPM model with RSA and ECC cryptographic models with the evaluation of the total objective of performance of CSPM model in the cloud computing environment. The experimentation is written by using Java language to simulate the performance of asymmetric cryptography in the cloud broker is placed on the user-side inside private cloud or the company network. CSPM model located on the user-side inside the company network. The experiments were executed on 32GB of RAM, quad-core up to 4.90 GHz, i7-10510U CPU connected to cloud serves provider that's to simulate data queries response from different location by using different data sizes such as 1MB, 5MB in the cloud environment.

The experimentation provides a comparison evaluation of two models: the RSA model using the asymmetric block cipher with public key and privet key[23],[24]. the ECC model elliptic curves cryptography is asymmetric technique block cipher with public key and privet key[25]. The main goal of comparison is to show the performance of using the RSA and ECC asymmetric cryptography in CSPM model in term storge and retrieval data inside our CSPM model.

5.1 Data Storage Performance (RSA vs ECC)

In this section we presents two different scenarios related data storage performance in the CSPM model with the two asymmetric cryptography RSA and ECC algorithms. Section 5.2 continue presents scenarios of data retrieval 3-5 related to data retrieval in CSPM model.

Scenario 1: Data storage procedure comparison between RSA asymmetric algorithm and ECC asymmetric algorithm inside CSPM model with data size 1MB. Figure 19 and 20 illustrate comparison of time cost between RSA and ECC data storing procedure for data size 1MB and 5MB.

Aim:

Scenario 1 shows the data storage procedure in the CSPM model. The objectives of this scenario are to presents the performance of data storage procedure by using RSA algorithm and ECC algorithm within proposed CSPM model in the cloud with data size 1MB. As clear in Figure19. illustrate comparison of time cost between RSA and ECC data storing procedure for data size 1MB with 5 cycle and the result shown by millisecond (ms).

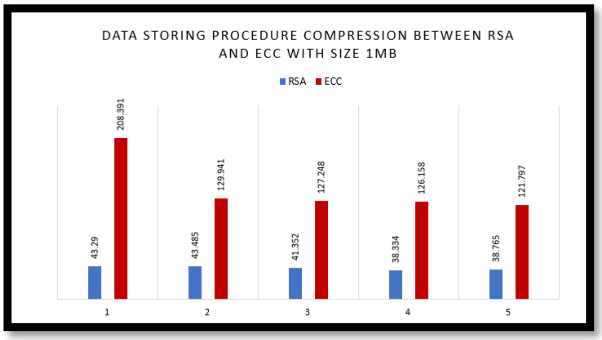

Figure19. Data storing procedure compression between RSA and ECC algorithm with size 1MB

Scenario 2: Data storage procedure comparison between RSA asymmetric algorithm and ECC asymmetric algorithm inside CSPM model with increase data size 5 MB.

Aim:

Scenario 2 Similar to Scenario 1 show the data storage procedure in the CSPM model but increases the size of data. The objectives of this scenario are to presents the performance of data storage procedure by using RSA algorithm and ECC algorithm within proposed CSPM model in the cloud with data size 5MB. As clear in Figure 20. It illustrates comparison of time cost between RSA and ECC data storing procedure for data size 5MB with 5 cycle and the result show by millisecond (ms).

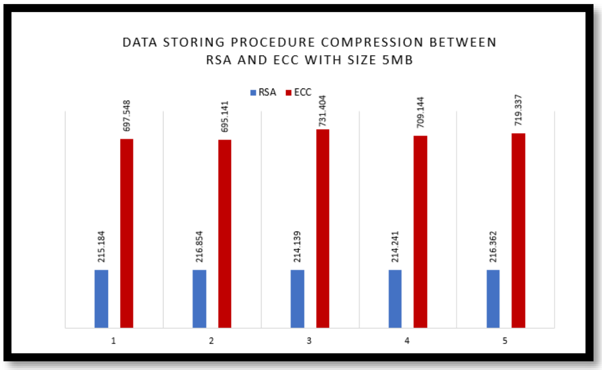

Figure20. Data storing procedure compression between RSA and ECC algorithm with size 5MB

Results and Discussion of Scenarios 1, 2 :

Based on result and analyze of scenario 1 and 2 with different size of data storage procedures. We did experimentation to simulate performance of data storage in the CSPM model with data size 1MB (Scenario 1) and the with size 5 MB in (Scenario 2) by using RSA and ECC models and both of two scenarios use asymmetric cryptographic techniques.

The RSA technique is asymmetric block cipher with public key and privet key was created in 1978 by Leonard Adleman, Ron Rivest and Adi Shamir. Asymmetric key encryption is used to distribute the key in a secure way [17]. However, ECC elliptic curves cryptography is asymmetric technique block cipher with public key and privet key was created by Koblitz and Victor Miller 1980s [25]. The Evaluation of results from Scenario 1 and 2 are used for the comparison based in performance in this section. the scenario begins from the user provide to storing data inside cloud. Receiver unit received the data from user to storing this data in the cloud. This is done in cloud broker encryption the data by asymmetric cryptography. We found that the RSA technique is much faster than the ECC technique in two scenarios with 1MB and 5 MB with 5 cycles in each scenario. Furthermore, the cloud virtual machine migration, load balancing process, and other cloud applications have [27-31] impact on it.

5.2 Data retrieval performance (RSA vs ECC)

This Section presents different scenarios in relation to the data retrieval performance in the proposed CSPM model with RSA and ECC technique.

The main idea is analyzing our CSPM model with different queries such as rang, exact much, aggregation and with different size of data such as 5MB.

In the side of data retrieval performance, we perform varies comparison forms of queries like the aggregation, the exact match, and the range query between RSA and ECC technique. The procedure of data retrieval in the CSPM model begin with rewriting the user's query in the DBMS and then send this query to CSP after decryption data inside cloud broker return the result of user's query. In scenario 3 ,4 and 5 evaluate the performance retrieval data comparison in RSA and ECC exact much type of query inside CSPM model with size of data 5MB.

The cost of time for the RSA exact much query procedure faster than ECC exact much query.

Scenario 3: Data retrieval procedure comparison the exact much query between RSA asymmetric algorithm and ECC asymmetric algorithm inside CSPM model with data size 5 MB.

Aims:

Scenario 1 show the data retrieval procedure inside the CSPM model. The objectives of this scenario are to presents the performance of data retrieval procedure by using RSA algorithm and ECC algorithm with exact much query within CSPM model in the cloud with data size 5MB. When the user sends exact much query how much the time takes in both techniques RSA and ECC. As clear in Figure21, the comparison of time performance between RSA and ECC data retrieval procedure for exact much query with data size 5MB. The shown result given in 5 cycle and the result presented by millisecond (ms).

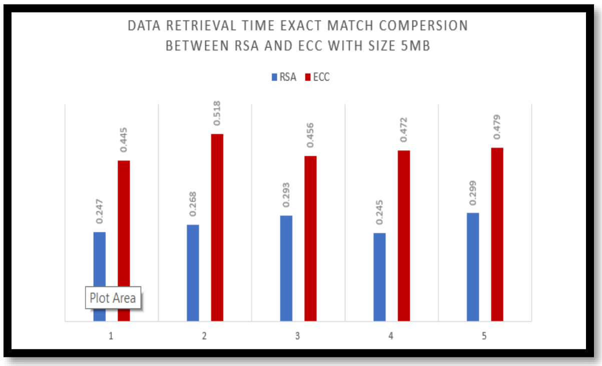

Figure21. Data retrieval time exact match comparison between RSA and ECC with size 5MB.

Scenario 4: Data retrieval procedure comparison the range query between RSA asymmetric algorithm and ECC asymmetric algorithm inside CSPM model with data size 5 MB.

<u>Aims:</u>

Scenario 4 Similar to Scenario 3, which show the data retrieval procedure inside the CSPM model. The objectives of this scenario are to presents the performance of data retrieval procedure by using RSA algorithm and ECC algorithm but with the range query and with same size of data with 5MB within CSPM model in the cloud. It discusses how much the time takes in both techniques RSA and ECC when user sends exact much query. As clear in Figure22. illustrate the comparison of performance between RSA and ECC techniques of data retrieval procedure with data size 5MB with 5 cycle and the result shown by millisecond (ms).

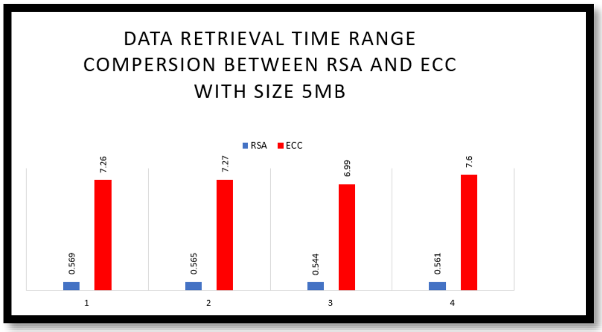

Figure22. Data retrieval time range comparison between RSA and ECC with size 5MB.

Scenario 5: Data retrieval procedure comparison the aggregation query between RSA asymmetric algorithm and ECC asymmetric algorithm inside CSPM model with data size 5 MB.

<u>Aims:</u>

Scenario 5 similar to scenario 4 and 3, which shows the data retrieval procedure inside the CSPM model. The objectives of this scenario are to presents the time performance of data retrieval procedure by using RSA algorithm and ECC algorithm but with the aggregation query and with same size of data with 5MB within CSPM model in the cloud. When the user sends exact much query, how much the time takes in both techniques RSA and ECC. As clear in Figure23. It illustrates the comparison of time performance between RSA and ECC techniques of data retrieval procedure with data size 5MB with 5 cycle and the result shown by millisecond (ms).

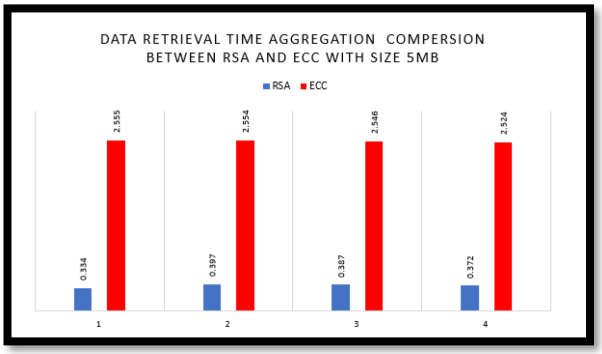

Figure23. Data retrieval time aggregation comparison between RSA and ECC with size 5MB.

Results and Discussion of Scenarios 3, 4 and 5:

Based on result and analyses of scenario 3, 4 and 5 with different queries of data retrieval procedures. We did our experimentation in the same size 5MB to simulate the performance of data retrieval in the CSPM model with exact much query in (Scenario 3) and with the range query in (Scenario 4) and with the aggregation query in (Scenario 5) by using RSA and ECC models . All scenarios using asymmetric cryptographic techniques.

as clear in pervious section The RSA technique is asymmetric block cipher with public key and privet key was created in 1978 by Leonard Adleman, Ron Rivest and Adi Shamir. However, ECC elliptic curves cryptography is asymmetric technique block cipher with public key and privet key was created by Koblitz and Victor Miller 1980.

The Evaluation of results from Scenario 3 ,4 and 5 in three queries exact much, range, and aggregation queries with size 5MB are used for the comparison based in performance in this section. The scenario begins from the user requested based in query to retrieval data from cloud. Retrieve the data from cloud to the concern user. This is done in cloud broker decryption the data by user's key public. We found the RSA technique is much faster than the ECC technique in three queries of retrieval. Table1: show the summery of five scenarios by using RSA and ECC cryptography to evaluated performance inside CSPM model.

Table1: Summery of performance scenarios 1-5.

Scenario	Performance metrics	Model type	Data size
Scenario 1	**Data storage**	RSA, ECC	1 MB
Scenario 2	**Data storage**	RSA, ECC	5 MB
Scenario 3	**Data Retrieval (exact much query)**	RSA, ECC	5 MB
Scenario 4	**Data Retrieval (range query)**	RSA, ECC	5 MB
Scenario 5	**Data Retrieval (aggregation query)**	RSA, ECC	5 MB

6 Algorithms

This section describes the data storing procedure (Algorithm 1) and the data retrieval procedure such as aggregation, exact much and rang (Algorithm 2).

6.1 Data Storing Procedure

In the CSPM model the data storing procedure include data from the data provider to cloud service provider to store into DBMS inside cloud. This is done after executing asymmetric encryption for

the data. Figure24. shows (Algorithm 1) the CSPM model-Store algorithm. The main idea of the CSPM model- Store algorithm starts from line 9 that's receive the data from the data provider or user to storing this data in the cloud. After that, the receiver unit inside the cloud broker received this data (line 11). This is done after check unit inside cloud broker check the validation of user. Then the key generation unit, generate the keys, public key and privet key, public key store it in data sours and privet key store it in user device in TPM “trust platform module” that located in user computer motherboard. The TPM “Trusted Platform Module " part of user computer motherboard, it's a chip designed for a secure hardware when integrate cryptographic keys. It’s stander for a secure and trust crypto processor. The major function of trusted platform module is storage, create keys and secure management for the cryptographic. Then, the encryption unit inside the cloud broker encrypted data inside of data storage. Figure 25. shows the sequential diagram of CSPM model storing data stage.
In the following acronyms algorithm will illustrated the acronyms used in the CSPM model-store algorithms: Cloud(C), user(U), key Generation Unit (KGU), Receiver Unit (RU), Sender Unit (SU), Check Unit (CU), Encryption Unit (EU), Decryption Unit (DU), Data(Da) and Data Storge (DS). LK length of keys, User Device (UD), Cipher Text (CT), Public Key (PuK), Privet Key (PrK).

Algorithm 1: CSPM Model-Store

```
1   Procedure CSPM Model -Store(Da)
2   Input:
3   Required modulus bit length of k. // Typical the bit of RSA key lengths
    are 1024,2048,3072,4096.
4   PuK // public key for each user
5   Da // data that should be submit by user in plain text PT form
6   Output:
7   CT // cipher text form stored in DBMS inside the cloud
8   Begin
9   U sends Da // user submit the data from user data device to cloud.
10  $CU \leftarrow U$ // check unit check the validation of cap2 exact much the
    authorize user inside cloud broker.
11  $RU \leftarrow Da$ // the data has been sent from user and received by RU inside
    cloud broker.
12  KGU Generate keys for each U // Before the encrypt data, Key
    generation should be done and each user have public key and private
    key
13  Select random two of distinct prime numbers A and B.

14  $N \leftarrow A * B$ // n is known as the modulus.

15  $Ø(N) \leftarrow [26]$. // calculate Euler’s totient function
16  $LK \leftarrow Ø(N)$ // Euler’s consider as length of key
```

```
Select an integer E. where 1 < E < Ø(N) & GCD of (E, Ø(N)) =1
Return E
PaK← E // The result of E released as public key of the user

D←modinv (E, LK) // D is a multiplicate of inverse of E mod Ø(n).
D ← $E^{-1} mod\ Ø$(N) // calculation D
PrK← D // The result of D released as Privet key of the user

DS sends PaK // Public key stored in data store
UD sends PrK // Privet key sends to user device
TPM store UD // In user device in motherboard there is a small chip
called trust platform module maintain privet key
EU← Da // data in plain text transfer it to encrypted unit to encrypted
data and conformant into cipher text form

EU← $C = Da^{PuK} mod\ N$ // calculate encryption equation

DS ← EU // after encrypted data then stored data in data storge

SU ← DS // Data storge unit sends cipher text to sender unit
SU sends CT to CSP into C // sender unit inside cloud broker sends
cipher text to cloud server provider inside the cloud
DBMS ← CSP into C // cloud server provider stored data in DBMS
inside cloud
  END
```

Figure24. CSPM Model-Store Algorithm

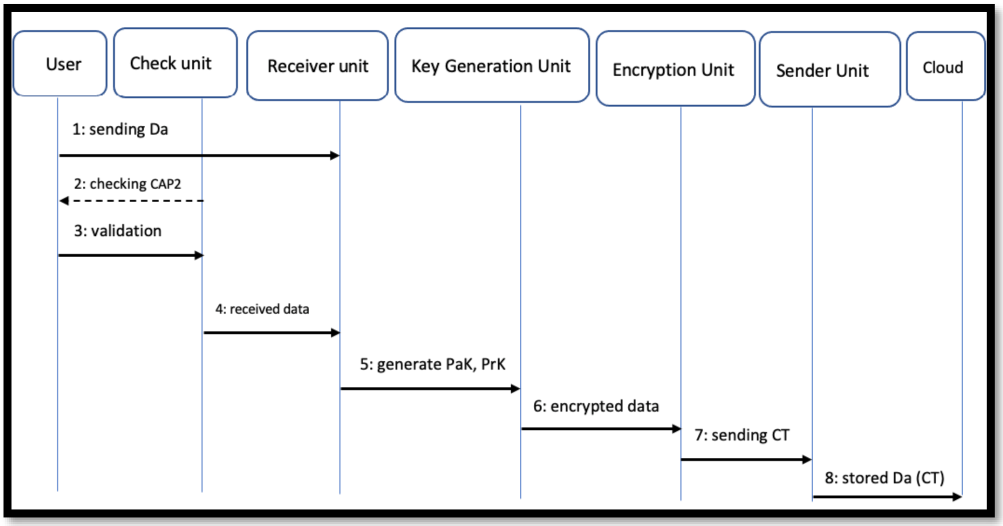

Figure25. Sequential diagram, CSPM model storing data stage.

6.2 Data retrieval procedure

In the CSPM model data retrieving process begins when the user request query to the cloud. User sends queries and received by the cloud broker. Figure26. shows (Algorithm 2) of the CSPM Model- Retrieve algorithm. The main idea of the CSPM Model- Retrieve algorithm start from (line 4) that's receive the query of user by receiver unit. This done after check unit inside the cloud broker check the user verification on CAP2. Then the sender unit sends the query to CSP. CSP rewriting the query and retrieved from DBMS. Then return result to decryption unit inside the cloud broker. Decryption Unit ask user to enter privet key to decrypt the query and sender unit return the result to user. Figure27. shows the sequential diagram of CSPM model retrieval data stage.

Algorithm 2: CSPM Model-Retrieve

```
1   Function CSPM-Model Retrieve (user query)
2   Input:
3   User's query
4   Output:
5   Result of user query
6   Begin
3   U sends Qu // user sends query, there are three types of queries (range, aggregation, exact much)
4   CU ← U // check unit check the validation of cap2 exact much the authorize user inside cloud broker.
5   RU ← Qu // received unit received user query
6   SU← RU // received unit pass the user query to sender unit
6   SU sends Qu to CSP // sender unit sends the query to cloud services provider to retrieve query
7   CSP rewriting Qu for DBMS // cloud serves provider rewriting the query and retrieved from DBMS
8   CSP return result (CT) // cloud serves provider return result in cipher text form
9   RU ← result (CT) // receiver unit inside cloud broker receives user's query
11  DU ← $Da = CT^{PrK} mode$ N // decryption unit received data in cipher form and calculate decryption equation
12  SU←DU // decryption unit after applied decryption equation sends query to sender unit
13  SU sends result Qu   // sender unit sends the result of query
14  Result // user gets the result of query
15  END
```

Figure 26. CSPM Model-Retrieve Algorithm

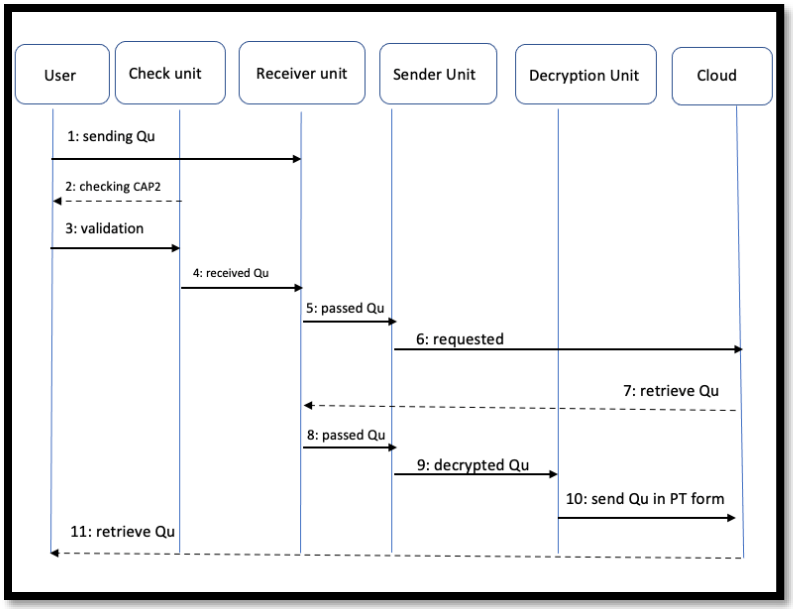

Figure 27. Sequential diagram, CSPM model retrieval data stage.

7 Conclusion and future work

Cloud computing offers great potential for improving productivity and reducing costs. There are still many security holes in the clouds, the attacker continues to exploit these vulnerabilities. The main key of this research is to analize the time performance of proposed new model namely CSPM model which use asymmetric algorithm encryption and combined authentication prosses. We did experimentation in storing and retrieval data inside proposed model. This research discussed some scenarios comparison between RSA and ECC asymmetric encryption in storing and retrieval data in different size.

In the future work we scheme and proposal to compare CSPM model with other models, systems, and cryptography algorithms in encryption and decryption other than the RSA and ECC. Also, we plan to apply our model in real environment in privet cloud and get more and reliable result. we will in line to provide to the efforts in examining risks of cloud security and the countermeasures to cloud security breaks.

8 References

1. 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.
2. Liu, F., et al., NIST cloud computing reference architecture. NIST special publication, 2011. 500(2011): p. 1-28.
3. Abeer F Alotaibi, et al., A Comprehensive Survey on Security Threats and Countermeasures of Cloud Computing Environment. Turkish Journal of Computer and Mathematics Education, 2021. 12 (9): p. 1978-1990.
4. Almorsy, M., J. Grundy, and I. Müller, An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107, 2016.

5. AlZain, M.A., et al. Cloud computing security: from single to multi-clouds. in 2012 45th Hawaii International Conference on System Sciences. 2012: IEEE.
6. Amara, N., H. Zhiqui, and A. Ali. Cloud computing security threats and attacks with their mitigation techniques. in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). 2017: IEEE.
7. Diaby, T. and B.B. Rad, Cloud computing: a review of the concepts and deployment models. International Journal of Information Technology and Computer Science, 2017. 9(6): p. 50-58.
8. 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.
9. G. K. Sodhi, G. S. Gaba, L. Kansal, E. Babulak, M. AlZain, S. K. Arora and M. Masud, Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code, Indonesian Journal of Electrical Engineering and Computer Science, 12 (2018), pp. 1297-1304.Padhy, R.P.,
10. Moghaddam, F.F., et al. Cloud computing: Vision, architecture and Characteristics. in 2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC). 2015: IEEE.
11. Masud, M., Hossain, M. Secure data-exchange protocol in a cloud-based collaborative health care environment. Multimed Tools Appl 77, 11121–11135 (2018). https://doi.org/10.1007/s11042-017-5294-5
12. Alzain, M.A. and E. Pardede. Using multi shares for ensuring privacy in database-as-a-service. in 2011 44th Hawaii International Conference on System Sciences. 2011: IEEE.
13. Panah, A., et al., Challenges of security issues in cloud computing layers. Rep. Opin, 2012. 4(10): p. 25-29.
14. AlZain, M.A., B. Soh, and E. Pardede, A survey on data security issues in cloud computing: From single to multi-clouds. Journal of Software, 2013. 8(5): p. 1068-1078.
15. S. Ibrahim et al., "Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps," in IEEE Access, vol. 8, pp. 160433-160449, 2020, doi: 10.1109/ACCESS.2020.3020746.
16. Shafiq, M., Ashraf, H., Ullah, A., Masud, M., Azeem, M., Jhanjhi, N. Z., & Humayun, M. (2021). Robust Cluster-Based Routing Protocol for IoT-Assisted Smart Devices in WSN. CMC-COMPUTERS MATERIALS & CONTINUA, 67(3), 3505-3521.
17. AlZain, M.A., B. Soh, and E. Pardede, A new model to ensure security in cloud computing services. Journal of Service Science Research, 2012. 4(1): p. 49-70.
18. Kumar, P.R., P.H. Raj, and P. Jelciana, Exploring security issues and solutions in cloud computing services–a survey. Cybernetics and Information Technologies, 2017. 17(4): p. 3-31.
19. M. Masud et al., "A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3047662..
20. Faragallah, O.-S., et al., Efficient Three-Dimensional Video Cybersecurity Framework Based on Double Random Phase Encoding. Intelligent Automation \& Soft Computing, 2021. 28(2): p. 353--367.
21. Mehedi Masud, Mamoun Alazab, Karanjeet Choudhary, Gurjot Singh Gaba, 3P-SAKE: Privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks, Computer Communications, 2021

22. Abeer F Alotaibi, et al., CSPM: A Secure Cloud Computing Performance Management Model. Turkish Journal of Computer and Mathematics Education, 2021. 12(9): p. 2114-2127.
23. Milanov, E., The RSA algorithm. RSA Laboratories, 2009: p. 1-11.
24. Kalpana, P. and S. Singaraju, Data security in cloud computing using RSA algorithm. International Journal of research in computer and communication technology, IJRCCT, ISSN, 2012: p. 2278-5841.
25. Koblitz, N., Elliptic curve cryptosystems. Mathematics of computation, 1987. 48(177): p. 203-209.
26. Al-Daraiseh, A.A., et al., Social networks' benefits, privacy, and identity theft: KSA case study. Soc. Networks, 2014. 5(12): p. 129-143.

27. 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.
28. 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), 2019, pp. 1-6, doi: 10.1109/MACS48846.2019.9024785.
29. 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), 2019, pp. 1-6, doi: 10.1109/MACS48846.2019.9024785.
29. S. Ali et al., "Towards Pattern-Based Change Verification Framework for Cloud-Enabled Healthcare Component-Based," in IEEE Access, vol. 8, pp. 148007-148020, 2020, doi: 10.1109/ACCESS.2020.3014671.
30. Z. A. Almusaylim, N. Zaman and L. T. Jung, "Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment," 2018 4th International Conference on Computer and Information Sciences (ICCOINS), 2018, pp. 1-5, doi: 10.1109/ICCOINS.2018.8510588