International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

A Retrospect of Prominent Cloud Security Algorithms

Ahmed Alrehaili, Aabid Mir, Mir Junaid

Abstract - The concept of Cloud Computing has been distinguished as one of the major computing models in recent years. This distinguish comes as a reflection of a rapid and intense interest from academic and industrial organisations which present it as an active area of research. Security has been always raised as one of the most critical issues of cloud computing where resolving such an issue would result in a constant growth in the use and popularity of cloud. Furthermore, issues related to service availability and interoperability has gained a substantial interest. Failing to address such issues would jeopardise consumers' satisfactions. This article mainly discusses the causes of obstacles and challenges related to security, reliability, privacy and service availability. In this work, we analyse and compare the performance of selected algorithms over "Google App Engine" which is a web framework and could computing platform. A comparative analysis of the efficiency of Advanced Encryption Standard "AES" (Rigndael), Rivest-Shamir-Adleman "RSA" and Triple Data Encryption "DES" have been performed locally and over the cloud as well. The efficiency analyses covered encryption and decryption procedures separately. Experiments results are given to analyses the effectiveness of each algorithm. The results show that Triple DES manifested a higher time efficiency ratio over cloud when subjected to different data loads compares to AES and RSA.

Keywords: Cloud Computing, cloud security, security threats, challenges, service availability.

I. INTRODUCTION

In recent years, cloud computing has been regarded as one of the most popular computing platforms in the field of information technology. It came as a consequence of developments in previous computing paradigms which include parallel computing, grid computing, distributed computing, etc. [1][2]. This evolutionary technology enables its users to deploy a connection to a network of computing resources in an effortless fashion, where users can rapidly scale up or down their demands with trivial interaction from service provider [1].

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Ahmed Alrehaili, FCIS, Islamic University in Medina, KSA. Email: ahmed_murayshid@hotmail.com
Aabid Mir*, MIIT, University of Kuala Lumpur, Malaysia. Email: miraabid@gmail.com
Mir Junaid, Laboratoire de Modelisation et Surete des Systemes (LM2S), Université de Technologie de Troyes, France. Email: mir.jnd@gmail.com

Cloud computing provides its consumers with three fundamental service models:

A. Software as a Service (SaaS)

This service is mainly intended to end users who need to use software as a part of their daily activities.

B. Platform as a Service (PaaS)

It is mainly intended to application developers who need platforms to develop their software or application.

C. Infrastructure as a Service (IaaS)

It is mainly intended to network architects who need infrastructure capabilities.

In a wider perspective, most of the previous consumers have their concerns over cloud computing vulnerabilities and challenges which might prevent them from their objectives. Information can be stored and accessed through the cloud, where consumers retrieve the information without knowing where it is being stored? Or how it is being stored and retrieved? Furthermore, consumers are free from the burden associated with maintenance and resource management costs. However, consumers are required to buy according to using time or number of used software. In contrast, the service provider must be responsible for maintaining and managing the information over the cloud. Obviously, securing the information is one of the primary objectives of cloud provider. Nowadays, information security is provisioned as a wonderful aspect of adapting any technology. While preserving the security would result in enormous popularity of this technology, compromising it can lead to catastrophic reality which can result in abandoning the technology. From the early days of distributed computing, standards and policies have been put in place to overcome any threat, vulnerability and risk which violates information security. Since the cloud paradigm is a distributed architecture, many worries have been raised over its vulnerabilities, security threats and challenges. Several of these security threats and challenges have been inherited from the internet. However, their influence intensified over the cloud platform

II. BACKGROUND

As mentioned before, cloud computing came as a consequence of continuous development of computing paradigms. In 1980's, with the development of internet, the foundation of emerging grid computation was established. The foundation involved various principals making the use of internet in a way where users are provisioned as resource nodes [14]. These principles paved the way of a novel computing paradigm which eventually carved today's distributed computing concepts.

In the 1990's, the concept of virtualisation was driven to the application tier. It followed by employing virtualised private network connections which share the same physical channel [14]. The emergence of these technologies has established the appearance of (SaaS) software as a service which states that consumers are not required to purchase the software rather than buying according to their own demand.

In the mid of 2006, Amazon achieved a prominent milestone by testing Elastic Computing Cloud (EC 2) that triggered the concept of cloud computing [14]. However, the term "Cloud Computing" was not coined until March 2007. The following year brought even more rapid development of the newly emerged paradigm. Furthermore, the cloud computing infrastructure services have widened to include (SaaS) software as a service [14]. In the mid-2012, oracle cloud was introduced, where it supported different deployment models. It was the first unified collection of cloud solutions which has been under continuous development since then. Nowadays, typing a cloud computing in any search engine will display hundreds and thousands of results.

III. SECURITY PERSPECTIVE WITHIN A CLOUD

This journal uses double-blind review process, which means that both the reviewer (s) and author (s) identities concealed from the reviewers, and vice versa, throughout the review process. All submitted manuscripts are reviewed by three reviewer one from India and rest two from overseas. There should be proper comments of the reviewers for the purpose of acceptance/ rejection. There should be minimum 01 to 02 week's time window for it.

A. DEPLOYMENT MODEL'S PERSPECTIVE

In cloud computing, several models can be deployed on the previously mentioned service models. These deployment models can be utilised based on their distribution nature which depends on cloud service location as following:

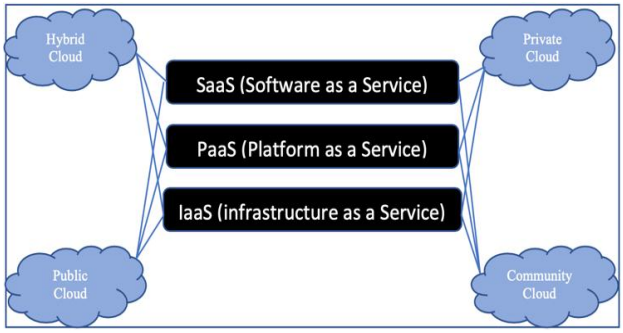

Figure 1. Cloud Service and Deployment Model

- **Public Cloud**

All services are being provided in a public environment where consumers can access a pool of resources which are managed by a hosted organisation. Due to its nature, this type of environment may raise critical concerns over security problems [4].

- **Private Cloud**

Services are being provided by a third-party vendor which separates it from public access. Consequently, it is safer than the previous development model due to the fact that it prevents unauthorised access [3][4].

- **Community Cloud**

Services are provided to a specified group where all members have equal rights of accessing the shared resources [4].

- **Hybrid Cloud**

Services are provided as a combination of more than one cloud (public cloud, private cloud and community cloud) [3].

B. CLOUD PARTY'S PERSPECTIVE

In the realm of internet, security has been perceived as a prominent factor leading to embracing of the cloud paradigm. Since the cloud environment is a distributed architecture in which its resource storage and management may be present in any part of the world, many concerns have been raised over its vulnerabilities, security threats and challenges. The involvement of various parties has widened these concerns based on each party's perspective. It was determined that there are three dominant parties which participate in the cloud environment.

- **Service providers:** Their concerns may be intensified over public and hybrid cloud where issues related to unauthorised access and cyber-attacks may jeopardise the service availability [4].
- **Service consumers:** Their concerns may focus on issues related to data privacy and quality of service. Besides, they are also concerned about service availability and interoperability [4].
- **Service regulators:** Their concerns may focus on issues related to service standard violations. Thus, issues related to interoperability would affect them greatly. It is fair to say that all previously mentioned party concerns might be correlated and associated to other parties [22].

C. SERVICE AVAILABILITY AND INTER-OPERABILITY

Consumers of cloud computing seek service continuity which means that providers are obligated to avoid even a single point of failure. Otherwise, they would end up in a trade-off between the satisfaction of consumers and security that would ultimately affect their reputation in the market. Since cloud computing is such an active environment, service continuity might be in a high alert especially with consumers moving from one service provider to another.

- **Service availability**

A service provider must primarily consider the likelihood of unavailability of crucial information when required [5]. The absence of information might act as a cause of physical or non-physical failures. Country's legal requirements, regulator rules, or domain standards can cause such a blackout of information. The blackout can also result from a faulty resource, suspicious attacks or software bugs. While the chances of materialising the previously mentioned reasons might be trivial, service providers should not overlook them. The mitigation of information availability can be resolved by two methods SLA and KPI.

Service Level Agreement (SLA) [7] is to ensure a standard agreement between cloud provider and consumers. It specifies the maximum shortage in the service which helps carving the expectation of consumers' [5]. Besides, it provides a backup plan for information to overcome any shortage which guarantee the present of information in case of emergency. While as, Key Performance Indicator (KPI) would measure the delivery of the defined service standards.

- **Service interoperability**

It means the potential of a group of service providers to exchange information and manage them according to agreed standards [8]. From a consumer perspective, it refers to the ability of moving between service providers and not being locked in an isolated cloud provider. Commonly, service consumers tend to be stunned by the concept of flexibility to shift among the clouds. However, it is a rigid task for them to relocate from one cloud provider to another, due to the absence of cloud computing standards [6]. It is known as the vendor lock-in problem [8]. Undoubtedly, various previous researches have signalled the lack of interoperability as a hurdle to the popularity of cloud computing [8].

Figure 2. Prominent use cases of interoperability

The mitigation of information interoperability can be addressed mainly by employing open standards [8]. Nowadays, there are various initiatives which try to establish standardisation of projects. Broadly speaking, these projects primarily give emphasis on standardising four prominent cloud interoperability use cases which are the following:

i. **User authentication:** It can be standardised according to Openid or protocols depend on OAuth (Open Authentication)[8].
ii. **Workload migration:** It can be standardised based on VM image file formats [8].
iii. **Data migration:** It can be standardised by addressing APIs differences.
iv. **Workload management:** It can be standardised by unifying workload management standards across various providers.

IV. INFORMATION SECURITY CHALLENGES AND THREATS

In this section, a high-level analysis of prominent challenges and threats is addressed. This helps summarising the causes of critical vulnerabilities in cloud platform. Once identifying these obstacles, our priority is easing and resolving them.

A. Service disruption due to attacks

In recent times, external attacks can be held responsible for major security breaches in cloud environment. This can be illustrated in the case of adobe systems, where its corporate databases were hacked, and data was stolen. It was reported that around 130 million consumer records got leaked [9]. Therefore, cloud provider must step up with some preventive measures to diminish the severity of these attacks.

- **Denial of Service attacks**

These are provisioned as unique, frequent and simple type of attacks. Their characteristics make them unpredictable and difficult to be intercepted. The primary idea behind these attacks is collaboration among multiple sources to put down targeted service provider by generating immense quantity of packets at the victim network entry [12][13][10]. Difficulty arises when it comes to distinguishing the illegal packet from the legitimate packet [10]. Obviously, these attacks have to be simultaneously to achieve their objectives, where it can be triggered by amateur hackers since they only have to run simple codes and tools [13]. As a result, the targeted service provider will be flooded by packets and becomes out of service. The mitigation of such attacks can be handled through various technologies. One of these technologies is the Intrusion Detection System (IDS) [12][13]. It is a software that demonstrates its efficiency especially when attack's duration for a long period of time [10]. Nowadays, there are efforts to make a brand-new hybrid intrusion detection technology which can sustain a variety of attacks [10]

B. Service Hijacking

This risk of service hijacking illustrates a crucial issue that compromises the confidentiality, integrity and the availability of service. It is an underestimated issue that is provisioned as a trivial challenge, yet it can jeopardise the credentials of consumers [11]. Intruders mainly tend to attack software vulnerabilities or use specified software to gain critical information such as passwords and usernames. As a result, attackers would gain a full control of cloud service and endanger it. The mitigation of such attacks can be addressed by preventing exchange of critical information such as password and user-names among consumers [11]. Furthermore, employing specified software to observe unauthorised access and report it can help preventing such attacks. Finally, cloud provider must deploy two factor authentication methods [11].

C. VM-level attacks

Since cloud environment is entirely built over the concept of virtualisation, cloud provider must deploy Virtual Machine (VM) technologies. One of these technologies is a hypervisor which is accountable of running and managing the VM. Service providers should critically consider all major fragile points within hypervisors. Basically, these technologies have been deployed and coded by developers who are aware of their vulnerabilities and how to overpass them [11]. The risk of such an attack is compromising a consumer VM and can endanger other consumers VMS. The mitigation of such a challenge can be addressed by employing technologies such as Intrusion Prevention System (IPS), Intrusion Detection System (IDS) and firewalls. All previously mentioned technologies work in collaboration to prevent, detect, and report any malicious activity at the VM- level [11].

D. Abuse and Nefarious Use of Cloud Computing

The concept of cloud computing lies behind providing services in a convenient way.

Basically, consumers are necessitated to have a valid credit card which enables them to register as cloud consumers [11]. Once they got their approval as consumers, they unrestrictedly use the services of clouds' in an anonymous fashion. Behaviours such as suspicious activities, malicious code authors, and unauthorised access are feasible in this relatively unobstructed environment.

As a consequence, the service would entirely be compromised and remain under threats. Obviously, a fragile registration policy and free trial use of service is the origin of such obstacles. The mitigation of such obstacles strengthens the initial procedure of registration. Besides, cloud provider must empathise on the validation step, where ensuring consumers' identities are verified. Furthermore, cloud provider should crucially inspect credit card fraud [17]. It is possible to investigate users' network traffic to identify suspicious activities. Finally, service providers are ought to check public blacklists to deploy proactive measures [18][19].

E. Insecure Interfaces and APIs

Ideally, service consumers primarily interact with interfaces and APIs. These interfaces and APIs are provisioned as an entry point, where they are in charge of critical tasks such as provisioning, observing, controlling, and orchestration of cloud service [11]. Practically, interfaces and APIs are loosely coupled to cloud service especially in term of their security and availability. Therefore, designing fragile interfaces, may pose a serious threats and vulnerability such as unauthorised access, restricted monitoring and inflexible access controls. In order to mitigate the threats arising due to insecure interfaces and APIs, implement a rigid authentication policy and access controls. Cloud provider must comprehend dependency chain related to API. Finally, cloud provider must crucially inspect security models of their interfaces.

F. Cloud Multi-tenancy

Cloud environment attracts its consumers by the leverage of sharing resources. To materialise the concept of sharing, cloud provider employs multi-tenancy. Practically, it is provisioned as software architecture to implement a full utilisation of resources [5]. Ideally, cloud providers retain network infrastructure, storage facilities, and software applications that support flexibility, efficiency, and scalability. Multi-tenancy deploys the previously mentioned resources in a shared fashion among cloud consumers (tenants). Given this deployment of multi-tenancy, tenants share infrastructure, software and platform resources in various deployment models. This sharing of resources might compromise the security, integrity, and confidentiality of information. As a consequence, the flow of information can be distributed, and unauthorised access may be feasible. As mentioned earlier, multi-tenancy is a necessity that must be deployed to fully utilise available resources. Therefore, it has to be enhanced to preserve the confidentiality of tenants. The enhancement can be done by carving a clear boundary between tenants [20][5]. The boundary must be deployed physically and logically at all layers, to evade vulnerabilities and risks. In IaaS, the boundary should be deployed within all resources such as network facilities and database storage. In PaaS, the boundary should be implemented in resources like operating systems. In SaaS, the boundary should be applied in all tenants' transactions on same software instant [5][6].

G. Cloud Elasticity

Cloud computing is a dynamic environment in which consumers (tenants) can rapidly scale up or down their demands. The toleration with such a behaviour is known as elasticity which is the ability of system to automatically adjust to the demand of tenants by provisioning and deprovisioning resources [13]. To implement this operation, a server placement engine is deployed to retain a pool of available resources and dispenses them to the tenants. The dispensing of resources is done through a migration technique to relocate services from a physical entity to another entity or from a logical cloud to another cloud to meet the requirements of tenants [13]. From practical perspective, this kind of energetic demands might lead to confidentiality issues. To comprehend these issues, imagine if "tenant A" decrease its demands, so it releases some recourses. Then, "tenant B" logged in and being assigned the previously mentioned resources. The primary problem is "tenant B" can infer the content of "tenant A" [13].

To mitigate the above risk, cloud provider must ensure implementing the required legal and security aspects within the placement engines. It should emphasise on retaining the information within tenants' country [13]. Moreover, it should take into consideration all security policies within the migration technique to deploy them physically and logically [13].

H. Data Loss or Leakage

Obviously, retaining the information of consumers is a crucial priority of cloud providers. This refers to avoiding the following scenarios:

- Unauthorised adjustment or moving of information.
- Inefficient encoding techniques.
- Unauthorised access to critical information.
- Loose coupling of a segment of information to its larger content

Honestly, not all previously mentioned scenarios are entirely associated with cloud environment. However, some of these risks intensified over cloud. This is mainly due to its architectural and operational specifications. The mitigation of these risks can be handled by employing a reliable encoding technique to safeguard the information in transit. Furthermore, cloud provider must implement a secure backup plan provably with a remote replica of most crucial information. It is possible to deploy a rigid API access control to avert unauthorised access.

I. Malicious Insider

Service provider must carefully deem malicious insiders who are capable of infiltrating their organisations. They can compromise the confidentiality, integrity, and security of information or even avert the accessibility to resources [5]. From consumers' perspectives, this vulnerability can be escalated by insufficient transparency with cloud provider. Obviously, employment policy and management standards play a vital role in the origin of this risk. For the mitigation of the above risk, cloud provider should support a rigid supply chain management with inclusive supplier evaluation. It is preferable to structure the management hierarchy to avoid a single point of control especially within lower levels.

Legal contracts must clearly state human resource requirements which can be designed to prevent such risk. Lastly, cloud provider can install an early notification system to detect suspicious activities.

V. SECURITY ALGORITHMS USED IN A CLOUD

This section describes some of the most commonly used security algorithms used in the cloud computing platform.

A. AES

A symmetric encryption standard, Advanced Encryption Standard also known by its original name Rijndael. A subset of Rijndael block, it was developed by two Belgian cryptographers Joan Daemon and Vincent Rijmen. It is one of the strong and highly secure algorithms till date. Based on substitution-permutation network, AES is efficient is efficient on both software and hardware platforms.

B. RSA

An asymmetric encryption technique, Rivest-Shamir-Adleman (RSA) was created by Ronald Rivest, Adi Shamir and Leonard Adleman in the year 1977 [15][16]. RSA is one of the initially used realistic public-key cryptosystems and is broadly used for secure data transmission. In this cryptosystem, the encryption key is public and is different from the decryption key which is kept as a secret. In RSA, this type of asymmetry has its basis on the practical difficulty of factoring the product of two large prime numbers [20].

C. Triple DES (3DES)

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) employs a 56-bit key and has not been deemed sufficient to encrypt sensitive data. 3-DES basically extends the key-size of DES via applying the algorithm three times successively with three different keys. The combined key-size is thus 168 bits (3 times 56) [15]. 3DES involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, i.e., the plain text is encrypted with K1, followed by decryption with K2, and then encrypted again with K3 [21][16].

VI. EXPERIMENTS RESULT

In this paper, we examined various security algorithms to determine the efficiency of these algorithms locally as well as over cloud. To acquire accurate results numerous tests were performed on each algorithm, then the mean value was computed for each data set. These data sets have different sizes ranging from as small as 2kb to 100kb file size. The experimentation process was done in Java programming language using IED Eclipse 4.7.0 (Oxygen). The cloud platform used to test the security algorithms was “Google App Engine”.

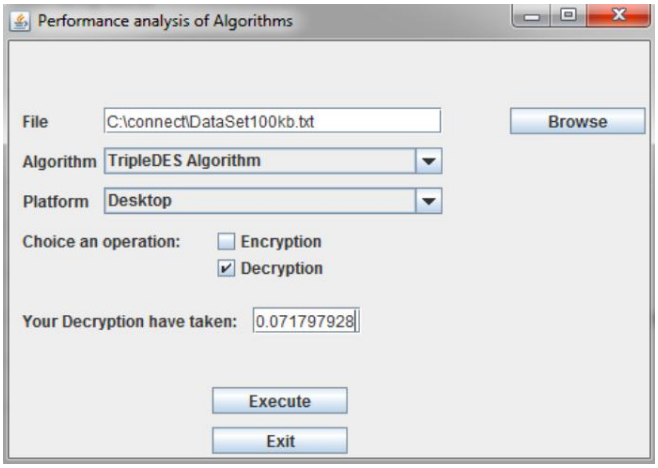

Figure 3. Graphical User Interface using Java Swing library

The execution times of each algorithm has been recorded where encryption process is examined separately from that of the decryption process. In the following analysis both encryption and decryption have been tested using various input file sizes: 2kb, 5kb, 10kb, 20kb, 50kb, and 100kb. Figure 4 represent execution time of encryption algorithms over cloud and locally, the execution time is calculated in seconds and input size in kilobytes.

Input Size	AES Locally	AES Cloud	RSA Locally	RSA Cloud	3DES Locally	3DES Cloud
2kb	0.64299 6045	0.00131 314	0.56708 467	0.2590 894	0.65031 6931	0.00084 1611
5kb	0.70234 7555	0.00181 243	0.67873 282	0.7567 361	0.67562 2031	0.00164 6998
10kb	0.72936 2178	0.00297 645	0.87245 185	1.6473 855	0.67698 5397	0.00314 9098
20kb	0.73232 7632	0.00560 514	1.19051 805	3.5930 78	0.67986 1803	0.00622 9267
50 kb	0.74307 1518	0.00660 252	2.21658 342	9.2094 83	0.68605 7414	0.01507 7759
100 kb	0.75768 7899	0.00695 636	4.14813 202	112.84 344	0.69102 8384	0.03013 9216

Table 1. Comparison of Encryption Algorithms

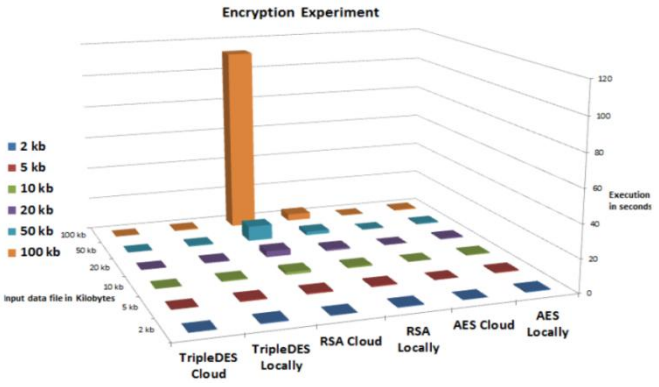

Figure 4. Comparative Analysis of Encryption Algorithms

Following observations were obtained from above encryption process:

- Among all the three encryption algorithms, RSA is the most time-consuming algorithm comparing to others during local implementation as well as over cloud environment.
- For smaller data tests, Triple DES encryption algorithm consumes less time over cloud while it increases exponentially with the increase in the input size. While as for AES encryption algorithm, it shows steady increase in time locally and over cloud environment as well.

Input Size	AES Locally	AES Cloud	RSA Locally	RSA Cloud	3DES Locally	3DES Cloud
2kb	0.00128 9577	0.00011 4107	0.00034 2078	9.30E-05	0.00102 3331	6.64E-06
5kb	0.00338 2725	0.00012 1956	0.00975 52	0.00012 3765	0.00270 8957	2.54E-05
10 kb	0.00644 1848	0.00017 4481	0.01892 297	0.00019 1988	0.00594 0145	3.74E-05
20 kb	0.00972 6768	0.00022 8818	0.03677 769	0.00032 4927	0.01003 2258	6.16E-05
50 kb	0.01259 1446	0.00026 142	0.07801 384	0.00136 5061	0.40508 779	0.00010 5654
100 kb	0.03070 2664	0.00034 1717	0.16211 64	0.00234 3233	0.07179 7928	0.00025 0771

Table 2. Comparison of Decryption Algorithms

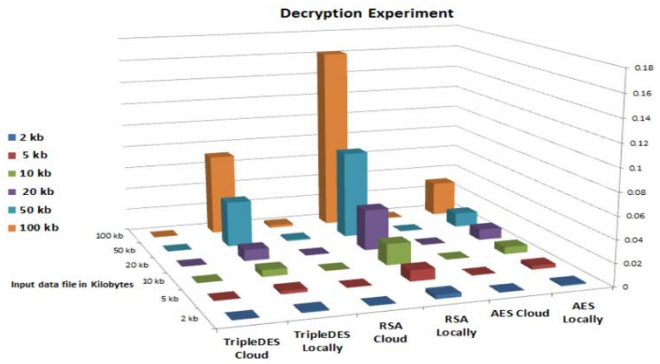

Figure 5. Comparative Analysis of Decryption Algorithms

Figure 5 represents execution time of decryption algorithms over cloud and locally, the execution time is calculated in seconds and input size in kilobytes.

Following observations can be obtained from above decryption results

- Amongst decryption algorithms, Triple DES decryption algorithm consumes less execution time over cloud than other algorithms.
- RSA decryption algorithm consumes more execution time locally and over cloud comparing to the other two algorithms.

VII. CONCLUSION

The field information technology has witnessed evolutionary progress in the past decade that lead to the concept of cloud computing. It distinguished itself as one of the major computing models, where several academic and industrial organisations showed their interests in the research about this promising paradigm. Unfortunately, there is an open question about security threats and challenges that rely behind the concept of cloud computing. Since the cloud platform is based on a distributed architecture, it is natural to inherit some risks and vulnerabilities that are related to distributed systems. However, several of these risks have intensified over the cloud computing platform. To overcome these risks, cloud providers and consumers should agree on the service level agreement (SLA) [7]. While the causes of interoperability have been discussed carefully, an open standardisation policy proposed for each of the prominent use cases. The paper primarily focused on major security threats of cloud paradigm, one of these threats related to service disruption which can result due to attacks such as denial of service attacks, service hijackings and VM-level attacks. The mitigation of the previously mentioned attacks has been discussed. Furthermore, the paper elaborated on risks and vulnerabilities related to abuse and nefarious use of cloud computing, insecure interfaces, multi-tenancy, elasticity, data loss and malicious insider. In addition to discuss the causes of these threats, key aspects to overcome them are addressed. One of these aspects is encryption and decryption algorithms. We tested prominent security algorithms over the Google cloud platform and locally as well. A comparison of the efficiency of these algorithms deployed over a cloud and locally is performed. The experiments were performed over the eclipse with designing a graphical user interface using Swing components. We noticed that the effectiveness of each algorithm various according to mood of development on cloud or locally, and data loads. The results show that Triple DES manifested a higher time efficiency ratio over cloud when subjected to different data loads compares to AES and RSA. In future, we have many algorithms to be evaluated and their results will be analysed comparing to this paper experiments.

REFERENCES

1. Yu, Y., Miyaji, A., Au, M. and Susilo, W. (2019). Cloud computing security and privacy: Standards and regulations, 2017 - Elsevier
2. Wentao Liu, "research on cloud computing security problem and strategy", IEEE, ISBN 978-1-4577-1415-3112,
3. Basu et al., Ieeexplore.ieee.org. (2019). Cloud computing security challenges & solutions-A survey
4. Peter Mell Timothy Grance, National Institute of Standards and Technology Special Publication 800-145,2011
5. Snehal R Rathi ,Vikas K Kolekar, Ieeexplore.ieee.org. (2018). Trust Model for Computing Security of Cloud
6. Swapnil M Parikh, "A Survey on Cloud Computing Resource Allocation Techniques". IEEE, ISBN,978-1-4799-0727,
7. Uttam Thakore, et al., "An Actor-Centric, Asset-Based Monitor Deployment Model for Cloud Computing". In 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing ,2013
8. Akhil behl, kanika behl, "An Analysis of Cloud Computing Security Issues". IEEE, ISBN,978-1-4673-44805, In 2012 World Congress on Information and Communication Technologies, pp. 109-114, 2012
9. Amit Gajbhiyel, Krishna Mohan, "Cloud Computing: Need, Enabling Technology, Architecture, advantages and challenges". IEEE, ISBN,978-1-4799-4236, in the 5th International Conference-Confluence the Next Generation Information Technology Summit (confluence),2014
10. Amazon EC 2 sla. Http://aws.amazon.com/ec2-sla/
11. Grace A. Lewis, "Role of Standards in Cloud-Computing Interoperability". In 46th Hawaii International Conference on System Science, pp. 1652-1661, Hawaii, the US, 2013

12. S Singh, YS Jeong, JH Park - A survey on cloud computing security: Issues, threats, and solutions, JOURNAL OF NETWORK AND COMPUTER APPLICATIONS, 2016 – Elsevier
13. Arpit Gupta, Vaishali Chourey, "Cloud Computing: Security Threats & Control Strategy Using Tri-Mechanism". IEEE, ISBN,978-1-4799-4190, In 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), pp. 309-316, 2014
14. Rajni Goel, et al., "Cloud Computing Vulnerability: DDOS as its Main Security Threats, and Analysis of IDS as a Solution Model". IEEE, ISBN,978-1-4799-3187, In 2014 11th International Conference on Information Technology: New Generations, pp. 307-311, 2014
15. M Almorsy, J Grundy, I Müller – An analysis of the cloud computing security problem, 2016 - arxiv.org
16. Alok Tripathi, Abhinav Mishra, "Cloud Computing Security Considerations". , In 2011 IEEE International Conference on Signal Processing , Communication and Computing (ICSPCC), 2011
17. Farzad Sabahi, "Cloud Computing Security Threats and Responses". IEEE, ISBN,978-1-61284-486, In 2011 IEEE 3th International Conference on Communication Software and Network (ICCSN), pp. 245-249, 2011
18. Anas Bouayad, et al., "Cloud Computing: Security Challenges". IEEE, ISBN,978-1-4673-2725, 2012
19. Shufen Zhang, et al., "Analysis and Research of Cloud Computing System Instance". IEEE, ISBN,978-0-7695-3940, 2010
20. RL Rivest, A Shamir, L Adleman, "Communications of the ACM", 1978 - dl.acm.org
21. "3DES", http://www.cryptosys.net/3des.html
22. NH Hussein, A Khalid , A survey of cloud computing security challenges and solutions - International Journal of Computer Science and Information Security, 2016 - researchgate.net

AUTHORS PROFILE

Ahmed Alrehaili received his master's in Applied Computer Science from Concordia University, Canada in the year 2012. The author joined Faculty of Computer and Information Systems at Islamic University of Medina, KSA, as a Lecturer soon after returning from Canada. He has been an active member of various research groups, has publications under his name and has since headed the IT unit in the Faculty of Computer and Information Systems at Islamic University, Medina. His research interests include, Cloud Computing, Blockchain, Artificial Intelligence, Information Security, etc. The author has been an active member of various committee during the ABET accreditation process.

Aabid Mir has done his masters from the university of Bedfordshire, Luton, United Kingdom. Soon after he joined the Faculty of Computer and Information Systems at Islamic University of Medina, KSA, as a Lecturer. At Islamic University, the author has been a part of many funded and non-funded research projects and has publications under his name. His research interests include parallel and distributed computing, network and information security, WSNs, The author was one of the active team members during ABET (American Board of Engineering and Technology) accreditation process. The author is currently pursuing his Ph.D. in Information Technology from the University of Kuala Lumpur, Malaysia.

Mir Junaid received his master's degree in Computer Science and Engineering with a specialization in Machine Learning from the VIT University, India in 2017. The author has worked on the classification of Images using Convolutional Neural Networks and has received the best Research-Based Learning (RBL) award from VIT University in 2016. The author is currently working towards a Ph.D. degree in Big Data and Machine Learning at the Laboratory of Modelling and Safety of Systems (LM2S), Universite de Technologie de Troyes (UTT), France. His work is funded by the European Regional Development Fund (Fonds européen de développement régional). His research interests include Machine Learning, Graph Signal Processing, Geometric Deep Learning, Big Data, Internet-of-Things (IoT) and Blockchains. The author is also the President of the doctoral students association of UTT, France