Integration of Searching and AES Encryption in Cloud Computing

Gudapati Syam Prasad, J Yashvin, S sunil kumar, A Keerthi

***Abstract:** To execute distributed storage and ensure the security of distributed storage, we utilize different encryption strategies. Besides, in the wake of encoding the information, the capacity to look through the information utilizing helpful search tokens is essential. The encryption ought to be sufficiently vigorous to oppose different savage power assaults like keyword guessing attacks (KGA). Moreover, the looking calculation which is executed ought to enable the keywords to scan for the information effectively and successfully. Since information being put away on the cloud has turned out to be ordinary, searchable encryption innovation is a developing area in cloud computing. The information is secured utilizing a solid, asymmetric encryption standard which will naturally encode the information which is gone into forms. The plaintext is covered up and only an approved client can see its genuine substance. Secure encryption innovation guarantees that information protection is undertaken and disposes of the likelihood of any plaintext being perused by undesirable clients. Ventures containing a lot of delicate information will locate that accessible encryption and will limit the opportunity for breaches. The utilization of searches on encoded information will proceed advance as more frameworks are built up that offer this innovation in a faster and increasingly lucid way. Using PHP and Ajax queries, we are able to create a cloud application which takes the data input in forms such as name, phone number, email, etc. The data in the forms is collected and encrypted using AES encryption algorithm and stored in a mySQL database. Moreover, the data is searched and decrypted results are retrieved using an AES token of arbitrary size.*

***Index Terms:** secure cloud storage, encryption, keyword guessing attack, searching algorithm, data privacy.*

I INTRODUCTION

A. Basics of Cloud Computing

Cloud computing is commonly different administrations which are facilitated over the Internet. They can be removed servers which can be utilized to store and control information, or they are exceptionally confined servers. Before cloud computing, numerous destinations were facilitated on nearby servers embracing pay-as-you go plans of action. Proprietors regularly needed to purchase enough server space to guarantee that servers could hold fast to approaching traffic and different issues like downtime, crashes, and so on. Computing devices on the cloud are relied upon to work constantly on interest and for the handling, they may run short with the registering assets like stockpiling, battery life memory, and etc. One approach to amend these limitations is to utilize cloud innovation which enables gadgets to drop certain errands to increasingly strong servers in the cloud. Cloud frameworks have various sending models, two of which are named public cloud and private cloud. Public cloud deals with the equipment in their own servers and offers the administrations utilizing different evaluating models. In the open cloud, registering or capacity assets are made accessible to the purchaser on interest at a cost.

Some organizations are able to outsource private local cloud to public cloud service providers. The cell phone's abilities can be enlarged by utilizing cross breed cloud engineering. Since the cell phone sends invocations to ingenious nearby clouds, it includes settling on choices with respect to the public cloud services or private cloud services to pick from.

Cloud computing has seen a fast increment in fame throughout the most recent decade as it reaps a few rewards. Cloud models have turned out to be very financially savvy and are soundly effective with low support and establishment costs. In addition, cloud administrations are very extensible, inferable from the way that asset distribution is possible promptly. Cloud innovation has turned out to dependable additionally having promising data backups, business progression models and offering recuperation for equipment and programming failures.

B. Types of Cloud Computing administrations

Cloud computing engineering can be isolated into three administrations:

B.1 Infrastructure as a service (IaaS) In this model, an enterprise’s finished data center is move into the cloud. A supplier will at that point track all the equipment dependent on the system and the capacity servers, henceforth disposing of the requirement for high asset use establishment.

B.2 Platform as a Service (PaaS)

This stage empowers an administration processing model which offers enterprises the chance to create programming for their organization without stressing over the support. PaaS suppliers make situations which are uniquely customized to every one of their client's needs including extra highlights like compilation amenities and control of the version.

Manuscript published on 30 June 2019.
* Correspondence Author (s)

Dr.Gudapati Syam Prasad*, Department Of Computer science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur,522501

J Yashvin, Department Of Computer science and Engineering Koneru Lakshmaiah Education Foundation,Vaddeswaram,Guntur,522501

S sunil kumar, Department Of Computer science and Engineering Koneru Lakshmaiah Education Foundation,Vaddeswaram,Guntur,522501

A Keerthi, Department Of Computer science and Engineering Koneru Lakshmaiah Education Foundation,Vaddeswaram,Guntur,522501

B.3 Software as a Service (SaaS)

Rather than having a client introduce an application on his own gadget,

SaaS will host that application on a private cloud. SaaS eliminates costs identified with programming protection.

C. Rationale

Cloud security is an issue that ought to be considered inconceivably important by any hopeful undertaking or any client. Numerous sellers of cloud administrations have complex security designs that have client approval, information encryption, infiltration testing, and so on. Cloud providers should make each essential move to guarantee that others can't get to their customer's information. Different associations utilize a kind of cross breed engineering that designates and strengthens information in a committed cloud. In any case, information security issues have been noticeable lately. The Cloud Security Alliance (CSA) have as of late shared worries about a progression of twelve dangers marked the "Deceptive Twelve". At the pinnacle of the rundown was information breaks. In 2017 alone, there were 456 recorded information breaks, with 40% expansion from the earlier year. Those attempting to break information are finding better approaches to go around the different conventions which are interlinked with the cloud services. As distributed computing design is regularly a mix of a few elements, the general cloud is as solid as its weakest connection. Aggressors regularly hope to assault different substances at a solitary time. Simultaneously, cloud suppliers who don't construct sufficient countermeasures will turn into the most helpless. In like manner, the cloud has turned into a spot for the individuals who look not bargain information and servers; they hope to scrutinize and move data for their very own loathsome purposes. This makes the cloud a prime area for individuals hoping to profit and as fast as could be expected under the circumstances. Assigning positions and authorizations among clients is one spot where information is frequently traded off. An undertaking ought to have full command over when they can repudiate and supply consents to the clients of their innovation. Organizations can prescribe multifaceted confirmation to be sure that the individual who is getting to the information is really the individual that he is said to be. Organizations need to stick by specific arrangements and techniques that will their product prosper without the danger of being undermined by information security issues like ruptures.

D. PROBLEM TO ASSESS

D.1 Algorithm based issues

There are numerous issues to address in a disseminated figuring condition with regards to distributed computing. For one, we need to pick and figure out which calculations to actualize. When contemplating our calculations, we should thoroughly analyze the time complexities of every one of the calculations to comprehend the run time of every calculation in a disseminated figuring condition. Another calculation-based issue is space unpredictability and how much stockpiling are required to apply the calculation effectively.

D.2 Remote based execution versus System Performance

Thusly, we ought to pick between remote execution and production. On the off chance that we settle on remote execution, at that point we are restricted with the execution capacity of our half and half cloud condition. Remote execution basically implies if a client control is in one area and a capacity exhibit is in somewhere else, we can get to them from a better place or remotely. In any case, this blocks the execution consistency of a client's demand. On the off chance that we incline toward system performance, we can just execute asks for on a similar cloud condition.

D.3 Virtualization issues

Virtualization hoards up important registering assets and frequently can clog the system traffic. There are additionally numerous issues with respect to programming authorizing. Real programming merchants regularly claim all authority to "audit" your association and confirm your permitting. Most merchants are essentially keen on getting their permitting expenses, particularly for "first guilty parties." But when you think about that a solitary permit may cost a great many dollars, indiscreet VM expansion can handicap an association monetarily.

II. LITERATURE REVIEW

A. Regular Language Search for Secure Cloud

A few procedures and approaches where examined preceding embracing our own safe accessible cloud storage strategy. One such way was that displayed in Y. Yang, X. Zheng, C. Rong, and W. Guo, "Proficient Regular Language Search for Secure Cloud Storage," IEEE Transactions on Cloud Computing, pp. 1– 1, 2018. Here Yang and his gathering built up a customary language look through that had moderately high effectiveness and autonomous trapdoor age to opposes keyword guessing attacks (KGA). Yang and the others could accomplish this by using a deterministic finite automata (DFA) that could be utilized for seeking watchwords which are first acknowledged as normal language by the DFA. Here, the DFA is 5-tuple $(Q, \Sigma, \delta, q0, F)$.

Here there are 5 states q0, q1, q2, q3, and q4. On input w1, the state will change from the q0 state to the q1 state. Ensuing advances are made until the last arrangement of strings, or the watchword, is acknowledged. These runs are made toward looking for scrambled information utilizing a catchphrase that is first acknowledged by the DFA.

Yang and the other proposed a kind of framework design that would utilize key pair encryption between the information proprietor, the information client and the expand proficiency while information proprietor and the cloud supplier.

Principally, the framework design is based around secure information recovery and the seeking of the encoded information utilizing a catchphrase.

The KGC will build up an open/private key pair and disseminate to both the information proprietor and the information client. The information proprietor will be able to scan for the information utilizing a watchword by getting to the cloud server which is held by the information proprietor. The information client will likewise have the capacity to see the crude information which has not been scrambled. Then again, the information client will be offered access to an inquiry token that they can use on a neighborhood cloud stage that is utilized for information recovery at a remote site.

Yang, Zheng, Rong and the others proceeded to close by contrasting the different seeking procedures utilized and their own ordinary language strategy with an end goal to demonstrate that their technique was the most reasonable to opposes catchphrase speculating and other animal power assaults.

B. An Efficient and Secured Framework for Mobile Cloud Computing

Among the other research papers, I. Elgendy, W. Zhang, C. Liu and C. Hsu, "An Efficient and Secured Framework for Mobile Cloud Computing", IEEE Transactions on Cloud Computing, pp. 1-1, 2018 makes a structure that floods just concentrated errands as opposed to offloading a wide range of uses. An improvement was made by Elgendy and the others to settle on choices powerfully dependent on a few imperatives like execution time of the assignment, CPU utilization, measure of vitality devoured, and so forth.

This paper likewise archives the utilization of symmetric encryption systems as layers to scramble the information of the errand before exchanging it to the cloud through the cloud administrator. Here three versatile applications which are worked with AES security layer over it and the three applications are thought about as far as effectiveness. These applications incorporate face identification, gaussian haze and brisk sort. After survey the consequences of the three applications, Elgendy and the others could state that the cell phone applications use about 30% of the CPU by and large. Be that as it may, through the offloading system, this use can be contracted to 12% with an AES security layer added to it and 7% of CPU without it. As AES has demonstrated to have most extreme productivity, we too embraced the encryption standard as our principle system in accessible encryption for distributed storage for our exploration.

LSH esteem will be the in particular the hashes. This is known as minhash. Awad and the rest of the analysts framed two LSH methods utilizing minhash. These are known as: GRP minhash and Omflip minhash.

B.1 GRP minhash

First make a change work R3=GRP(R1, R2). The essential reason of Grp is to separate the R1 hash esteems into 2 bunches as per R2 values. This implies for each piece we check in R1, we should check the relating bit in R2. In the event that the bit in R2 is 0, we should move the bit from R1 to the primary gathering. If not, place it in the second gathering.

B.2 Omflip minhash

Here the irregular stage work is supplanted with an omflip strategy. This is essentially a two-change organize type of least hashing.

III. THEORETICAL ANALYSIS

A. Advanced Encryption Standard (AES)

A.1 Overview of AES

AES comprises of a system of substitution and change activities which includes substituting inputs and moving around bits. Here every one of the calculations are done on bytes, not on bits. AES will take a 128-piece square of plaintext and view it as 16 bytes. These 16 bytes will be in this way orchestrated into a 4x4 network.

Here the quantity of rounds in AES relies upon the key length. There are 10 rounds for 128-piece keys, 12 rounds for 192-piece, and 14 rounds for 256-piece keys. Every one of the rounds utilize their very own diverse 128-piece round key.

A.2 Encryption of AES

Each AES round comprises of 4 subprocesses: byte substitution, move lines, blend sections, and include round key. The info bytes will be substituted utilizing a S-box table whose outcome is a 4x4 grid. The following procedure is move lines where every one of the four lines are moved to one side. Next, blend sections utilize a particular scientific capacity to supplant the whole segment of 4 bytes. Ultimately, every one of the bytes are taken as 128 bits and the XOR work is connected to these bits with the 128 bits of the round key.

A.3 Decryption of AES

Decoding of AES is like encryption aside from that the 4 sub procedures are done in the turn around request. Here dissimilar to different figures like Feistel, the encryption and decoding must be done independently.

B. Techniques for Searches on Encrypted Data

Consider a grouping of words w1… .wn containing k areas where F is a protected pseudorandom capacity and G is a pseudorandom generator and S is pseudorandom esteems.

B.1 Basic Scheme

In the event that an individual needs to look through a word W, at that point that individual will tell someone else the W and the ki as per the area I. The primary individual would then be able to look for W in the figure message by checking in straight time if Stream Cipher ⊕ the plaintext has a place with the type of <s,Fk(s)>. Here the client checking won't know about the plaintext.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

B.2 Hidden Scheme

In the concealed plan, an individual ought to pre-encode each word W of the plain content utilizing a different calculation Ek which is deterministic.

At that point the individual can post scramble in the wake of shaping the encoded words utilizing the stream figure development Ci= Xi⨁Ti. So as to scan for the word W, the individual will at that point register X=Ek(W) and k=fk(X). This permits someone else who need a similar word to look W without uncovering the genuine substance.

IV DESIGN

A. Rudimentary Designs

For the design of our secure searchable encryption technology, we have used Unified Modelling Language (UML) to outline our project.

B. Object Diagram

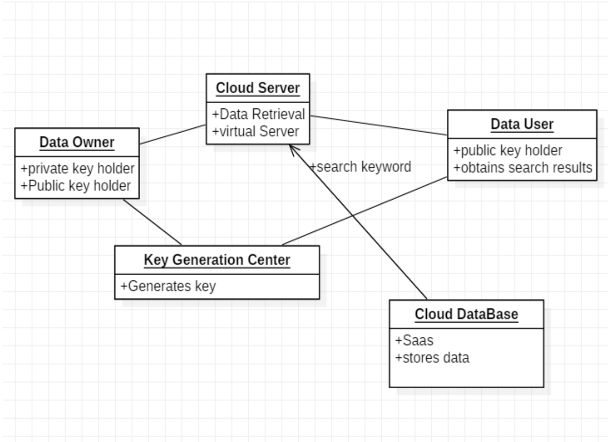


Figure 1 Object Diagram

C. Sequence Diagram

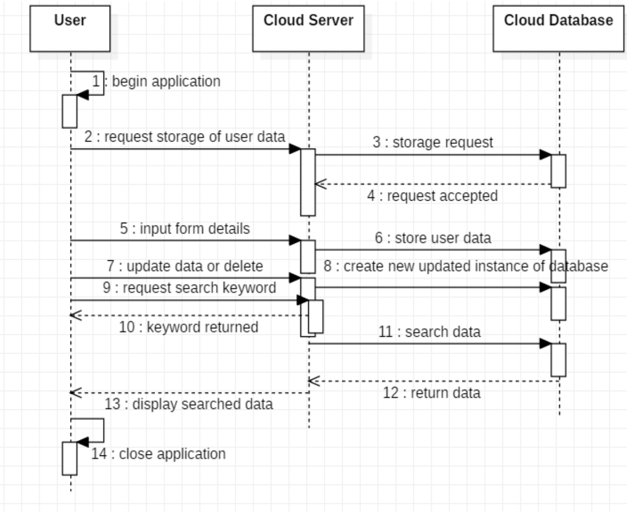
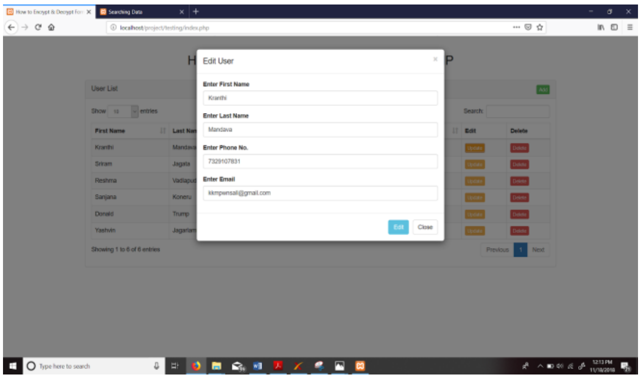


Figure 2 Sequence Diagram

V RESULTS



Edit User

Enter First Name: Kranthi

Enter Last Name: Mandava

Enter Phone No.: 7329107831

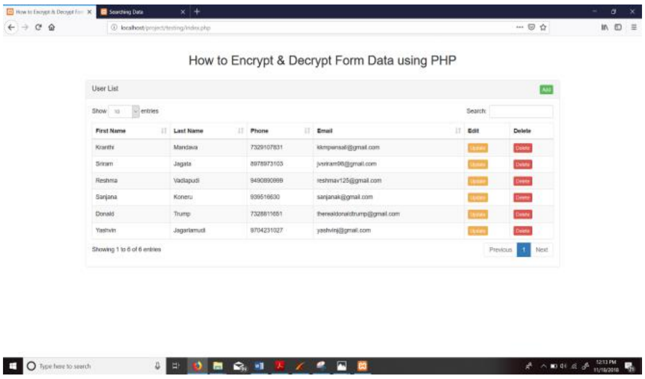
Enter Email: kkmpensall@gmail.com

Edit Close

First Name	Last Name	Edit	Delete
Kranthi	Mandava	Update	Delete
Sriram	Jagata	Update	Delete
Reshma	Vadlapud	Update	Delete
Sanjana	Koneru	Update	Delete
Donald	Trump	Update	Delete
Yashvin	Jagarlam	Update	Delete

Showing 1 to 6 of 6 entries

Fig 3 User entry



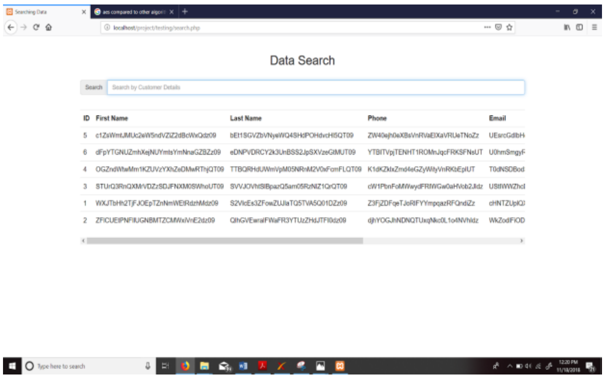
How to Encrypt & Decrypt Form Data using PHP

User List

First Name	Last Name	Phone	Email	Edit	Delete
Kranthi	Mandava	7329107831	kkmpensall@gmail.com	Update	Delete
Sriram	Jagata	8978973103	jvsriram98@gmail.com	Update	Delete
Reshma	Vadlapudi	9490890888	reshmav125@gmail.com	Update	Delete
Sanjana	Koneru	939516630	sanjanak@gmail.com	Update	Delete
Donald	Trump	7328811651	therealdonaldtrump@gmail.com	Update	Delete
Yashvin	Jagarlamudi	9704231027	yashvinj@gmail.com	Update	Delete

Showing 1 to 6 of 6 entries

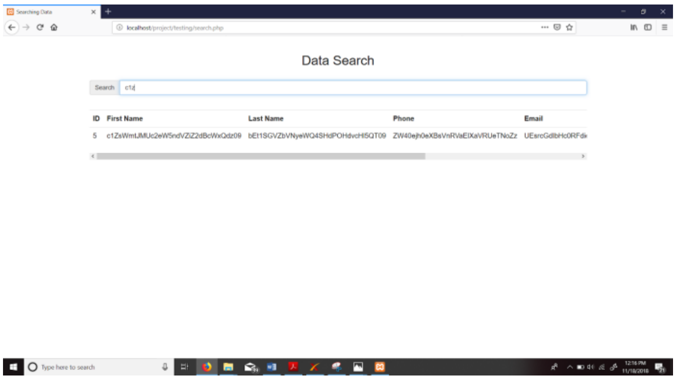
Fig 4: Project UI


Searching Data
aes compared to other algori
localhost/project/testing/search.php
Search
Search by Customer Details
Type here to search
12:20 PM
11/18/2018

Data Search

ID	First Name	Last Name	Phone	Email
5	c1ZsWmtJMUc2eW5ndVZiZ2dBcWxQdz09	bEt1SGVZbVNyeWQ4SHdPOHdvcHI5QT09	ZW40ejh0eXBsVnRVaElXaVRUeTNoZz	UEsrcGdlbH
6	dFpYTGNUZmhXejNUYmtsYmNnaGZBZz09	eDNPVDRCY2k3UnBSS2JpSXVzeGtMUT09	YTBITVpjTENHT1ROMnJqcFRKSFNsUT	U0hmSmgyF
4	OGZndWtwMm1KZUVzYXhZeDMwRThjQT09	TTBQRHdUWmVpM05NRnM2V0xFcmFLQT09	K1dKZklxZmd4eGZyWitjVnRKbEplUT	T0dNSDBod
3	STUrQ3RnQXMrVDZzSDJFNXM0SWhoUT09	SVVJOVhtSlBpazQ5am05RzNlZ1QrQT09	cW1PbnFoMWwydFRlWGw0aHVob2Jldz	UStlWWZhcl
1	WXJTbHh2TjFJOEpTZnNmWEtRdzhMdz09	S2VlcEs3ZFowZUJlaTQ5TVA5Q01DZz09	Z3FjZDFqeTJoRlFYYmpqazRFQndiZz	cHNTZUpIQ
2	ZFlCUEtPNFlUGNBMTZCMWxlVnE2dz09	QlhGVEwralFWaFR3YTUzZHdJTFl0dz09	djhYOGJhNDNQTUxqNkc0L1o4NVhidz	WkZodlFiOD

Fig 5: AES Encryption



Data Search

Search: c1z

ID	First Name	Last Name	Phone	Email
5	c1ZsWmtJMUc2eW5ndVZiZ2dBcWxQdz09	bEt1SGVZbVNyeWQ4SHdPOHdvcHI5QT09	ZW40ejh0eXBsVnRVaElXaVRUeTNoZz	UEsrcGdlbHc0RFdi

Fig 6 Encrypted Data Search

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

VI DISCUSSION OF RESULTS

A Overview of the Results

Here we have effectively actualized every one of the parts of our protected accessible distributed storage venture. At first, a user interface (UI) was intended to effectively demonstrate the information which should have been included alongside the liquid structures for the client get to. The client just embeds every one of his subtleties and the information is quickly encoded utilizing AES calculation. Increasingly resulting clients can be added to the cloud database by tapping on the include catch and different clients can be refreshed and erased. Refreshing task will promptly encode the adjusted information again utilizing AES methods. Erasing will drop the information from the database inside and out.

For seeking, an encoded wrd is given to the client. It is of variable length yet for the most part it is around 4-5 bits for comfort. The client can look through that watchword in the hunt box and they will probably inquiry from the rundown of all out records. While seeking in any case, the id will show up which is the essential key in the database. The client would then be able to utilize this id number to allude to the plaintext.

VII. SYNOPSIS

Cloud computing has been expanding relentlessly in our consistently lives and cloud security is turning into a problem that needs to be addressed. Numerous aggressors are discovering approaches to sidestep the security conventions made by organizations. So as to guarantee that a product isn't helpless against assaults like KGA, a more grounded and effective encryption standard like AES is suggested which has higher effectiveness and isn't defenseless to trapdoor assaults. Notwithstanding concealing plain content. a client should likewise have the capacity to quickly get to the information he has encoded. Utilizing fluffy catchphrase seeking, a client will recover results that are near the watchword.

In our execution of secure accessible distributed storage, we could make UI that was stylishly simple to use by having clients submit information in the method for structures. The information was effectively put away in the cloud and shrouded utilizing AES calculation. In the wake of encoding, clients would then be able to see the information which they have just put away in the cloud database or they can refresh/erase information. Refreshed information is promptly encoded and put away once more. Ultimately, the client is given a catchphrase and the encoded watchword can be utilized to file the real plain content.

VIII FUTURE SCOPE

Innovation is consistently changing and enhancements can be made anyplace. This undertaking can be improved by acquainting an alternative with pick an encryption standard. Rather than simply constraining a client via naturally scrambling utilizing AES encryption, the client can be given different encryption gauges to look over like blowfish, Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES), and so forth. Furthermore, multifaceted verification can be utilized to confirm the client who is getting to information to guarantee they are not taking on the appearance of somebody else.

IX OTHER DANGERS TO CLOUD COMPUTING

There is a heap of other security dangers that numerous clients of distributed computing are uninformed of other than information misfortune and information ruptures. Among these is insider dangers. Representatives utilizing cloud security could conceivably offer access to digital aggressors whom generally would have thought that it was difficult to infiltrate the cloud. Others incorporate Specter and Meltdown which are license side channel assaults where an assailant can peruse and get to a framework from a log which is unprivileged, giving the aggressor different data about the piece and the undertaking. At long last, shaky application programming interfaces (API) have enabled a few aggressors to cross limits utilizing open Internet Protocol (IP) addresses. Every one of these dangers must be viewed as when structuring and supporting new cloud situations.

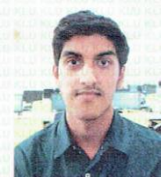
REFERENCE

1. 2018C. T. G. A. F. 13, “6 Top Cloud Security Threats to Consider in 2018 and Beyond,” The State of Security, 23-Mar-2018. [Online]. Available: https://www.tripwire.com/state-of-security/security-data-protection/cloud/top-cloud-security-threats/. [Accessed: 18-Nov-2018].
2. Y. Yang, X. Zheng, C. Rong, and W. Guo, “Efficient Regular Language Search for Secure Cloud Storage,” IEEE Transactions on Cloud Computing, pp. 1–1, 2018.
3. M. Ali, M. Khan, A. Abbas, and S. Khan, “Software Piracy Control Framework in Mobile Cloud Computing Systems,” Advances in Mobile Cloud Computing Systems, pp. 257–268, 2015.
4. I. Elgendy, W. Zhang, C. Liu, and C.-H. Hsu, “An Efficient and Secured Framework for Mobile Cloud Computing,” IEEE Transactions on Cloud Computing, pp. 1–1, 2018.
5. “Platforms of Cloud Computing,” Trustworthy Cloud Computing, pp. 33–90, 2016.
6. V. Fedak, “Cloud Advancements of 2017-2018 - DZone Cloud,” dzone.com, 27-Jul-2018. [Online]. Available: https://dzone.com/articles/cloud-advancements-of-2017-2018. [Accessed: 18-Nov-2018].
7. J. Mason, “What is Advanced Encryption Standard (AES): Beginner's Guide,” TheBestVPN.com, 22-Jun-2018. [Online]. Available: https://thebestvpn.com/advanced-encryption-standard-aes/. [Accessed: 18-Nov-2018].
8. A. Awad, A. Matthews, Y. Qiao, and B. Lee, “Chaotic Searchable Encryption for Mobile Cloud Storage,” IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 440–452, Jan. 2018.
9. “How to approach cloud computing and cyber security in 2018,” Information Age, 15-May-2018. [Online]. Available: https://www.information-age.com/approach-cloud-computing-cyber-security-2018-123466624/. [Accessed: 18-Nov-2018].
10. “What is Cloud Computing Security? - Definition from Techopedia,” Techopedia.com. [Online]. Available: https://www.techopedia.com/definition/25114/cloud-computing-security. [Accessed: 11-Nov-2018].

11. Y Yang, "Towards Multi-user Private Keyword Search for Cloud Computing," 2011 IEEE 4th International Conference on Cloud Computing, 2011.
12. M. Kretzschmar, M. Golling, and S. Hanigk, "Security Management Areas in the Inter-cloud," 2011 IEEE 4th International Conference on Cloud Computing, 2011.
13. Common Standards in Cloud Computing," Cloud Computing, pp. 183–212, 2017.
14. M. Balaji and A. K. Cherukuri, "Inter-Application Based Resource Management Approach for Cloud Infrastructure," 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018.
15. P. Kamongi, "Cloud Security and Privacy Management," Security, Privacy, and Digital Forensics in the Cloud, pp. 109–127, 2019.
16. D. S. Linthicum, "Cloud Computing Changes Data Integration Forever: Whats Needed Right Now," IEEE Cloud Computing, vol. 4, no. 3, pp. 50–53, 2017.
17. S. A. Ghafour, P. Ghodous, and C. Bonnet, "Privacy Preserving Data Integration across Autonomous Cloud Services," 2015 IEEE 8th International Conference on Cloud Computing, 2015.
18. D. Tomar and P. Tomar, "Integration of Cloud Computing and Big Data Technology for Smart Generation," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2018.
19. J. Xu, "Network Information Searching Technology Research Based on Cloud Computing," 2016 International Conference on Smart Grid and Electrical Automation (ICSGEA), 2016.
20. L. Zhou, "Cloud Computing Research Vehicle Traffic Information Service System Based on Network," Applied Mechanics and Materials, vol. 727-728, pp. 944–947, 2015.

AUTHORS PROFILE

Dr. G. Syam Prasad, is Currently working as Professor in CSE at KLEF(Deemed to be University), Vaddeshwaram, Guntur . Andhra Pradesh, India. He received the B.Tech and M.Tech degrees from the Department of computer Science and Engineering , Acharya Nagarjuna University, Guntur, India in 1999 and 2004 respectively, and Ph.D. degree from the Department of Computer Science and Systems Engineering , Andhra University at Visakhapatnam, India , in 2015. His research interests include network Security, cryptography, security and privacy, image processing, Data Mining, compilers and algorithms.



J Yashvin, is currently perusing B.Tech in CSE at KLEF (Deemed to be university), Vaddeswaram, Guntur, Andhra Pradesh, India. His research interests include cloud computing, security and privacy.

S Sunil Kumar, is currently perusing B.Tech in CSE at KLEF (Deemed to be university), Vaddeswaram, Guntur, Andhra Pradesh, India. His research interests include cloud computing, security and privacy.

A Keerthi, is currently perusing B.Tech in CSE at KLEF (Deemed to be university), Vaddeswaram, Guntur, Andhra Pradesh, India. Her research interests include cloud computing, security and privacy.