

Authentication System For Secure Cloud Storage Through Digital Threat Intelligence Framework

N.Manasa, Dr.K.Shirisha, Dr.Prasantakumarsahoo
Department Of Computer Science and Engineering
Sreenidhi Institute Of Science and Technology

Abstract: In the digital era ,attacker are becoming more stronger with latest techniques to steal users data or file from the cloud server without knowing to users or cloud providers. Data owners are storing the data in encrypted form in the remote untrusted data server. Most of the users are storing their data in public clouds, they wont provide much security to users data files because these are free service providers. Even encryption of data or files are becoming less secure from the attackers. Because of new automation tools are very powerful to decrypt the encryptions. Present days man in the middle attacks are getting very popular for stealing detail of users. Its getting very hard to find them because they are changing or adding content to original data without their identity. So users are not aware of changes made in data. Proposing Digital Threat Intelligence to find out malicious persons with IP, Url, and Domain. It consumes less amount of resources and gives more efficient results with less amount of time.

Index Terms:Authorized Searchable Encryption, Cloud Computig, Digital Threat Intelligence, Malicious Activities, Threat Hunting, Traceability

1 INTRODUCTION

Passed on enlisting is the on-request transparency of PC framework assets, particularly information gathering and dealing with power, without direct extraordinary association by the client. The accessibility of high-limit systems, inconsequential effort PCs and breaking point contraptions likewise as the regardless of what you look like at it task of rigging virtualization, association planned structuring and autonomic and utility figuring has incited headway in appropriated handling. The word of cloud was used because it stores data in internet, this data can be accessible anywhere from the world , this gives good and feasible services to users. Users can select any frameworks according to his works and frame sheets. With this services users can get good internet traffic quality from the cloud services. Users don't need to buy complete hardware for their small works this service can save lot amount to users. If any kind of attacks are happened to cloud server then users doesn't need bothers for it because cloud providers always maintain backup server which can keep users data safely. [4] efficient and privacy-preserving outsourced calculation under multiple encrypted keys (EPOM) .

Using EPOM, a large scale of users can firmly source their data to a cloud server for storage. The target of appropriated registering is to allow customers to take benefit by these advances, without the necessity for significant data about or capacity with each and every one of them. The cloud intends to lessen costs and empowers the customers to focus on their middle business instead of being prevented by IT impediments. The essential enabling development for disseminated figuring is virtualization. Virtualization programming confines a physical considering device along with at any rate one "virtual" contraptions, all of which can be easily used and made sense of how to perform preparing assignments. With working structure level virtualization fundamentally making a versatile plan of different free figuring contraptions, idle preparing resources can be apportioned and used even more beneficially.

which makes especially organized circulated figuring fitting for business congruity and disaster recovery. security can improve on account of centralization of data, extended security-focused resources, etc., anyway concerns can continue on about loss of order over certain sensitive data, and the nonattendance of security for set aside parcels. Security is as often as possible in a similar class as or better than other standard structures, somewhat since authority associations can devote advantages for lighting up security gives that various customers can't stand to deal with or which they miss the mark on the specific aptitudes to address. Private cloud foundations are in part prodded by customers' hankering to hold control over the establishment and avoid losing control of information security. Present day cryptography is seriously established on numerical speculation and programming designing practice; It is theoretically possible to break such a system, anyway it is inconvenience to do as such by any known suitable strategies. Whenever developers uses the complex codes the application will huge amount of ram and cache memory in the systems.

If system doesn't has sufficient ram then system will automatically becomes slow to perform tasks which are allocated by the user. [8] Security-relevant applications need to be designed with core security-services failure-tolerant measures (referred to as security failure-tolerant services) so that they protect security assets from attacks even though the unbreakable core security services are broken. Cache memory always stores recent and temporary data which is frequently used by system to run or perform task very fastly but whenever system has low memory then system will automatically becomes very slow to perform tasks by users.

These plans are as such named computationally secure; speculative advances, e.g., updates in number factorization counts, and snappier figuring development require these responses for be continually balanced. figures were consistently used direct for encryption or unscrambling without additional

Availability improves with the usage of various tedious goals,

methodologies, for instance, approval or decency checks. There are two sorts of cryptosystems: symmetric and disproportionate. In symmetric structures a comparative key (the secret key) is used to encode and unscramble a message. Data control in symmetric systems is speedier than upside down structures as they all around use shorter key lengths. Veered off systems use an open key to encode a message and a private key to decipher it. Use of hilter kilter systems updates the security of correspondence. Essential types of either have never offered a great deal of security from aggressive foes. The Digital World is an area of pseudo-the web arranged on the framework, where digimon and other progressed life forms involve. It is a monstrous world essentially equivalent to the Real World. when ever attacker attack on servers they will get huge amount of data with low efforts. If they attack on single system they will get only very little amount of data from single user. While implementing the existing system they have used very complex algorithms which consumes lots of resources to process small amount of service or query.

This shows impact a lot on system because whenever system uses lots of resources for small works then system won't be able to allocate resources to process remaining tasks. With this type of works application won't work efficiently and cant process very fastly. To standardize this control, scholastics and specialists collaborate to offer course, procedures, and industry gauges on mystery key, antivirus programming, firewall, encryption programming, genuine commitment, security care and getting ready, and so forth. This standardization may be moreover controlled by a wide combination of laws and rules that impact how data is gotten to, arranged, set aside, moved and pulverized. Information security threats arrive in a wide scope of structures. Presumably the most broadly perceived threats today are modifying ambushes, theft of authorized advancement, discount extortion, robbery of apparatus or information, harm, and information coercion. A large number individuals have experienced programming ambushes or something like that. Diseases, worms, phishing ambushes and Trojan horses are several ordinary examples of programming attacks. There are various ways to deal with assistance shield yourself from a bit of these ambushes anyway one of the most valuable careful steps is lead periodical customer care. The primary risk to any affiliation are customers or internal specialists, they are also called insider threats.

2 EXISTING WORKS

In the existing system escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption method is used to find weather encryption and decryption are done. Free traceable attribute based system is very oldest method for tracing encryption and decryption methods. It has very low level security features , if users uses this method as their security feature then attackers will easily attack their system without knowing to user and they can take

data from system whatever they want. Not only in single system if attackers attack on server then it will be huge lose to companies because thousands of users uses companies data services, if attacker attack on server then services will interrupt and users wont access the companies services. Recent years sonyplaystation got hacked just because of poor security levels. Attackers will always tries to find new kind of ways to break security systems to get data from the servers in easy way. Because when ever attacker attack on servers they will get huge amount of data with low efforts. [7] Moderators either remove adverse comments or send them back to the users to give them the chance to reformulate. However, such tasks are both time consuming and costly.

From a national security and law enforcement perspective, it is impossible to manually monitor even a fraction of the enormous amount of activity on social media. If they attack on single system they will get only very little amount of data from single user. While implementing the existing system they have used very complex algorithms which consumes lots of resources to process small amount of service or query. This shows impact a lot on system because whenever system uses lots of resources for small works then system won't be able to allocate resources to process remaining tasks. With this type of works application won't work efficiently and cant process very fastly. To perform encryption techniques system need to perform lots of rounds to encryption of readable text to unreadable text. Based on encryption levels , rounds will be increased. Whenever encryption is in very high then system has to perform more rounds to encrypt the data in it. Rounds in the encryption means for every round it does the encryption and generates the unique key for decryption, this key will be valuable to this round only, like this in every round encryption generates unique key for decryptions but finally it gives only one key that is connected to for all keys which are generated in the encryption rounds. [9]Thereisanenormousrate of increase in threats with ever growing releases of smart devices and rapid advancement in innovative technologies. If application has vulnerability then attacker can break only application level users, which means attacker can take data from vulnerable application only because every application is different to each other so they maintain different levels of security levels and types. [6] These threats can be categorized as mobile network, mobile device, digital convergence, authentication and payment threats, and service development threats. If attackers can bypass the security levels or firewalls in the server level then attacker will get huge amount of users data.

It's very complex algorithm which is consuming lots of system resources with give less efficacy. Even encryption levels are very low which 64bit only, it leaves in vulnerable stage to users. Whenever attackers finds some vulnerable in the server or system then attackers tries to breaks in every single possible way to get into the servers or systems. Even attackers turns the vulnerable system or server to their fun things like sending

funny things to users without knowing to service providers. Whenever developers uses the complex codes the application will huge amount of ram and cache memory in the systems.

If system doesn't has sufficient ram then system will automatically becomes slow to perform tasks which are allocated by the user. Cache memory always stores recent and temporary data which is frequently used by system to run or perform task very fastly but whenever system has low memory then system will automatically becomes very slow to perform tasks by users. With this of codes in the application, system will automatically loses the efficiency in hardware also then automatically system software will takes burden to run the application without any delay but this type of applications will makes system worse and consumes huge amount of time and resource in the system.

3. RELEATED WORKS

whenever data sharing in the groups, some of group members can leak sensitive personal information to others without knowing to users. Proposing a searchable attribute-based proxy re-encryption system. With this method if user share sensitive information to others then need decryption attribute key. Because it re-encrypts the data. Whenever re-encryption has occurred then it will create new key with existing key in the encryption system .this makes good security to users database in the cloud servers[1]In the existing system KNN-SE(k-nearest neighbor for searchable encryption) has limit in practical applications. To overcome that problem, proposed MRSE system , it can support very flexible search authorization and time-controlled revocation and it achieves better data privacy protection.

Users no need to worry about their data privacy because it controls based on authorization techniques. User can keep any kind of attribute to encrypt the users data files in the cloud computing. It can handle only data files in the cloud system[2]In the existing system they have used traditional searchable encryption schemes which users can search requests over encrypted data, this schemes supports only on Boolean searches. It consumes too much of computational power and while retrieving all files it losing some of data packets. Proposing ranked search keyword system which showed great enhance system usability by returning the matching files in the ranked order in the cloud data.

It can perform operation on anything for better security reasons. It consumes low amount of computational power in the cloud computing[3]Cloud computing has lot of capability to give enormous services to user like storing and providing operations to your defined operations for user works. Proposing a toolkit EPOM(efficient and privacy-preserving outsourced calculation under multiple encrypted keys). With this method users can encrypt large scale of data in the servers. Efficient

and privacy-preserving outsourced calculation under multiple encrypted key can encrypt user complete database at a time

but when it comes to security feature it might take time taking process[4]cloud service providers may intentionally leak the users data to outside persons for their profit without knowing to users. Proposing escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption(EF-TAMKS-VOD).

It can prevent the duplication of key generation with the help of key generation center. With this users can have their own key. If cloud service providers uses duplication of key for users data then it will alert the users my mailing them or in other features[5]major information security vulnerable are created by developers because of their negligence in the implementation of applications. Whenever attack is done then it can be examined by the digital forensics. With this method attackers can be caught easily. Whenever attackers uses tools to attacks on users mobile devices with the help of vulnerabilities then mobile will note the details from the request occurred by attackers. These details can be helpful in cybercrimes to investigate the attackers details and where it happened[6]whenever attacker attack on users devices they have to connect through IP or url, so in digital forensics it will connect IP address or url based connectivity attacker can caught with the digital forensics. Presentdays attackers Are using latest techniques to hide or cover their path do not to caught by any digital forensics.

4. PROPOSED SYSTEM

Proposing Digital Threat Intelligence, it works based threat formed by users in the server or online in the application, it catches the malicious threats in the application with the help of IP's, URL's and domain and Hash of malicious files. Every malicious file contains signature and hash value for the virus or malware. Users will upload their data file by logging into the application, if user uses wrong credentials then application wont allow into the application and cant be able to upload the data files into server. Once users uploads data files into the application then application will connects to Digital Threat Intelligence. The Digital Threat Intelligence will finds them by using the blacked listed IP's , URL's , Domain and Hashes. Checks for virus,Malwares and .bat files.Moreover it mainly checks malicious IP's, malicious domains,Malicious URL's and latest malicious Hashes.

Digital Threat Intelligence uses the user defined intelligence to catch the malicious attackers or users in the application. Servers always contains very sensitive information, to get this sensitive information from the servers attacker uses the latest vulnerable scanners to find vulnerabilities in the server or application. If attackers find any small issue in the application or server then attackers got the jack pot. If attackers can bypass the security levels or firewalls in the server level then attacker will get huge amount of users data. If application has vulnerability then attacker can break only application level users,

which means attacker can take data from vulnerable application only because every application is different to each other so they maintain different levels of security levels and types.

More over servers always maintains firewalls if attacker can bypass the server firewall then no-one can stop attacker because once attacker bypass then server firewall then attacker can do any changes in any application or even attacker can crash the server or can delete the applications. Because attackers uses weak secure domains and creates new malicious URL's and spoofed IP's to get connection with user. Viruses and malwares are in excel sheet format which contains their hashes. Ip's, domains, Hashes and url's will be in text format which will checks with everything to find malicious. With the proposed system malicious threats can be easily catch them.

It works with low resources with efficiently in small computers also. To run the application it doesn't required many resource like other applications, it can manage limited resource also because all users cant afford the high configuration in the systems. It doesn't eat too much of memory in the computers or in the servers, it always tries to use very low amount RAM or resource in the system. With this type of requirements system can run very efficiently , when it comes to application it works very fast and smooth without any lagging in the system to process then tasks in the system. Encryption levels have been upgraded to RSA 256bit level which makes very hard to crack them to attackers. RSA encryption does 14 rounds of encryption. In every round it generates unique key and that key will be used for that round only and next round will generate another key for doing encryption.

The conversion of plain text to unreadable text , it doesn't take much time to do encryption. Moreover its very powerful and very secure one in the encryption system. It encrypts with the help of public key from the users but when it comes in the rounds of encryption it will start works in different way because not to caught by the attackers. With the upgraded encryption levels users can safely store their data in the server without any doubt. If any attacker wants to break the encryption levels then it will take years to break the security of encryption levels. With the encryption levels attacker cant break user files in the server or application.

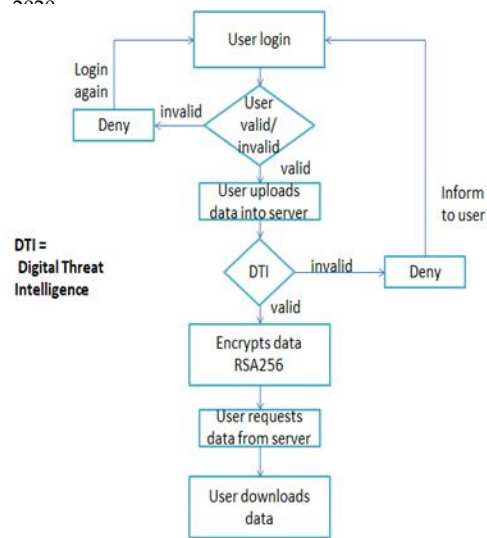


Figure1: The Architecture of Proposed System

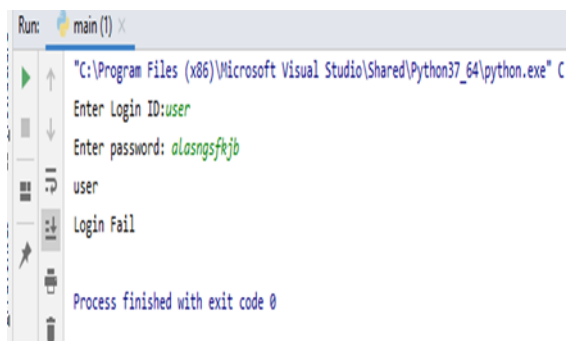
5. Input and Output Screenshots:

Finding user IP and check with DTI

```

    "C:\Program Files (x86)\Microsoft Visual Studio\Shared\Python37_64\python.exe" C:/Users/Sujatha/Documents/project/efficient/dti.py
    Enter Login ID:user
    Enter password: admin
    user
    Login success
    Hostname : DESKTOP-DOINF4UT
    IP : 192.168.56.1
    DigitalThreatIntelligence
    192.168.56.1 Not Malicious
    enter the file name with complete extension
    
```

Login Fail



```
Runc: main() x
"C:\Program Files (x86)\Microsoft Visual Studio\Shared\Python37_64\python.exe" C
Enter Login ID:user
Enter password: aLasngsfkjb
user
Login Fail
Process finished with exit code 0
```

10.1109/SocialCom.2013.89.
[9] EzhiKalaimannan, "Smart Device Forensics - Acquisition, Analysis and Interpretation of Digital Evidences", 2015 International Conference on Computational Science and Computational Intelligence, 978-1-4673-9795-7 2015 U.S. Government Work Not Protected by U.S. Copyright DOI 10.1109/CSCI.2015.58.
[10] Kennedy A. Torkura, Muhammad I.H. Sukmana, Feng Cheng and ChristophMeinel, "SlingShot - Automated Threat Detection and Incident Response in Multi Cloud Storage Systems", 978-1-7281-2522-0/19/\$31.00 ©2019 IEEE.

4 CONCLUSION

Digital Threat Intelligence have been successfully developed and getting very positive results while finding the malicious threats. Even it works and finding malicious threats in Domain based request to application or server. Users can easily upload their files safely to sever by using application because encryption levels has increased to 256bit levels previous we have only 64bit encryption so its getting easier to attacker to break them, now its has increased to 256bit level its impossible to break this encryptions. It consumes very less amount of resources and works very efficiently.

REFERENCES

[1] Kaitai Liang and Willy Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage", Citation information: DOI 10.1109/TIFS.2015.2442215, IEEE Transactions on Information Forensics and Security.
[2] Yang Yang, Ximeng Liu, Robert H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language", Citation information: DOI 10.1109/TDSC.2017.2787588, IEEE Transactions on Dependable and Secure Computing.
[3] Cong Wang, Ning Cao, Jin Li, Wenjing Lou and kuiren, "Secure Ranked Keyword Search over Encrypted Cloud Data", 2010 International Conference on Distributed Computing Systems, 1063-6927/10 \$26.00 © 2010 IEEE.
[4] V.Sumalatha&Dr.Santhi. R, "An Efficient Privacy-Preserving Outsourced Calculation Toolkits with Multiple Keys", Volume 119 No. 15 2018, 3589-3599 ISSN: 1314-3395 (on-line version) url: <http://www.acadpubl.eu/hub/>.
[5] Yang Yang, Ximeng Liu, XianghanZheng, ChunmingRong, WenzhongGuo, "Efficient Traceable Authorization Search System for Secure Cloud Storage", Citation information: DOI 10.1109/TCC.2018.2820714, IEEE Transactions on Cloud Computing. IEEE TRANSACTIONS ON CLOUD COMPUTING.
[6] PasiAhonen, ReijoSavola, "Security Threats to Mobile Service Development in the Age of Digital Convergence", 1-4244-0049-X/05/\$20.00 (C2005 IEEE).
[7] Hugo L. Hammer, Michael A. Riegler and LiljaØvrelid, Erik Velldal, "THREAT: A Large Annotated Corpus for Detection of Violent Threats", 978-1-7281-4673-7/19/\$31.00 ©2019 IEEE.
[8] Michael Shin; SwethaDorbala; Dongsoo Jang, "Threat Modeling for Security Failure-Tolerant Requirements", 978-0-7695-5137-1/13 \$26.00 © 2013 IEEE DOI