RESEARCH ARTICLE OPEN ACCESS

A PROFICIENT PRIVACY PROTECTION METHOD FOR CLOUD COMPUTING

Ms. N. Zahira Jahan, M.C.A., M.Phil.,[1], Mr. S. Vijay[2],

[1]Associate Processor, Department in Computer Applications,

Nandha Engineering College, (Autonomous), Erode – 638 052, Tamil Nadu, India

[2]Final MCA, Department in Computer Applications,

Nandha Engineering College, (Autonomous), Erode – 638 052, Tamil Nadu, India

[1]zahirajahan1977@gmail.com, [2]vijayshanmugam24072000@gmail.com

Abstract. With the rapid development of Cloud computing, further Cloud services are into our daily life, and therefore security protection of Cloud services, especially data privacy protection, becomes more important. Still to perform privacy protection causes huge outflow. Therefore it's a critical issue to perform the most suitable protection to decline performance consumption while give privacy protection. In this design, the Complete Sequestration Protection Scheme (CSPS) is proposed to give the applicable privacy protection which is satisfying the stoner- demand privacy demand and maintaining system performance contemporaneously. At first, the privacy position is anatomized by druggies those bear and quantify security degree and performance of 3DES and AES encryption algorithms. Also, an applicable security composition is deduced by the results of analysis and quantified data. Eventually, the simulation results show that the CSPS not only fulfills the stoner- demand privacy but also maintains the Cloud system performance in different Cloud surroundings.

Keywords: Cloud Computing, Cryptography, Symmetric Encryption, Third Party Auditing.

I. INTRODUCTION

Cloud computing is rising as the most suitable paradigm for individualities and associations to pierce affordable, scalable, ubiquitous, and on- demand computing coffers, operations, and data storehouse services. Cloud storehouse systems, similar as Dropbox, Google Drive, Apple's iCloud, Microsoft OneDrive,etc., enable druggies to ever store a large volume of data that can be penetrated and participated among druggies, anyhow of time and position constraints. With the growing fashionability of Cloud computing, the number of enterprises and individualities shifting toward the use of Cloud has increased fleetly.

As a result, a vast quantum of important particular information and critical association data, similar as particular health records, government documents, and company finance data, etc., are transmitted across the Internet and stored in Cloud waiters. Still, outsourcing sensitive data suffers from critical security pitfalls, sequestration, and access control problems.

These are common enterprises of associations and individualities using Cloud services. When data possessors resettle their sensitive data to the pall, they lose an element of control over their data. Cloud druggies have no guarantee about the way these sensitive data will be treated and defended by Cloud providers.

Although the Cloud provides druggies with the convenience of data access across multiple bias, by using Cloud services, stoner data are vulnerable to a verity of vicious attacks and pitfalls. Security incidents do constantly. Indeed worse, Cloud service provider may blunder stoner data to unauthorized realities for illegal profit.

One doable result to overcome these problems is to use cryptography. All sensitive data have to be translated by data possessors previous to storing them into the potentially untrustworthy pall. The strength of the encryption scheme is largely dependent on the strength of the crucial operation fashion used. The security of the encryption scheme lies on the secretiveness of the keys that are known only to the druggies authorized to read their separate data, and not only on the secretiveness of the encryption algorithm used.

Given the quantum of data being stored and participated in Cloud and the adding number of data druggies, designing a cryptographic scheme for Cloud storehouse that meets the conditions of security, effectiveness, ease of use, and inflexibility is a grueling task. Traditional encryption operations, generally, suffer from limited usability due to the homemade result handed by operations. Data possessors must cipher their data manually prior to uploading to the pall. Also, druggies have to manually induce, manage, and store the encryption keys.

Still, the involvement of data possessors in performing multiple encryption and decryption operations is clumsy and time consuming. Also, it's delicate for druggies to manage further than a many keys, and if the keys are blurted or else compromised, security will be hovered. Encryption operations are designed to be bandwidth-empty and quiescence-sensitive, in which the increased number of outsourced lines taking encryption would significantly affect the system performance and data access response time.

Recent works manage with the limitations of the encryption operations by espousing a transparent encryption approach. This type of encryption medium is enforced most effectively with the help of operating system train systems. The common approach is composed of a customer operation that interacts with the original cryptographic train system, and the translated data are accompanied or backup to connected back- end Cloud storehouse waiters. In this design, In this script, the situations can be seen as the kinds of speed, mongrel, and security.

They're explained as follows.

1 (Speed) The demand of this position presents that no sensitive information in the data. Druggies want to use the weak encryption composition to gain further performance for using Cloud services.

2 (Hybrid) The demand of this position presents that data include some sensitive information. The data requires weak encryption for partial data (similar as address, correspondence id of corporates') and strong encryption for remaining data (similar as account balances and other secure information).

3 (Security) In this sequestration position, the data contains most important information. In order to cover the data security, further privileged druggies view utmost of the data and lower privileged druggies view limited data.

• To cipher/ decipher the data of lower significance using weak encryption system so that communication is fast.

• To cipher/ decipher the partial data using weak encryption system and other partial data in strong encryption system so that communication is fast and security position is raised.

• To cipher/ decipher the some fields using strong encryption system and some other fields using weak encryption system so that all fields are displayed to high honor druggies and some fields are displayed to low privileged druggies.

• To cipher/ decipher the watermarked contents with weak encryption system and non-watermarked contents with strong encryption system.

II. LITERATURE REVIEW

In this paper [1], the authors stated that the adding volume of particular and sensitive data being gathered by data regulators makes it decreasingly necessary to use the cloud not just to store the data, but also to reuse them on cloud demesne. Still, security enterprises on frequent data breaches, together with lately upgraded legal data protection conditions (like the European Union's General Data Protection Regulation), advise against outsourcing vulnerable sensitive data to public shadows.

To attack this issue, this check covers technologies that allow sequestration-apprehensive outsourcing of storehouse and processing of sensitive data to public shadows. Specifically and as a novelty, they reviewed masking styles for outsourced data grounded on data splitting and anonymization, in addition to cryptographic styles covered in other checks. They also compared these styles in terms of operations supported on the masked outsourced data, above, delicacy preservation, and impact on data operation. Likewise, they listed several exploration systems and available products that have materialized some of the surveyed results. Eventually, they linked outstanding exploration challenges.

Numerous companies are outsourcing at least some of their information technology to the cloud, from bare data storehouse to e-mail and other productivity operations. Reduced costs, no need for conservation, nearly unlimited computational coffers and increased vacuity are the main forces driving this change. Yet, security and sequestration misgivings are still cardinal walls hindering a countersign migration to the cloud. Security is defined as achieving confidentiality, integrity and vacuity of the data outsourced to the cloud. Druggies want to be assured that no meddler can hack the cloud and/ or impersonate them to steal or alter their sensitive data, and that no denial of service will do. In the E.U., 57 of large enterprises using the cloud reported the threat of a security breach as the main limiting face scarpment in the use of cloud computing services [4]; in a check by the cloud Security Alliance to over 165 information technology and security professionals in the U.S., utmost of the repliers considered cloud storehouse as high threat [5]; the European Network and Information Security Agency linked " loss of governance" over the data outsourced to the cloud as a critically inhibiting factor [6].

Security breaches are, in fact, veritably real pitfalls. Some well- known exemplifications include the Sony PlayStation Network outage 1 as a result of an external intrusion, in which particular details from roughly 77 million accounts were stolen, the multi-day outage in Dropbox 2 that temporarily allowed callers to .log into any of its 25 million client accounts as a result of a misconfiguration, or the leakage of private filmland of a number of celebrities from the Apple iCloud storehouse service due to weakly defended login credentials [6].

Regarding privacy, it is most widely approved definition in information society is in informational self-determination terms, that is, "the claim of individuals, groups or institutions for determining for themselves how, when, and to what level, information about them is spread to others" [7].

Hence, for a cloud user to store and/or process sensitive data in the cloud, she needs the guarantee that no one other than herself not even the CSP will be capable of chekcing

or inferring the user's data. Thus, cloud computing methods have to improve the user's control on data, which will reduce the need for users blindly trusting the providers. Otherwise, a user might be reluctant to give their sensitive data to the cloud service providers.

In addition, when data are private i.e., personal, individuals to whom the data referred have privacy rights which have recently European Union's GPDR (General Data Protection Regulation) enshrined. To stay with GDPR-compliant, the data controller an entity that obtained consent from subjects for collecting, storing and processing their data may only outsource subject data to cloud if that user can get full control and confidentiality for outsourced data. The above is an important issue because GDPR is also becoming a de facto legal standard outside EU, especially in Australia, USA, Japan and Canada, and any companies wish to sale information technology solutions to the markets must consider it into account.

In fact, reports by U.S. Federal Trade Commission [5] stated that public CSPs collect and analyze the data of their users regularly without latter's knowledge, and that those analyses could yield sensitive inferences; for example, a CSP could detect individuals that suffer from diabetes because of their interest in sugar-free products and share this information with an insurance company that could use that clue to classify a person as higher-risk (and possibly higher-premium).

There are several legal issues here. Meanwhile, in most of the scenarios, the data subjects entrust data controller with their private data (e.g., healthcare industry data), but this doesn't mean they allowed the controller to further transfer the data to whomever controller chooses to believe. The CSP is under U.S. law but controller as well as subjects are under E.U. law and those may be violated.

Eventually, numerous public CSPs offer their services free of charge in return for the possibility of monetizing druggies'data. For illustration, a recent sequestration policy in Google [8] specifies that whatever information a stoner decides to outsource to any Google service can be used, reproduced, modified or distributed by Google with the end of perfecting or promoting its services, but also to conduct targeted advertising (e.g., the Gmail filtering system scans the content of our emails to serve individualized advertisements). To assuage the below issues and restore the stoner's control and trust on the protection of the data outsourced to the cloud, several results have been proposed in recent times. All of them involve masking sensitive data so that only defended values are stored in the cloud and only the stoner/ regulator retaining the data is suitable to unmask the defended values recaptured from the cloud.

Still, if the stoner wants to use not only the cloud's storehouse but also the cloud's computational power, the challenge is indeed harder, because data protection should be made compatible with outsourced calculations on cloud demesne on masked data In this paper we survey the state of the art on security and sequestration- enabling results towards the cloud, with a focus on those that save cloud service functionalities, similar as the capability to outsource queries and computations on defended data to the cloud. In comparison with recent checks on this area, ours offers the following benefactions:

• Utmost checks concentrate on data security vs external bushwhackers [9-12] rather than on sequestration versus the cloud. Thus, they center their analysis on security attacks and on mechanisms to help, descry and alleviate them. In discrepancy, our check considers mechanisms that cover outsourced data not only against third- party bushwhackers, but also against interposers and honest-but-curious shadows 6 storing and managing similar data.

• Numerous checks concentrate on outsourced data storehouse [11-13]. Their paper goes a step beyond and puts the limelight on the preservation of cloud service functionalities (e.g., queries, computations, etc.) on the defended data outsourced to the cloud. Taking advantage of the cloud's computing power on defended data is significantly further grueling than simply using the cloud to store defended data.

• All checks covering sequestration- enabling service preservation mechanisms are limited to cryptographic results [14-15].

Indeed though these styles are important to secure data, they also affect in significant computation charges (which incompletely neutralize the cost- saving benefits of cloud computing), they bear crucial operation, and they oppressively limit cloud functionalities on the outsourced data because they need acclimatized results for each type of outsourced computation [15].

They also studied cryptographic results but, for the first time, they exhaustively survey non-cryptographic styles (grounded on data splitting and anonymization) that can be used to efficiently cover data outsourced to the cloud while conserving a variety of cloud services. In addition to the security enabling results proposed in the literature, they surveyed exploration systems and products that apply some of these styles in the cloud script and bandy the outsourced functionalities they support.

They concluded that their analysis complements other checks in the field by i) considering the analysis issues related to data outsourcing to (untrusted) public shadows; ii) fastening on the preservation of pall functionalities on outsourced data (beyond bare data storehouse); iii) surveying functionality- conserving data protection ways not only grounded on (precious) encryption, but also on (more effective and flexible) anonymization and splitting; iv) comparing the surveyed ways and v) relating exploration systems and products that offer analysis-enhancing and functionality- conserving results for the pall or that can be employed to apply data protection delegates.

Each of the three examined data protection approaches (data splitting, anonymization and encryption) has its pros and cons, that have been anatomized over. Challenges for

unborn exploration include mollifying some of the linked limitations, especially when it comes to outsourcing big data or at any rate large volumes of data.

In this paper [2] the authors stated that pace of connecting physical devices around us to the Internet is adding fleetly. According to a recent. Gartner report, there will be around8.4 billion connected effects worldwide in 2020. This number is anticipated to grow to20.4 billion by 2022 [1]. The use of IoT operations is adding in all corridor of the world. The major driving countries in this include western Europe, North America, and China [1]. The number of machine to machine (M2M) connections is anticipated to grow from5.6 billion in 2016 to 27 billion in 2024.

This vault in figures itself declares IoT to be one of the major forthcoming requests that could form a foundation of the expanding digital frugality. The IoT assiduity is anticipated to grow in terms of profit from$ 892 billion in 2018 to$ 4 trillion by 2025. M2M connections cover a broad range of operations like smart metropolises, smart terrain, smart grids, smart retail, smart husbandry, etc.

The history, present and unborn armature Internet of effects (IoT) is the coming period of communication were studied. Using IoT, physical objects can be empowered to produce, admit and change data in a flawless manner. Colorful IoT operations concentrate on automating different tasks and are trying to empower the insensible physical objects to act without any mortal intervention. The being and forthcoming IoT operations are largely promising to increase the position of comfort, effectiveness, and robotization for the druggies. To be suitable to apply such a world in an ever growing fashion requires high security, analysis, authentication, and recovery from attacks.

In this regard, it's imperative to make the needed changes in the armature of IoT operations for achieving end-to- end secure IoT surroundings. In this paper, a detailed review of the security- related challenges and sources of trouble in IoT operations is presented. After agitating the security issues, colorful arising and being technologies concentrated on achieving a high degree of trust in IoT operations are bandied. Four different technologies Blockchain, fog computing, edge computing, and machine literacy to increase the position of security in IoT are bandied. of IoT.

In future, the devices aren't only anticipated to be connected to the Internet and other original devices but are also anticipated to communicate with other devices on the Internet directly. Piecemeal from the devices or effects being connected, the conception of social IoT (SIoT) is also arising. SIoT will enable different social networking druggies to be connected to the devices and druggies can partake the devices over the Internet.

With all this vast diapason of IoT operations comes the issue of security and analysis. Without a trusted and interoperable IoT ecosystem, arising IoT operations cannot reach high demand and may lose all their eventuality. Along with the security issues faced generally by the Internet, cellular networks, and WSNs, IoT also has its special security challenges similar as analysis issues, authentication issues, operation issues, information storehouse and so on.

Due to all these issues and vulnerabilities, the IoT operations produce a rich ground for different kinds of cyber pitfalls. There have been colorful security and analysis attacks on the formerly stationed IoT operations worldwide. Mirai attack in the last quarter of 2016 was estimated to infect around2.5 million devices connected to the Internet and launch distributed denial of service (DDoS) attack. After Mirai, Hajime and Reaper are the other big botnet attacks launched against a large number of IoT devices.

III. PROPOSED METHODOLOGY

Cloud computing is an emerging computing style which provides dynamic services, scalable and pay-per-use. The different between cloud computing and other computing models are service- driven, participating resource, and data hosting in outsourcing storehouse. Sharing resource makes the hardware performance be used more efficient and provides economic benefits for users to reduce the capital cost and additional expenditure.

In the existing system, the privacy level is divided into three levels, since it is believed that users can not clearly distinguish between their privacy requirements more than three levels. In this scenario, the levels can be seen as the kinds of speed, hybrid, and security. They are explained as follows.

• Privacy Level 1 (Speed): The requirement of this level presents that no sensitive information in the data. Users want to use the weak encryption composition to gain further performance for using cloud services. Here only 3DES encryption technique is used.

• Privacy Level 2 (Hybrid) The demand of this position presents that data include some sensitive information. The data requires weak encryption for partial data (similar as address, correspondence id of corporates') and strong encryption for remaining data (similar as account balances and other secure information). Here both 3DES and AES encryption techniques are used.

• Privacy Level 3 (Security) In this sequestration position, the data contains most important information. In order to cover the data security, further privileged users view utmost of the data and lower privileged users view limited data. Here only 3DES encryption technique is used.

• The traditional debit of cloud computing is that since the structure of the sharing resource stored and reused

druggies'data that don't possessed by them, druggies'data may be revealed or traduced by other vicious stoner in the cloud.

• Since encryption and decryption medium increase the processing and outflow, it reduces the overall effectiveness.

• Since all the data is handled with same protection medium, unwantedover-security is applied.

• If same honor is given to all kind of druggies, tight security can't be maintained.

In the proposed system, the existing privacy levels which were divided into three levels seen as the kinds of speed, hybrid, and security are implemented. In addition content type wise security is provided. In this aspect, some of the document types such as already watermarked images and audio content are given less security and accessed by all kind of users whereas normal content are given more security i.e., strong cryptography is applied. This reduces the processing and communication overhead since the secure breach is not a major concern in terms of watermarked content.

IV. FINDINGS

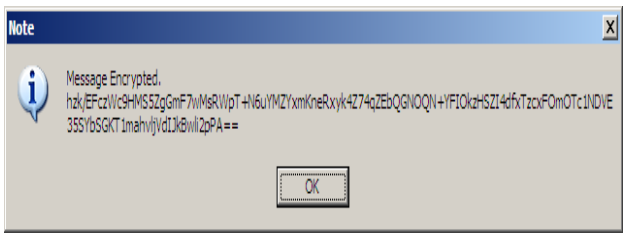
• Since different levels of encryption and decryption mechanism are applied, the processing and storage overhead is different and reduced in most of the situation.

• Since the different data is handled with same protection mechanism, communication overhead is also reduced.

• Different privilege is given to different kind of users, so tight security need not be maintained.

• Different content types can be accessed with different security level and so speed is increased.

• Security is increase as both 3DES and AES partially is used to encrypt the single text message.



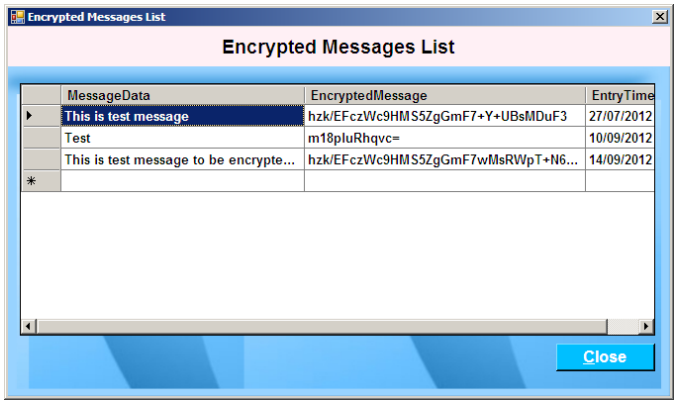


FIG 4.1 ENCRYPTED MESSAGES LIST

V. CONCLUSION

Through this design, the problem of secure communication is excluded. In addition, the operation needs less working experience in systems to run the software. The operation is tested well so that the end users use this software for their whole operations.It is believed that nearly all the system objects that have been planned at the inception of the software development have been net with and the implementation process of the design is completed. A trial running of the application has been made and found that it gives good results and the processing is found to be simple and in proper order. The process of preparing plans been missed out which might be considered for farther revision of the operation. The design effectively stores and retrieves the records from the cloud space database server. The records are translated and deciphered whenever necessary so that they're secure. The following advancements should be made in upcoming developments. The operation if developed as web services, also numerous operations can make use of the records. The data integrity in cloud environment isn't considered. The error situation can be recovered if there's any mismatch. The web appication and database can be hosted in real cloud space during the implementation.

REFERENCES

[1] J. Domingo-Ferrer, O. Farràs, J. Ribes-González, and D. Sánchez, ‘‘Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges,’’ Comput. Commun., vols. 140–141, pp. 38–60, May 2019.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, ‘‘A survey on IoT security: Application areas, security threats, and solution architectures,’’ IEEE Access, vol. 7, pp. 82721–82743, 2019.

[3] H. Deng, Z. Qin, Q. Wu, Z. Guan, R. H. Deng, Y. Wang, and Y. Zhou, ‘‘Identity-based encryption transformation for flexible sharing of encrypted data in public cloud,’’ IEEE Trans. Inf. Forensics Security, vol. 15, pp. 3168–3180, 2020.

[4] Eurostat, Cloud computing - statistics on the use by enterprises (Dec. 2016 (Accessed 14 February 2019)). URL http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

[5] C. S. Alliance, Cloud usage: Risks and opportunities report (Sep. 2014 (Accessed 14 February 2019)). URL https://downloads.cloudsecurityalliance.org/initiatives/collaborate/netskope/Cloud_Usage_Risks_and_Opportunities_Survey_Report.pdf

[6] T. Haeberlen, L. Dupr´e, Cloud computing. benefits, risks and recommendations for information security (rev. b), European Network and Information Security Agency (Dec. 2012).

[7] A. Westin, Privacy and Freedom, Atheneum, 1967.

[8] E. Ramirez, J. Brill, M. K. Ohlhausen, J. D. Wright, T. McSweeny, Data brokers: A call for transparency and accountability, U.S. Federal Trade Commission (May 2014).

[9] M. A. Khan, A survey of security issues for cloud computing, Journal of Network and Computer Applications 71 (2016) 11–29.

[10] S. Singh, Y.-S. Jeong, J. Park, A survey on cloud computing security: Issues, threats, and solutions, Journal of Network and Computer Applications 75 (2016) 200–222.

[11] A. Singh, K. Chatterjee, Cloud security issues and challenges: A survey, Journal of Network and Computer Applications 79 (2017) 88–115.

[12] P. Praveen-Kumar, P. Syam-Kumar, P. Alphonse, Attribute based encryption in cloud computing: A survey, gap analysis, and future directions, Journal of Network and Computer Applications 108 (2018) 37–52.

[13] N. Kaaniche, M. Laurent, Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms, Computer Communications 111 (2017) 120–141.

[14] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, R. Buyya, Ensuring security and privacy preservation for cloud data services, ACM Computing Surveys 49 (1) (2016) Article No. 13.

[15] Z. Shan, K. Ren, M. Blanton, C. Wang, Practical secure computation outsourcing: A survey, ACM Computing Surveys 51 (2) (2018) Article No. 31.