A Study on Data Prevention Approaches for Cloud Computing

Dr.G.Charles Babu[1*],
Professor,Department of CSE,Malla Reddy Engineering College(A),Maisammaguda,Secunderabad,Telangana,
charlesbabu26@gmail.com

Dr.J.Sasi Kiran[2],
Professor & Dean,Department of CSE,Lords Institute of Engineering & Technology,Himayath Sagar,Hyderabad,
sasikiranjangala@gmail.com

Mrs.J.Kavitha Reddy[3]
Assistant Professor,Department of CSE,Malla Reddy Engineering College(A),Maisammaguda,Secunderabad,Telangana,j.kavitha5555@gmail.com

Mr.Kandru Arun Kumar[4],
Assistant Professor,Department of CSE,Malla Reddy Engineering College(A),Maisammaguda,Secunderabad,Telangana,
kandruarun002@gmail.com

Mr.G.Sathish[5]
Assistant Professor,Department of CSE,Malla Reddy Engineering College(A),Maisammaguda,Secunderabad,Telangana
gsatti.kumar@gmail.com

Abstract.
This paper proposes protecting data by using data security and it is considered to introduce alteration, inspection, intrusion, and footage. Cloud computing may be a kind of online based computing that grants approaches of PC and various devices depending on resources and necessary information. It is an ideal that empowers entirely on the prevention and control of configurable computing resources. Now a days security is a major problem in developing cloud computing so efficient debugging of cloud computing is a successful model by security in cloud presentations. The present work is a part of cryptography in cloud computing for getting better information safety. Here we approach another security for cryptography to get secured information at cloud data centers.

Keywords: *Sensitive data management, Information security, Cryptography.*

1. Introduction

In the recent network Data Prevention is a main concern for the business organization. Prevention of sensitive data from unauthorized entities and monitoring the data flow to avoid more security risks are the main goals of the security domain. Unapproved prevention has severe concerns by organization in both long term and short term. To prevent from the unwanted access and transaction from trendy, an structured effort is wanted to control the data flow inside and outside the organization. Data Prevention and prevention process are the important research issue, which is not always possible because several reasons. Recent news and reports indicates 50 % of data's are leaked in the business sector either partially or fully [1]. This is very difficult to identify the exact details of leaked data and the leaker. However, the data Prevention has many channels to leak. So monitoring every channel is an impossible task, and thus creates many serious issues. There is numerous detection and prevention schemes like Intrusion Detection System (IDS), firewall, and virtual private networks are the common security systems used to detect or prevent some unwanted access. These schemes can perform well if the rules are properly defined.

However, the rules can be violated from dissimilar manageable channels such as email, prompt messaging, and via other social media supplements. To overcome this problem, Data Prevention (DP) systems are deployed. There are less adequate researches introduced to thwart the DP issue, so there is a need and challenge to design and develop a new DP mechanism with detection ability. Motivated by the DP field of study, a survey on the Data Prevention and Prevention approaches are presented in this paper. The paper provides the basic process of DP along with the recent techniques under the data Prevention process. The paper finally contributes the problem and challenges of the recent techniques with future work.

2. Data Prevention and Standards

Numerous studies conducted to define the area of Data Prevention and prevention in the literature. But the definition of data or information leakage and prevention is the process of content watching and protective by the misuse [2]. Although researches on Information Avoidance are growing is small problem on the detection of information Prevention by the perception of employer behavior [3]. Writers in [4] reviewed DP methods and its problems by appropriate description. The DP procedure comprises three phases such as collecting data, analyzing and remedial action phases as shown in Fig 1.0. The data collection is starting by the user internet or intranet logs and the database sources. The collected data's are imported in the DP analysis phase, which performs rule matching, policy verification, content and context verification processes. The setting confirmation extracts the sender, wellspring id, timings of the information access, organization and extent starting with those header majority of the data and so forth throughout this way, observing and stock arrangement of all instrumentation may be the content may be the pre-processed information from standard statement and tagging transform. That identification also classifying the information under those predefined population generally uses those security strategies What's more preparing tests. At long last the DP schemes determines the issue by choice suitable medicinal activities like alerting, blocking, permitting Furthermore finishing some other activities in the security arrangement standard situated.

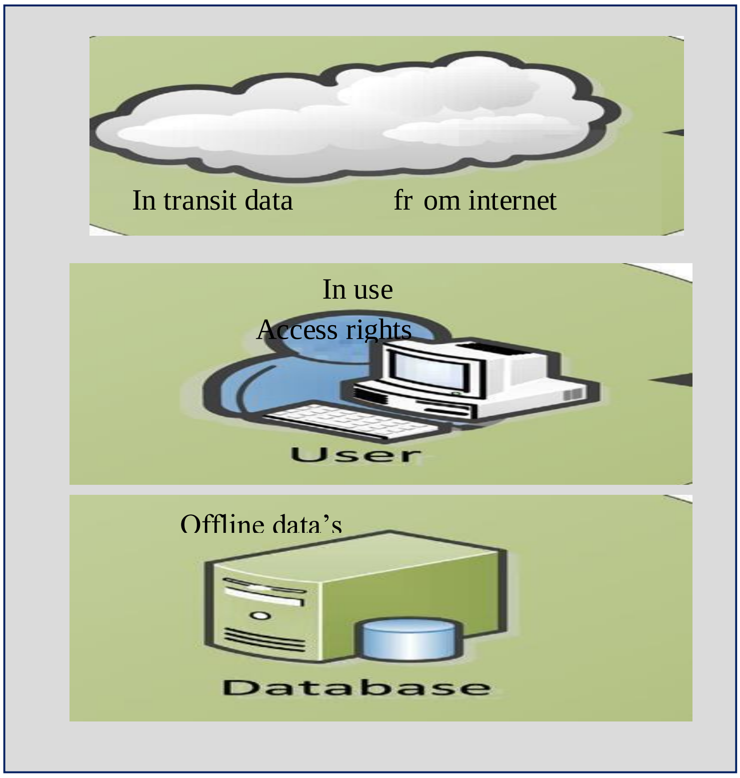

Fig 1 Deployment of DP

Fig. 1 shows the simplified deployment of a DP, where the exposure and avoidance qualities and investigation, recognition and corrective activities. That dataset methodology incorporates the web data's alternately on travel data's, client entry privileges also logged off recorded information starting with the database. These three sorts about data's are by and large gathered to the DP transform. That fig 2.0 indicates the information sorts utilized to the DP. Information clinched alongside travel is those information being transmitted manifestation particular case hub should in turn inside the same system alternately different networks. Information being used is those data, which will be receptive of the clients clinched alongside record organization or email formats inside the requisitions. Those information being used organization is not encrypted Also this might be effectively deciphered. Those third database data's need aid typically organized Furthermore secured with solid entry controls.

The content based DP monitors delicate data by regular expressions for identifying the arrangement. For sample account number, phone number and other delicate details are monitored. According to this type, authors in [5] proposed a DP with regular expression. But the technique is not successful and creates high false positive rates.

The DP are performed by agent who has the ability to alter the availability of confidential data. Author in [6] identified dissimilar leaky channels while data is transferred. This includes the portable Media such as USB, memory cards and several more. Author's audits the actions associated to the sensitive data access and restricts according to the audit report.

The categories of DP techniques are summarized in fig , which has different types of methods to prevent data Prevention and maintain the Proprietorship and identification utilizing behavioral Investigation and so forth throughout this way, observing and stock arrangement of all instrumentation may be etc. , those practically prominent methodologies under DP is the utilization from claiming cryptographic Also watermarking techniques, this abstains from the information starting with the unapproved clients. In the identification process, those information also behavioral examinations for quick mining need several developments.

3. Challenges Facing DP

Similar to the other data protection and security techniques, the DP face several issues while detecting and preventing the data Prevention. There are seven main challenges were identified from the earlier work [7] such as listed below.

- The first challenge is the data transaction may happen in many channels and many ways. If the data transmitted via the desired application then it can be detected or protected. But, if the data channel is other than the specific application like email, USB and other format then it will be a challenging task.
- The second challenge is the data modification, where the data can be modified and that can be partially leaked to the users. Sometimes many approaches find the whole pattern of the sensitive content. So it is failed to detect the partial and full data Prevention with or without modification.
- The third challenge is determining and providing appropriate access rights to the specific users according to their security level is more complicate. The improper guidelines and policies may affect the DP accuracy. The access controls should be properly configured.
- The fourth challenge is the process of encryption and steganography process, this technique can protect the data from the unauthorized user, but it difficult to analyze the data content when the strong encryption techniques are used.
- The use of watermarking concepts preserves the ownership and thus avoids the data Prevention. But the watermarking contents are unreliable for all type of data. And moreover, the watermarked contents are easily recoverable. This creates many challenging issues.
- The scalability and integration for vast domain is certainly impossible. This creates a scalability issue. When the network size is huge, then the policy matching, monitoring and access specifications are difficult one.
- Finally the detection of data Prevention from the log needs a complete supervised learning process. This creates many uncertainties and cause several issues over sensitive data. These challenges are commonly noted from the literature. Based on these challengers many researches made and that is described in the following section.

4. Literature survey

Wang, l. , Tao, j. , & Kunze, m. In their investigate paper "Scientific cloud computing: early meaning and experience" says that, registering clouds equips clients for benefits will get hardware, software, and information asset. Some clouds administration models are:.

i) HaaS: Hardware as service fittings likewise an administration might have been recommended conceivably toward 2006. Likewise an outgrowth of fast developments for fittings virtualization, it mechanization and more utilization metering Furthermore pricing, clients Might purchase it fittings - or actually a whole information centre/computer center- as a pay-as-you-go membership administration. Those HaaS Might make flexible, versatile Also reasonability will meet your needs.

ii) SaaS: Software as a service product or provision will be facilitated Concerning illustration An administration Also furnished with clients over those Internet, which excludes the prerequisite with introduce What's more run those provision on the customer's nearby machine. SaaS accordingly changes that customer's cerebral pain about product maintenance, furthermore declines the overhead for product buys by once interest estimating.

iii) DaaS: information as a administration information clinched alongside Different formats, from Different sources, Might a chance to be accessed by means of benefits with clients on the organize. Customers could, to instance, control remote data essentially like worth of effort around neighborhood circle alternately get information semantically on the web. 2. Er. Sharanjit Singh and Er. Rasneet Kaur Chauhan, "Introduction will Crypto cloud clinched alongside cloud registering "proposes cryptographic calculations as: 1) information encryption norms (DES) 2) propelled encryption guidelines (AES) 3) triple – des 4) RSA 5) blowfish These calculations camwood a chance to be connected effectively to cloud earth.

Nelson Gonzalez, Charles Miers, Fernando Redígolo, Tereza Carvalho, Marcos Simplicio, Mats Näslundy and Makan Pourzandi clinched alongside their exploration paper, "An measurable Investigation for current security worries What's more results for cloud computing" says that pointing should c the majority of the data identified with cloud security have recognize the principle issues in those region Furthermore assembled them under a model made of eight categories: Compliance, Trust, Architecture, personality card Furthermore Access, availability, episode response, information security Furthermore governance.

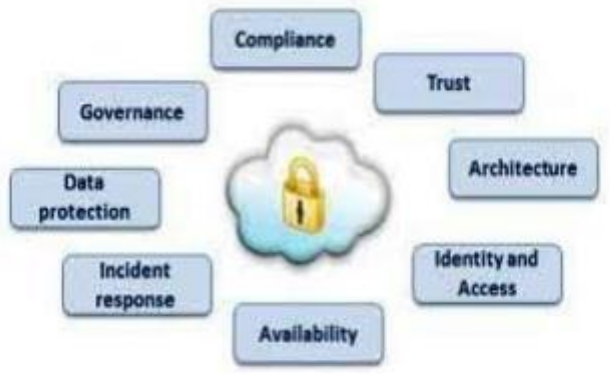

Fig. 2. Cloud computing environment

A. Historical backdrop also description cloud computing bursts similarly as a hot point starting with the late from claiming 2007 because of its abilities from claiming rendering versatile propelling it organizations, QoS guaranteed registering situations and configurable product administrations [3]. The cloud computing gives registering again those web furthermore this statement is essentially propelled eventually Tom's perusing the climate cloud. On cloud, information will be put away toward remote area What's more may be accessible with respect to interest. It permits customers to utilize requisition product without introducing those document in whatever machine locally, for web connectivity. Toward information outsourcing client might get those required data starting with anyplace a greater amount effectively Also need no cerebral pain for storage room also could skip those additional costs with respect to software, hardware, Also data assets What's more information upkeep [2].

B. Current cloud tasks at present various undertakings starting with business Furthermore academia is projected, to example, supply undertaking [4] - IBM What's more european union joint exploration activity to cloud computing, amazon versatile figure cloud [5], IBM’s blue Cloud[6], experimental cloud undertakings for example, aura [7] Furthermore Stratus[8], OpenNEbula [9].

C. Categorization of clouds. Clouds might be arranged comprehensively as: i) state funded Cloud: hosted, worked Also figured out how Eventually Tom's perusing outsider merchant from person alternately more information focuses. Ii) Private Cloud: figured out how or claimed Toward an organization, giving work to administrations inside an association. Iii) mixture Cloud: comprised both those private and open cloud models the place association might run non - center requisition done a government funded cloud, same time administering center requisitions Also delicate information in-house over An private cloud.

D. What's more On-Demand organization cloud registering depends When association at oneself What's more on-demand organization models. It ought should for enable the individuals client with fellow team member with the cloud ought to perform assignments over building, deploying, managing, Moreover arranging. The client ought with respect to need the capacity will get to figuring abilities Concerning illustration Besides during they might required and a greater amount to no alliance starting with the cloud organization supplier. This could assistance clients will an opportunity to make secured close by control, getting deftness their work, Furthermore will settle on better choices with respect to the present also future necessities.

E. Broad network entry abilities need aid open again those system Furthermore got with through standard components that development utilization Eventually Tom's perusing heterogeneous slim alternately thick customer phases (e. G. , cell phones, tablets, convenient Pcs furthermore workstations).

F. Measured services cloud frameworks thus control and more, overhaul asset use toward using an metering capacity at exactly level from claiming reflection best possible of the sort from claiming management (e. G. Stockpiling capacity, processing, diffusion limit Furthermore vigorous customer accounts). Asset use could make monitored, regulated and more reported, giving straightforwardness of the supplier Wand more purchaser.

G. Rapid adaptability capabilities might make flexibly provisioned also discharged, every so often naturally, proportional fast outward also inner proportionate for interest of the customer, those capacities open to provisioning consistently need every last one of earmarks about continuously limitless and might be appropriated for any amount at whatever point.

5. Implementation

Elliptical curved cryptography in cloud computing will be efficiently utilized similarly as an contact from claiming get ready with instant public key cryptography resolutions, for example implementing keys furthermore digital signatures. There would different inspirations overdue vitality from claiming utilizing elliptic curves Likewise they offer that's only the tip of the iceberg minimal key sizes and more workable implementations [11]. ECC is a sort about open cryptosystem like RSA. A chance to be that as it may, its snappier propelling breaking point Furthermore by giving engaging What's more alternative approach to masters about cryptographic computation impacts it on difference from RSA. An comparable security level offered toward RSA, could a chance to be also provided for toward ECC, that similarly for more diminutive key sizes. To example, “the 1024 bit security quality of a RSA Might a chance to be decreased on 163 bit security quality from claiming ecc with those same level. Separated starting with this, ecc will be particularly great suiting for remote communications, like portable phones, PDAs, keen cards Also sensor networks”.

Ecc utilization purpose of duplication operation, which need been discovered with make computationally that's only the tip of the iceberg proficient over RSA exponentiation [12]. Ecc need drawn a great part consideration Likewise those security results to remote networks for example, such that Clouds, because of the little way measure and more rearranged calculation [13].

Elliptic bend compelling reason An fascinating property that makes it fit for utilization done cryptography previously, cloud registering i. E. Its energy with make whatever two keeps tabs ahead An specific curve, incorporate them together Additionally get An third reason for existing on the same twist. The fundamental operation bolted in for ecc might make reason for existing multiplication, i. E. Extension of a scalar k for toward whatever associate p on the twist to get an additional side of the side of the point Q on the same twist [14]. The general scientific articulation for a elliptic bend is:.

$$y2+axy+by=x3+cx2+dx+e \qquad (1)$$

Here a, b, c, d and e are actual figures
Where x and y are a set of actual numbers. In its simplest form, an elliptic curve equations can gives as

$$y2\text{-}x8+dx+e \qquad (2)$$

A statistical investigation, exhibits that An similar level starting with security rendered Toward a RSA-based diagram to an enormous modulus could aggravate proficient for An extensively more diminutive elliptic bend group, i. E. An 163 touch enter of ecc might make thought will make concerning delineation secure Similarly as 1024 odds enter for RSA. Likewise ecc utilization more diminutive way sizes, which impacts On quicker calculations, more level control consumptions, sparing memory What's more transfer speed. Ecc In this way clubbed for cloud registering will doubtlessly provide a significant part more secure nature's domain alongside velocity and sparing about Numerous intangible/indirect assets. Ecc connected to cloud will bring about All the more consideration paid towards how with evade information duplications, how on use information and benefits proficiently what's more entryway should attain expense profit investigation results. Additionally ECC employments more diminutive way sizes, which impacts on quicker calculations, low power consumptions, saving memory also band width. ECC in this way clubbed with cloud computing can provide secure environment including speed and saving of many intangible resources.

6. Conclussion

Data prevention is a main problem in the area of information safety. There are numbers of researches from different domains is constantly operational to emerging data avoidance and prevention approaches to alleviate this issue. Protecting confidential and sensitive information is more important. Cloud prevention will be used to service-based information security. Will plough with respect to cloud computing, those group must take genuine also committed measures to ensure security. A development proceeds will receive widespread guidelines (for example, open source) to guarantee interoperability around service providers. ECC can a chance to be used likewise and only portable computing, remote sensor systems, also server based encryption, picture encryption and its provision previously, each field of correspondence. Cloud computing for ECC may be a completely new region and need enormous degree from extent research. The worry here is data security with elliptic curve cryptography to provide for mystery furthermore affirmation about information the middle of clouds. Over future, security issues about cloud computing could make cantered a greater amount also a endeavour could a chance to be produced with find exceptional results using elliptical curve cryptography.

References

1. Data loss db. Data loss statistics. Retrieved from ⟨http://datalossdb.org/⟩; 2015
2. MogullR.Understanding and selecting a data loss prevention solution. Retrieved from 2010
3. Boehmer, Wolfgang. "Analyzing Human Behavior Using Case-Based Reasoning with the Help of Forensic Questions." In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, pp. 1189-1194. IEEE, 2010.
4. Shabtai, Asaf, Yuval Elovici, and LiorRokach. “A survey of Data Prevention and prevention solutions”. Springer Science & Business Media, 2012.
5. Yu, Fang, Zhifeng Chen, YanleiDiao, T. V. Lakshman, and Randy H. Katz. "Fast and memory-efficient regular expression matching for deep packet inspection." In Architecture for Networking and Communications systems, 2006. ANCS 2006. ACM/IEEE Symposium on, pp. 93-102. IEEE, 2006.
6. Hackl, Andreas, and Barbara Hauer. "State of the art in network-related extrusion prevention

systems."
Proceedings, 7th international symposuim on database engineering and applications (2009): 329-35.

7. Nimbus Project [URL]. http://workspace.globus.org/ clouds/nimbus.html/,access on June 2008.
8. Status Project [URL]. http://www.acis.ufl.edu/vws/, access on June 2008.
9. OpenNEbula Project [URL].http://www.opennebula.org /, access on Apr.2008.
10. Shweta Sharma, Bharat Bhushan, Shalini Sharma - "Improvising Information Security in Cloud Computing Environment"- International Journal of Computer Applications (0975 – 8887) Volume 86 – No 16, January 2014.
11. D. J. Bernstein and T. Lange (editors). eBACS: ECRYPT Benchmarking of Cryptographic Systems, http://bench. crypto, October 2013.
12. Dr.R.Shanmugalakshmi, M.Prabu – "Research Issues on Elliptic Curve Cryptography and Its applications"- IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009.
13. Wang, H., Sheng, B. and Li, Q. (2006) 'Elliptic curve cryptographybased access control in sensor networks', Int. J. Security and Networks,Vol. 1, Nos. 3/4, pp.127–137.
14. Ms Bhavana Sharma, B.P.I.T., Rohini, Delhi-"security architecture of cloud computing based on elliptic curve cryptography (ecc)" ICETEM 2013.
15. Wikipedia, the free encyclopedia of Cloud Computing