An Enhanced Approach in Cloud Computing to reduce security risks and minimize data loss in railways

Article · January 2016

CITATIONS
0

READS
2,302

4 authors:

Ravi Gaurav
Dayananda Sagar Institutions
7 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Shubham Kumar
Indian Institute of Technology Kanpur
4 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Venkatesan Selvam
B.S Abdur Rahman Crescent Institute of Science & Technology
35 PUBLICATIONS **143** CITATIONS
SEE PROFILE

Ramesh Babu
Dayananda Sagar Institutions
72 PUBLICATIONS **379** CITATIONS
SEE PROFILE

International Journal of Electrical Sciences & Engineering (IJESE)
Print ISSN: _____; Online ISSN: _____; Volume 1, Issue 1; 2015 pp. 6-12

An Enhanced Approach in Cloud Computing to Reduce Security Risks and Minimize Data Loss in Railways

Ravi Gaurav[1], Shubham Kumar[2], S. Venkatesan[3], D.R. Ramesh Babu[4]

[1,2]Department of computer science & Enginnering, Dayanand Sagar College of Enginnering, Bangalore
[3,4]Professor, Department of Computer Science&Engineering, DayanandaSagar College of Engineering, Bangalore

***Abstract*: The distributed computing is another registering model which originates from framework processing, appropriated figuring parallel processing, virtualization innovation, utility figuring and other PC advances and has more point of interest characters, for example, huge scale calculation and information storage, virtualization, highexpansibility, high unwavering quality and low value service. Cloud processing has conveyed new changes and chances to IT industry. It is the consequence of the advancement of an assortment of techniques. And the railroad office will utilize the distributed computing innovation to accomplish the sharing of the rail route data assets furthermore, to enhance the limit of data handling. In any case, with the advancement of the distributed computing, it additionally confronted with numerous troubles, distributed computing security has turned into the main source of obstructing its improvement. Distributed computing security has turned into an intriguing issue in industry and scholarly research. This paper will investigate the status of the advancement of distributed computing security, break down the information privacy, security examining, information checking and different difficulties that the distributed computing security confronted with. We will depict the arrangements which the industry and the educated community proposed for some key issues of distributed computing security, for example, virtualization security and movement observing between virtual machines et cetera. Also, we broke down the security of distributed computing in railroad environment. We proposed a distributed computing security reference system. The motivation behind this paper is endeavored to bring more noteworthy clarity scene about distributed computing security.**

Keywords-cloud computing; cloud computing security; cloud security framework; data leakage; encryption;

1. INTRODUCTION

Since 2007, cloud computing has been able to be hot issue, various associations began to attempt to use appropriated processing organizations. The common dispersed registering organization are Amazon's EC2 and's Google App Engine, they use the Internet to unite with outside customers, and take the broad number of programming and IT establishment as an organization provided for customers. With the solace, economy, high versatility and diverse purposes of interest, appropriated registering enables the endeavor opportunity from the generous weight of the IT establishment organization and backing. Circulated registering change the Internet into another figuring stage, is an arrangement of activity that fulfill purchase on-interest and pay-per-use in framework, has a wide progression prospects. Railroad is the zones' one that proposed to offer need to make in national "Eleventh Five-Year Plan"; the change example of quick, overpowering and thick in rail line, makes an extensive variety of data including highlight and sound data in considerable scale growing, so it passes on enormous challenges to the information method of the railroad, including significant - scale appropriated figuring, data examination and taking care of, data sharing and the joining of enrolling resources and so forth; the conveyed registering as the improvement of distinctive progressions, has the key particular characteristics of dealing with the issues abovefl].

Yet, the change of disseminated processing is standing up to various separating issues, the most perceptible is the security issue, with the creating reputation of dispersed figuring, the importance of security show relentless upward example, transform into a basic segment in the headway of appropriated registering. 2009 Gartner diagram exhibited that more than 70% of respondents said they don't plan to use the circulated processing at later, the essential reason fears the data security and insurance. Moreover, the burst of different security events continue extending more people pushed over the cloud. Case in point, in March 2009, the event that a far reaching number of customer's archives were discharged happened in Google. Henceforth, remembering the final objective to affiliations and associations can make usage of tremendous scale cloud organizations, circulated processing advancement and stages, rest ensured that their data were migrated to the cloud, we must clarify the issues that dispersed registering security faced with. The inspiration driving this paper is tried to bring more paramount clarity scene about circulated figuring security.

2. II. THE CONCEPT OF CLOUD COMPUTING AND CHALLENGES

A. The concept of Cloud Computing

The thought of Cloud Computing Distributed registering is in being taken a shot at, there are no for the most part recognized bound together definition. In unmistakable periods of progression or from a substitute perspective has a substitute cognizance on the cloud. U. S. National Institute of Standards and Technology (NIST) portrays 5 key segments, 3 organization model and 4 course of action model of cloud[2], This definition is wide industry gathering.

B. Challenges

In 2008, the U. S. data innovation research and counselling firm gartner issued a “distributed computing security hazard appraisal” report, fundamentally from the seller perspective about security abilities investigated security dangers confronted by the cloud, posting seven noteworthy security chances that the distributed computing innovation exists [3], as appeared in table 1

TABLE 1: SEVEN TOP SECURITY RISKS GARTNER

RISK	Description
Privileged user access	Delicate information handled outside the undertaking carries with it an inborn level of danger
Regulatory compliance	Distributed computing suppliers who decline to outside reviews and security affirmations
Data location	When you utilize the cloud, you most likely won't know precisely where your information is facilitated
Data segregation	Information in the cloud is ordinarily in a common situation nearby information from different clients
Recovery Investigative support	Regardless of the fact that you don't know where your information is, a cloud supplier ought to let you know what will happen to your information and administration in the event of a catastrophe
Long-term viability	Researching unseemly or illicit movement may be incomprehensible in distributed computing. You must make certain your information will stay accessible even after such an occasion

- Data protection: As a client, we lose control over physical security, by what means would we be able to guarantee that information won't spillage and privacy can be protected
- Key administration: If the data is encoded, then who controls the encryption/unscrambling key? Client or Service supplier?
- Data Integrity: It is not exist that a typical standard to guarantee information hone.

3. SAFETY STATUS OF THE CLOUD.

A. The government concern about the safety of the cloud

November 2010, the U. S. government and agency CIO

CSA appropriated in 2009 "in key locales of the cloud Safety Guide" and moved up to frame 2. 1 [4], generally from the perspective of the aggressor packed the huge threats that conveyed figuring environment may be stood up to, proposed 12 key fields that security concerns, then issued a cloud reduced reports security perils, the Security Guide was concentrated to 7 of the most broadly perceived, the best hazard to pernicious levels, as showed in Table II.

TABLE 2: SEVEN TOP SECURITY RISKS CSA

Risk	Description
Abuse and Nefarious Use of Cloud Computing	By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity
Insecure Interfaces and APIs	It increases risk as organizations may be required to relinquish their credentials to third parties in order to enable their agency.
Malicious Insiders	A provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.
Shared Technology Issues	The underlying components that make up this infrastructure (e. g., CPU caches.) were not designed to offer strong isolation properties for a multi-tenant architecture.
Data Loss or Leakage	The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the

	cloud environment.
Account or Service Hijacking	Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.
Unknown Risk Profile	Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture.

Asked the government to assess the security risks about the cloud computing, described the challenges of cloud computing and the security for cloud computing.

September 2010, Westone held a conference about cloud security and cloud storage in Beijing, responded enthusiastically.

May 2010, in the second session of the China Cloud Computing Conference, the Ministry of Industry Vice Minister Lou said, we should strengthen the information security of cloud computing to solve common technical problems.

March 2010, the European Network and Information Security Agency (ENISA) announced they will promote the management department to request cloud service provider not conceal attacks on cloud.

B. The Cloud Security Standards Organization and Progress on Cloud

Many standards organizations have begun to develop standards of cloud computing and cloud security, in order to enhance interoperability and security, to promote the healthy development of cloud computing industry. Such as: Open Cloud Manifesto (OCM), National Institute of Standards and Technology (NIST), Cloud Security Alliance (CSA) and Distributed Management Task Force (DMFT).

- ***Open Cloud Manifesto (OCM)***

There are more than 300 units join in the organization currently, the main results of the organization is open cloud manifesto [6], the open cloud manifesto describes the challenges that cloud computing faced with, including governance and management, security, data and application interoperability and portability, measuring and monitoring.

Other challenges to be aware of: [5]

- ***National Institute of Standards and Technology (NIST)***

NIST fundamentally through specialized direction and elevate the institutionalization work to help government and industry sheltered and compelling utilize the distributed computing innovation. In the May 2010, the NIST held symposium about the distributed computing, in October 2009, issued a "sheltered and compelling utilization of distributed computing" scholastic discourse. The primary aftereffects of NIST are:

NIST meaning of distributed computing VI5 [7], the archive gives the meaning of distributed computing, and portrays five attributes of distributed computing, three administration models and four arrangement examples, and reference by numerous Standards Alliance, for example, DMTF.

Sheltered and productive utilization of distributed computing report [8], the report presents the idea of distributed computing, elements, outline, and nitty gritty examination of the distributed computing security, relocation and other related advances and the institutionalization about cloud security.

- ***Cloud Security Alliance (CSA)***

CSA is a non-advantage affiliation, establishment in the RSA Conference in 2009, rule focused on the security dangers that the endeavor went up against with when sending the conveyed registering structure and given the correct wellbeing urging. CSA suggestion a conveyed processing security basic arranging reference model [4], as showed in Figure

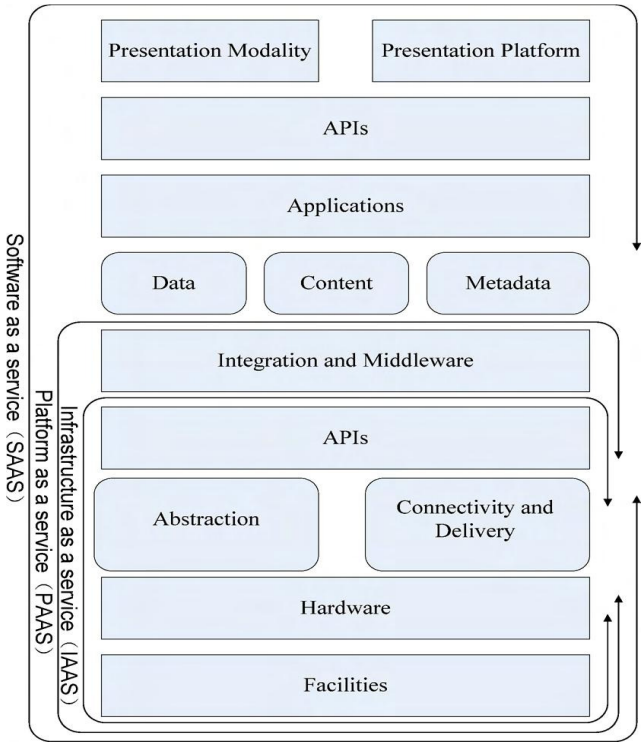


Fig. 1. CSA cloud computing security architecture reference model

CSA proposed 15 focus areas of cloud computing security from the point of cloud management and cloud computing run, as shown in Tablelll

TABLE 3. CSA 15 FOCUS AREAS OF CLOUD SECURITY

Cloud	Cloud computing run	
management		
Compliance and	Traditional Security	Disaster Recovery
Audit		
Governance and	Emergency	Notification and
Enterprise risk	Response	Repair
management		
Portability and	Business Continuity	Application Security
Interoperability		
Legal and	Encryption and Key	Virtual ization
Electronic	Management	
discovery		
Information	Data Center	Identity Access
Lifecycle	Security	Management
Management		

- ***Distributed Management Task Force (DMFT)***

The association worried about the distributed computing administration principles, concentrate on enhancing the interoperability about cloud administration between cloud administration suppliers and clients, and between cloud administration suppliers and cloud administration designers, built up the interoperability measures through improvement the assention of cloud assets administration, embodiment organization and security components. The primary aftereffects of DMTF [9] are: the Open Virtualization Format Specification (OVF), cloud administration construction modeling, cloud interoperability white paper.

4. STEPS TO PREVENT DATA LEAKAGE AND DETECTION

Data Leakage Detection: With the snappy advancement of database business on the net, the data may be hazardous in the wake of experiencing the unsecure framework. The data purchasers may dither to buy the data organization for the going with suspicion. In any case, the data recipient may suspect that the data are upset by unapproved person. Second, they may suspect the data got are not conveyed and gave by the endorsed suppliers. Third, the suppliers and purchasers truly with differing interest should have particular parts of rights in the database organization or using. So how to secure and affirm the data ends up being fundamental here. The late surge in the web's improvement results in offering of a broad assortment of electronic organizations, for instance, database as an organization, mechanized chronicles and libraries, e-exchange, online decision sincerely strong system et cetera. All through coordinating, here and there delicate information must be offered over to obviously trusted outsiders. For example, an expert's office may give patient records to specialists who will devise new arrangements. We call the information's proprietor the shipper and the to the degree anyone knows trusted outsiders the professionals. We will apparently perceive when the merchant's delicate information have been spilled by experts, and if conceivable to see the directors that released the information.

We consider applications where the first fragile data can't be irritated. Inconvenience is a particularly important system where the data are balanced and made "less tricky" before being given to masters. For example, one can add unpredictable clatter to particular properties, or one can supplant exact qualities by scopes [13]. On the other hand, on occasion, it is essential not to adjust the first shipper's information. For example, if an outsourcer is doing our cash, he must have the accurate compensation and client record numbers. On the off chance that supportive specialists will be treating patients (instead of fundamentally planning estimations), they may require definite information for the patients. For the most part, spillage watermarking in order to recognize evidence is managed, e.g., a novel code is embedded in each appropriated copy. If that copy is later found in the hands of an unapproved assembling, the leaker can be recognized.

Watermarks can be especially profitable from time to time, however again, incorporate some adjustment of the first data. In addition, watermarks can now and again be crushed if the data recipient is vindictive. In this paper, segment I gives the examination of systems to perceiving spillage of a game plan of things or records. In the wake of giving a course of action of things to experts, the wholesaler discovers some of those same articles in an unapproved spot. (For example, the data may be found on a site, or may be overcome a true blue revelation process.) At this point, the dealer can overview the likelihood that the spilled data began from one or more administrators, as opposed to having been self-rulingly aggregated by distinctive means. In case the dealer sees "enough verification" that an experts spilled data, he may stop working with him, or may begin honest to goodness strategies. In area II a blameworthy operators is present which is create for evaluating the "blame" of specialists furthermore display calculations for disseminating articles to operators, Sections III and IV, introduce a model for computing "blame" probabilities in instances of information spillage. At long last, in Section V, assessing the methodologies in distinctive information spillage situations, and check whether they without a doubt distinguish a leaker.

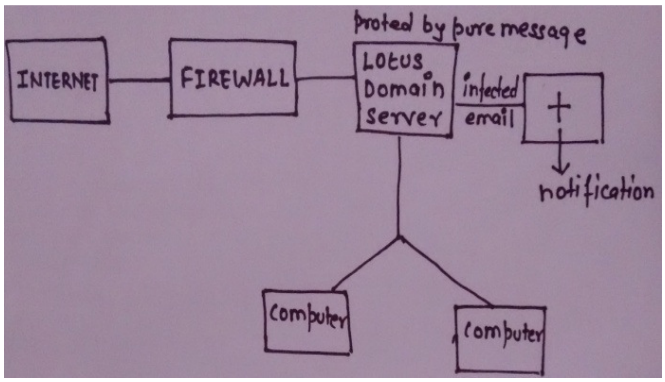
I HOW IS ACCESS TO THE DATA GAINED?

"Who brought on the gap?" quality. These qualities are not tradable, yet rather comparing and the diverse ways to deal with acquire access to sensitive data can be bundled into the going with social affairs. Physical spillage channel suggests that physical media (e.g., HDD, convenient PCs, workstations, CD/DVD, USB devices) containing unstable information or the record itself was moved outside the affiliation. This more every now and again infers that the control over data was lost even before it leaved the affiliations.

Difficulties are **an) Encryption**: and averting information spills in travel are hampered because of encryption and the high volume of electronic interchanges. While encryption gives intends to guarantee the privacy, credibility and uprightness of the information, it likewise makes it hard to recognize the information holes happening over encoded channels. Encoded messages and document exchange conventions, for example, SFTP suggest that correlative DLP mechanisms should be employed for greater coverage of leak channels. Employing data leak prevention at the endpoint – outside the encrypted channel can possibly identify the breaks before the correspondence is scrambled. **b) Access Control**: It gives the first line of guard in DLP. On the other hand, it doesn't have the best possible level of granularity and may be obsolete. While access control is suitable for information very still, it is hard to execute for information in travel and being used is not included in. **C) Semantic Gap in DLP**: DLP is a multifaceted issue. The meaning of an information hole is liable to differ between associations relying upon the delicate information to be ensured, the level of cooperation between the clients and the accessible correspondence channels. The present cutting edge principally concentrates on the utilization of abuse identification (marks) and after death examination (criminology). The regular deficiency of such methodologies is that they do not have the semantics of the occasions being observed. At the point when an information hole is characterized by the conveying gatherings and the information traded amid the correspondence, a straightforward example coordinating or get to control plan can't induce the way of the correspondence. Hence, information spill counteractive action components need to stay informed concerning who, what and where to have the capacity to guard against complex information spill situations. The characterization by spillage station isimportant with a specific end goal to know how the occurrences may be averted later on and can be named physical or logical. enerally, spillage disclosure is dealt with by watermarking, e. g. , a noteworthy code is introduced in each flowed copy. If that copy is later found in the hands of an unapproved assembling, the leaker can be recognized. Watermarks can be to a great degree accommodating once in a while, yet again, incorporate some change of the first data. Plus, watermarks can as a less than dependable rule be devastated if the data recipient is malicious. E. g. A facility may give patient records to researchers who will devise new medications

II Guilty Agent

To perceive when the wholesaler's tricky data has been spilled by administrators, and if possible to recognize the authorities that discharged the data. Disturbance is an amazingly important methodology where the data is changed and made "less fragile" before being given to administrators. An unassuming system is made for distinguishing spillage of a game plan of articles or records. Accept that in the wake of offering articles to pros, the shipper finds that a set S _ T has spilled. This infers some untouchable, called the goal, has been gotten having S. For example, this target may be demonstrating S on its site, or perhaps as a noteworthy part of a genuine disclosure change, the goal turned over S to the wholesaler. Since the administrators U1; Un have a data's rate, it is sensible to suspect them discharging the data. Then again, the administrators can battle that they are guiltless, and that the S data were gotten by the target through diverse means. Case in point, say that one of the things in S identifies with a customer X. Possibly X is moreover a customer of some other association, and that association gave the data to the target. Then again perhaps X can be repeated from distinctive straightforwardly available sources on the web. We will probably gage the likelihood that the spilled data started from the masters rather than diverse sources. Intuitively, the more data in S, the harder it is for the experts to battle they didn't discharge anything. So additionally, the "rarer" the things, the harder it is to battle that the target procured them through diverse means. Not simply would we need to gage the likelihood the administrators spilled data, on the other hand we may moreover get a kick out of the chance to see whether one of them, particularly, was more disposed to be the leaker. For instance, if one of the S things was simply given to administrators U1, while substitute articles were given to all experts, we may suspect U1 more. The model we show next gets this sense. We say an administrators Ui is at risk and if it contributes one or more dissents the goal. We mean the event that administrators Ui is accountable by Gi and the event that masters Ui is subject for a given discharged set S by Gi/jS.

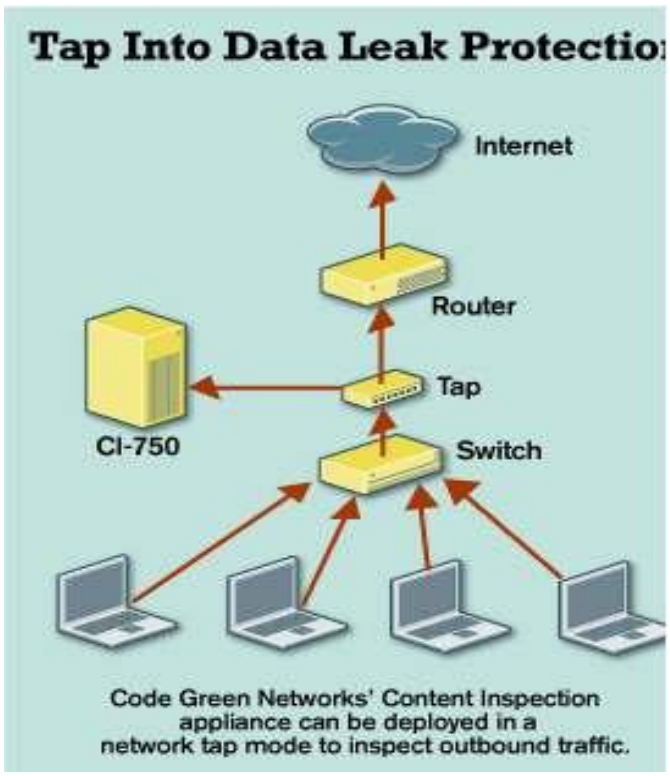


DATA LEAKAGE PREVENTION: Data spill revultion (DLP) is a course of action of information security gadgets that is proposed to keep customers from sending delicate or fundamental information outside of the corporate framework. Appointment of DLP, contrastingly called DATA mishap evasion, information incident expectation or removal neutralizing activity, is being driven by essential insider threats and by more exhaustive state security laws, a critical number of which have stringent data confirmation or access fragments. DLP things use business rules to take a gander at record substance and label private and separating information with the goal that customers can't reveal it. Marking is the technique of requesting which data on a system is private and checking it suitably. A customer who adventitiously or malevolently attempts to uncover mystery information that has been named will be denied. Case in point, marking may even keep a sensitive budgetary spreadsheet from being informed by one delegate to another within the same organization. DLP things generally have the going with fragments: Endpoint: Monitor and control activities Network: Filter data streams Storage: Protect data still. Actualizing an undertaking DLP item can be entangled.

Most expansive associations have several servers with a huge number of catalogs and records put away on them and particular sorts of information that should be labeled. The product can be helpful for recognizing very much characterized substance (like Social Security or Mastercards numbers) yet tends to miss the mark when a chairman is attempting to distinguish other delicate information, similar to protected innovation that may incorporate realistic parts, recipes or schematics. To actualize undertaking DLP effectively, work force from all levels of administration should be effectively included in making the business rules for labels. . Information spill aversion (DLP) is a suite of advances went for stemming the loss of touchy data that happens in endeavors over the globe. By concentrating on the area, grouping and observing of data very still, being used and in movement, this arrangement can go far in helping an undertaking understand what data it has, and in ceasing the various breaks of data that happen every day. DLP is not a fitting and-play arrangement. The fruitful usage of this innovation requires critical readiness and industrious progressing upkeep. Ventures trying to coordinate and actualize DLP ought to be arranged for a huge exertion that, if done accurately, can extraordinarily lessen danger to the association. Those executing the arrangement must take a key approach that addresses dangers, effects and alleviation ventures, alongside fitting administration and affirmation measures. New little and fair size endeavors can assimilate both the monetary and PR harm dispensed by genuine breaks focusing on delicate information. But, they're frequently under ensured in light of the fact that information spill counteractive action, or DLP, items are, generally speaking, essentially excessively costly. In the interim, there's been a critical rise in cybercrime following a consistent five-year decrease, as indicated by the 2007 CSI Computer Crime and Security Survey. Insider misuse of system resources is the most common assault, ahead even of infections, with normal misfortunes of around $350, 000. Code Green Networks, which was dispatched by the originators of Sonic Wall, means to handle this issue. Code Green's most up to date offering, the CI-750 Content Inspection Appliance, is designed particularly for systems with 250 or less clients and offers the same components and usefulness as its higher-finished items, beginning at $10, 000. The CI-750 uses "fingerprints" to distinguish both organized information, for example, Social Security or charge card numbers, and unstructured information, for example, records, documents, source code, etc. Where numerous DLP items for littler organizations depend on sifting for certain document sorts or give just essential pivotal word or example matching, Code Green's technology creates hash values of the actual data to be protected and scans outgoing traffic for matches. We found Code Green's fingerprinting technology accurate, and a built-in mail transfer agent. However, without the help of third-party proxies, the appliance is blind to encrypted data, and it can't stop movement of internetwork and web-based traffic. This means the appliance represents only part of a robust.

DLP system. FINGERPRINT TRAIL: The CI-750 can be deployed in a variety of ways. Included a kit it was a network tap device, which let us passively monitor traffic flowing through our WAN connection, and a mail transfer agent. Customers can route outgoing messages from their mail servers through the mail transfer agent for additional mail-filtering abilities; questionable e-mail can be held until approved by an administrator. Admin also can create policies to encrypt e-mail carrying sensitive information. This functionality is provided via Code Green's partnership with the Voltage Security Network, which offers e-mail encryption as a service. After connecting the device to network, A selected sources of data that the appliance should protect. It has built-in functionality to fingerprint both structured and unstructured data such as that in CIFS. Setup for CIFS was simply a matter of providing the server and share name, along with appropriate access credentials. The device then scans the share at user-defined intervals. CIFS scanning was trouble-free and didn't cause performance issues on our Windows file server.

Be that as it may, it's officeholder on IT to guarantee that substance to be fingerprinted gets put into the fitting CIFS offer. This can be tricky. For instance, our organization depends vigorously on private wiki pages and not shared volumes for the majority of our interior data. Code Green's proposed workaround is to have a script that dumps the substance of our wikis to a CIFS offer all the time. Given the uptick in communitarian workspaces, for example, wikis in the business group, we'd like to see a completely computerized approach to get such information fingerprinted.



It in like manner would look good if the contraption could use Web pages as sources clearly; support for other data stores furthermore would grow the compartment's out convenience of this machine and discard the prerequisite for extra scripting. It should be noted, then again, that various battling offerings, some essentially more excessive, don't even offer database joining. Resulting to selecting data hotspots for fingerprinting, IT then describes development to screen and what moves should be made in the event a break is recognized. We organized some comprehensively scrutinized chooses and found that the CI-750 made a wonderful demonstrating alerted us to data discharges happening within email, Web, IM, and even stuffed report transmissions. We fused a two-sentence part from an assention in an email to a client. Following a moment, we had an email communicating that there had been an encroachment. The official interface on the machine exhibited that an email had been sent to our customer and had the full association of the email to show the encroachment. The interface can similarly appear past encroachment that may have been joined. Partial PREVENTION: While we were awed with the fingerprinting's exactness, the contraption did not have the limit truly seclude the message in light of the way that it was sent by method for Web mail. Associations that need healthy frustrating of Web and framework movement should place assets into a mediator device. The Code Green machine can be outlined as an Internet Content Adaptation Protocol server when joined with an ICAP delegate, for instance, those from Blue Coat Systems or Squid. Exactly when so joined, Code Green can square HTTP, HTTPS, and FTP action. It in like manner can unscramble development for examination. Versatile workstations similarly will speak to an issue for Code Green customers. The association offers an endpoint experts that controls the usage of removable media, for instance, glimmer drives and CDs.

5. CONCLUSION

From the investigation of the information spillage, we can identify and keep the information from the break by utilizing a few calculations and methods and can apply in Indian railroads. Ideally there would be no compelling reason to hand over touchy information to specialists that may accidentally or perniciously spill it. Furthermore, regardless of the possibility that we needed to hand over delicate information, ideally we could watermark every article so we could follow its starting points with supreme sureness.

REFERENCES

[1] LIU Zhen, LIU Feng, ZHANC Baopeng, MA Fei, CA 0 Shiyu. Research on Cloud Computing and Its Application in Railway [J]. Journal of Beijing Jiaotong University, 2010, 34(5): 14-19. (inChinese)

[2] MELL P, GRANCE T. The NIST Definition of Cloud Computmg [EB/OL]. [2010-05-10]. http://csrc. nist. gov/groups/SNS/cloud-computing/.

[3] MATHER T, KUMARASWAMY S, LATIF S. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance [M]. [s. l.]: O'ReillyMedia, Inc., 2009.

[4] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing V2. 1. 2009.

[5] http://www. infosectoday. com/Articles/Cloud_Security_Challenges. htm

[6] http://www. opencloudmanifesto. org/

[7] National Institute of Standards and Technology. NIST definition ofcloud computing VI5. 2010

[8] National Institute of Standards and Technology. Safeand efficient useof cloud computing report. 20094362

[9] http://www. dmtf. org/

[10] L. Sweeney, "Achieving K-Anonymity Privacy Protection UsingGeneralization and Suppression," http://en. scientificcommons. org/43196131 2002.

[11] Ravi Gaurav Shubham Kumar et. al, Cloud Security in Southern Railways in India National Conference on Information and Technology organised by Dayananda Sagar College of Engineering 2015. PP 42-47