A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats

R.Barona
Assistant Professor
Computer Science and Engineering
Narayanaguru College of Engineering
Manjalumoodu,India
rbaronajose@gmail.com

E.A.Mary Anita
Professor
Computer Science and Engineering
S.A.Engineering College
Chennai, India
drmaryanita@saec.ac.in

Abstract— Cloud computing is an innovation methodology for giving pay per utilize access to a gathering of shared resources for specific systems, stockpiling, servers, administration and applications, without physically getting them. So it spares overseeing expense and time for organizations. Numerous businesses, for example, keeping money, social insurance and instruction are moving towards the cloud because of the productivity of administrations gave by the compensation per-use design in view of the assets, for example, preparing influence utilized, exchanges completed, storage capacity devoured, information exchanged, or storage room possessed and so on. Cloud computing is a totally web based innovation where customer information is put away and kept in the server farm of a cloud supplier like Google, Amazon, Salesforce.com and Microsoft and so on. Constrained control over the information may acquire different security issues and threats which incorporate data breach, unreliable connectivity, sharing of resources, data accessibility and inside attacks. A breach of security may lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. There are different research challenges likewise there for embracing data breaches on cloud computing. This paper examines about cloud computing, different cloud models and primary security threats and data breach issues that are right now exploring in the cloud computing framework. This paper investigates the noteworthy research and difficulties that presents data breach in cloud computing and provides best practices to service providers and additionally endeavors plan to influence cloud servers to enhance their main concern in this serious economic scenario.

Keywords— cloud computing, data breach, security services, service providers

I. INTRODUCTION

Cloud Computing is a growing field in the area of computing. It is a way to maximize the utilization and computing capabilities without spending a lot to buy a new infrastructure. Cloud computing services are having various features such as liability, versatility, dependability, adaptability, profitability and element property. The resources in the cloud can be scaled in any direction, by the prerequisites of the client, to build the assignment execution. Cloud computing is a distributed network computing technology [13].It conveys infrastructure, programming and application as administrations to the client through the internet. These amenities are delivered by using virtualization technique of the data center. Data center is a pool of servers which accommodate all the applications of the clients of cloud. The clients and undertakings can utilize these server farms to store and process their information in outsider, by the utilization of cloud computing. Cloud computing relies on sharing of resources to achieve lucidity and economy of scale. Users can get faster access to their data on cloud due to this immense storage mechanism. The service availability issues are monitored by the service provider. As per NIST Cloud computing is characterized as "an approach to empower suitable, on-request network access to a mutual group of computing resources that can be promptly provisioned and released with least administration effort"[19].One of the examples for such a noble innovative technology is the popular social networking site called Face book. Users need only an internet connection to access the site through their login credentials. Users can use Face book to share photos, images and multimedia contents. All these data can be accessed by the users anytime anywhere if they are having internet connection because information is put away in remote computer framework rather than neighborhood computer framework using cloud computing.

Types and service models of cloud computing

Cloud computing exists when several computers are accessing the services from the internet. The cloud computing systems are fault tolerant. Hence they provide dependable services to the client. Cloud computing offers different services to the users such as hardware, software, information get to and capacity. The clients can get to these services from the cloud

978-1- 5090-4967- 7/17/$31.00 © 2017 IEEE

without having any data about the physical area and arrangement of the framework which offers the services. In view of the utilization necessity of the clients, Cloud is categorized into three models.

Private Cloud: The cloud infrastructure is developed for the own purpose of the organization. The specific group of workers can access this cloud. Public users cannot access this cloud.

Public Cloud: The cloud can be used by the general public. Any user at anytime from anywhere can access the services from public cloud. The users are charged based on the utilization level of the cloud services.

Hybrid Cloud: The mix of private and public cloud is called hybrid cloud. This is built up when the private cloud needs a few amenities from the public cloud.

Cloud computing environment offers three types of service models. Users can select any one of these three services based on their need. The users can use these services based on pay for use model. The users are charged based on their usage volume. The three Service Models offered by cloud computing are:

Software as a Service (SaaS)*:* The different applications running on a cloud can be approached to by the client through a web program. Face book, Whatsapp, Gmail etc. are such services.

Platform as a Service (PaaS): The level above SaaS is PaaS. The client is permitted to get to the operating framework to deploy the developed applications on the cloud. The required resources can be provided to the users through this model. It is not essential for the user to install and maintain the required software in his/local system. So the cost required for developing the application through cloud computing environment is very less. Example: Google App Engine.

Infrastructure as a Service (IaaS): The required infrastructure can be given to the clients through this model. A portion of the infrastructure assets are hard ware equipment, storage and bandwidth. For example if a user wants to have five computer systems with some specific configurations to develop an application, he/she can access or use those computers through this service model from the cloud service provider without spending a lot to buy new computers. Example: Amazon EC2 cloud.

II. Related Work

Security is a primary concern when it comes to adoption of cloud computing as a primary source for data storage. In recent years, work has been dedicated to develop security framework and mechanisms to protect user data. Ida Madieha et al layout the issues and difficulties from the purposes of legitimate structure that Malaysia ought to expect and address in keeping up and maintaining its national critical information infrastructure(CII). They likewise have first take a gander at the issue of information breach on the planet and analyze how as the innovation turns out to be more predominant, the digital world turns out to be more defenseless against information breaks. Attached to that is the thought of critical information infrastructure [12]. The potential cost of data misfortune to organizations and society is expanding yearly. Along these lines, there is a requirement for a monetary model to compute the costs identified with data breach occurrences with solid prescient abilities. Abdullah M. Algarni et al analyze the present condition of existing methodologies, which frequently differ as far as strategies and results. There is a need to accommodate all the profitable methodologies and expand on them. This would permit us to make a more total single approach that could dependably survey the different data breach cost segments [1]. Chandramohan.D et al focus on privacy preserving technique. They have perceived the week benefit holding of cloud suppliers in fulfilling, and guarding clients' mystery and failed to have an all inclusive service level understanding. To encounter the privacy issue, the authors have proposed a privacy preserving algorithm [5]. Nina Pearl Doe and Suganya V ensure the corrective measures to protect the integrity of data as well as detecting and preventing possible risks thus ensuring data breaching is prevented. The system, however, concentrates on mainly data breaches but there are more threats that cloud security faces [17]. Mark L. Huson and Barbara Hewitt examine the effectiveness of regulation within several industries to determine whether increased regulation would result in a reduction in information compromises [15] .David Kolevski and Katina Michael reviewed cloud computing data breaches using a socio-technical approach. The three major dimensions in the socio technical theory are- the social, the technical, and the environmental. The 7 key themes identified are: security, availability of data, privacy issues, trust, data flow, service level agreements, and regulation. [7]. Aryan TaheriMonfared and Martin GiljeJaatun review existing security monitoring mechanisms compared with new challenges which are caused by this new model. They highlight possible weaknesses in existing monitoring mechanisms, and propose approaches to mitigate them [4]. A general analysis framework was proposed by Yoga chandran et al to compute risk related with data breaches by using pre-agreed Sec SLAs for various cloud providers. The framework contains a tree based structure to find potential attack which leads to data breaches in the cloud and a way to evaluate the use of possible mitigation approaches to reduce them. [24]. There have been initial attempts to model the security of cloud in terms of securing stakeholder’s computational space. Some recent attempts formally model the CBS (Cloud based systems) as modularized actor models, using rewriting &equation logic based modeling languages. Building on these works has presented a framework for building executable models of CBSs for security analyses and illustrate its validity showing how the recent security breaches and security solutions can be modeled and analyzed using this framework [22].

Although security is analyzed from different perspective, more attention is given for enhancing security and actual data breach issues are not considered. Our focus is to dig deep into the security issues of data breaches and their significances in data security.

III. SECURITY ASPECTS

Security is the major factor to be concentrated while adapting to the cloud. The users will maintain lot of personal and secured data in their personal computers. When they are using the cloud computing technology these data will be transferred from their computer to the cloud. Hence the cloud should have efficient security mechanisms to secure these data. The security issues in the cloud are - confidentiality, integrity, availability, and privacy. The security issues are as follows:

Confidentiality Preventing the secured information from unauthorized access is known as confidentiality. The users will always fear about confidentiality aspect while their information is transferring to the cloud. In cloud confidentiality is connected with the areas such as intellectual property rights, covert channels, traffic flow analysis over the network, encryption techniques used to store the information and inference mechanisms.

Integrity Preserving the consistency and the correctness of the data is known as integrity. The cloud provider should ensure that unauthorized modifications are not made on the stored data.

Availability It ensures that the systems are functioning properly when needed. The users can able to use the cloud resources and systems when needed is termed as availability. DDoS attack is an example of a threat against availability in which they target the availability of networks, services and applications.

Privacy issues Since all the data from cloud users are stored in cloud data centers some issues may arise in the regard of privacy. Some privacy issues are loss of control, invalid storage, access control and data boundary [13].

To overcome the cloud security issues efficient security algorithms should be used by the cloud. Research should be carried out to make the cloud more secure. The relationship between data security concerns and the causes of data breach is shown in figure1.

A. Security threats and challenges

Cloud computing is having advantages such as easy implementation, accessibility, scalability, reliability, fault tolerance, shared resources, increased storage capacity and cost saving technology. Although Cloud computing has many advantages it comes up with lots of security issues and breaches faced by both cloud service providers and users [3].

According to the Cloud Security Alliance paper, "data breaches, information misfortune, record or administration activity commandeering, shaky interfaces and Application Programming Interfaces (APIs), DoS attacks, malignant insiders, mishandle of cloud administrations, inadequate due tirelessness, lastly shared innovation vulnerabilities", are identified as nine top most threats to cloud computing [14].

Data Breach A data breach is an activity which involves the unauthorized viewing, access or retrieval of data by an individual, application or service. It is a type of security breach designed to steal and/or publish sensitive data to an unsecured or illegal location. A data breach is also known as a data spill or data leak. Data leakage has become one of the greatest organizational risks from security standpoint [8]. The reasons, including: Data corruption, Data being purposely or accidentally deleted or modified by a user or an attacker, Data stolen over the network by network penetration or any network intrusion attack, Data storage device physically damaged or stolen, Virus infection deleting one or more files[11].

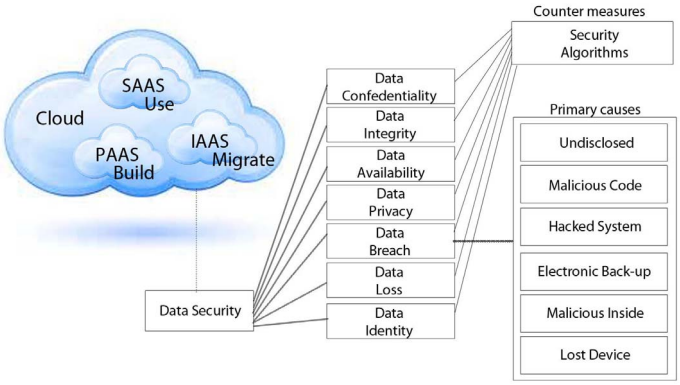

Figure 1. Primary causes of Data breach

Account or Service Traffic Hijacking Cloud account hacking is a procedure in which an individual or association's cloud record is stolen or captured by an assailant. Assault strategies, for example, phishing, extortion, and abuse of programming vulnerabilities [6] are utilized by the aggressor to seize a record. By cloud account hijacking the attacker uses the stolen account information for unauthorized access to the user account. An attacker uses a compromised email account or other credentials to impersonate the account owner.

Insecure Interfaces and Application Programming Interfaces (APIs) Service provider demonstrates all the APIs that are utilized by the customer to connect with the cloud. Information course of action, personality administration, service checking, all happen on the cloud. Validation and get to control is inspected by these interfaces [13].

Denial of Service (DOS) In DOS attack, an attacker accomplishes spoofing and sends extensive number of solicitations to the server. So the server gets occupied and not ready to offer service to the valid user requests.

Malicious Insiders The employees who are working inside the company will do some malicious functions such as misuse the user or client information. This occurs inside of an enterprise and clients are uninformed of it.

Abuse of Cloud Services This threat arises due to relatively weak registration systems existing in the cloud computing environment. In cloud computing enrollment process, anybody having a legitimate charge card can enlist and utilize the services. This encourages obscurity, because of which spammer, vindictive code creators and culprits can assault the framework [9].

Deficient Due Diligence An absence of due ingenuity is one of the top progressing dangers to cloud computing. While organizations may have a readiness of the general way of cloud innovation and related security threats, numerous organizations attempt minimal due perseverance about their cloud specialist organizations (CSPs). Indeed, even essential due steadiness, for example, assessing the money related soundness of the CSP or deciding the timeframe the CSP has been doing business, are frequently not cons diligence about their cloud service providers (CSPs). Even basic due diligence, such as evaluating the financial health of the CSP or determining the length of time the CSP has been in business, are often not considered[10].

Shared Technology Vulnerabilities Ingredients of working underneath the cloud which make condition for registering does not bolster solid partition for multi execution mode [13].

Among these threats, data breach is the most significant threat in the cloud computing technology. Data breaches to cloud services are increasing every year due to hackers who are trying to abuse the security vulnerabilities of the cloud [16].

A data breach occurs when an unauthorized hacker or attacker accesses a secure database or repository of the user in the cloud. This security destruction may cause serious damage to the users' data stored on the cloud.

Data breaches can be occurred on logical or digital data over the internet or a network connection. A data breach may result in data loss, including the sensitive information stored on the cloud. A hacker may use the stolen data to imitate himself as the original user to gain access to a more secure location. For example, a hacker's data breach of login credentials of a net banking user can result in access of his entire account information.

IV DATA BREACH

Data breach is the key security issue in cloud computing environment. The sensitive data of user or organization are stolen and they are become victims of financial fraud and identity theft. There are different sorts of data breaches, for example, [1][23] representative manhandle, Human oversights, System bugs, Malicious assaults, Intrusions with no robbery of information and Intrusions with burglary of information. Threats can have a variety of root causes, including environmental conditions, such as: storms or floods, human error, malicious attacks, hardware or software failures, and third party failures. Security violations are usually defined when there has been a demonstrated compromise of a security policy and are often associated with threats of a malicious nature. A data breach takes place when there is an impact related to the data such as the data being lost or illegitimately accessed, and effects have repercussions not only on the system security but also on the protection of personal data of the individual affected. Figure 2 shows the relationship between security threats, security violation and data breaches.

Employee Misuse It is an insider attack of a cloud. The employees who are working in the cloud environment may involve in data breach activity. These employees may have some access rights over the sensitive data stored on the cloud. They may misuse those rights and cause loss or damage to the data.

Human Errors Human error is the main cause for security breaches. Human error occurs since the cloud user fail to follow the instructions and guidelines and general carelessness. Such kind of data breaches is called accidental data breaches. The errors include: wrong delivery of sensitive information to the unauthorized person by email or sms, innocently publishing personal information on social networks, losing paper records containing sensitive data, losing laptop, mobile phone or storage devices (external hard disk, pen drive etc.) which are not protected with login credentials and improper closing of websites after using it.

System Glitches The breach due to system problems or failures is called system glitches. System glitches can cause the stored data to be corrupted or destroyed. Authentication failures and data recovery failures are also due to system glitches. The user cannot get access to his resources stored on the cloud due to the failure of systems. System glitches are mainly technological, but they can have contributing causes such as gaps in funding as well as in rules and procedures [23].

Malicious Attacks The hackers can attack the system by sending malware or virus to the targeted system. If the targeted system is affected by the malware then the hacker can easily penetrate into the system and retrieve all the stored sensitive information such as login credentials, personal information about the user, medical records, financial information etc. This will cause severe damage to the data. Some of the examples for malicious attacks are as following: [23]

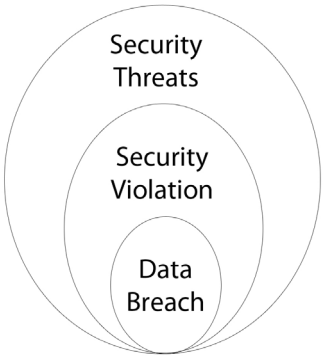

Figure 2. Relationship between Security threats, violation and data breach

Attacks include web applications through exploitable weaknesses in coding or theft of user identifications, phishing and other social engineering attacks. Sending out legitimate-looking emails to the users, make them ready to freely deliver fiscal or other private gen, damaging or installing malicious software that misdirects innocent users to fake websites, where they are encouraged to deliver sensitive information that can be abused, Distributed Denial of Service (DDoS) attacks intended to block the availability of networks and systems.

Intrusions with no theft of data The intruder can get access to the system and view the data. No damage or modification can be done. The data cannot be stolen by the intruder. It is difficult to identify such kind of intrusion attacks.

Intrusions with theft of data The intruder can get access to the system and causes serious damage to the system by performing activities such as modification, deletion and publishing the content over unauthorized places. The data can be stolen by the hacker. It is easy to identify such kind of intrusion attacks.

Online cyber theft The services offered by the cloud are most popular because of powerful processing ability and huge amount of storage space to the users. With their low-cost, enterprises could migrate their business into clouds so that they do not have the necessity to buy their private servers to store customers' information and handle traffic from customers. The issue here is, the online cyber thieves could use stolen passwords to access users' accounts, as well as, to launch malicious attacks to users. The login credentials of the users stolen from other websites were used to sign in to users' accounts.

Economic Costs of Data Breaches The cybercrimes that happen, taking after data breaches, and the effect of these violations on the economy as far as harm and cost can be huge. Much of the time, the harms to individual associations have been assessed in a huge number of dollars. A few expenses are not effectively quantifiable, for example, affect on fragments of the economy or national security [1].

Databases of Data Breaches There are several databases that provide information about security data breaches and help researchers analyze and contribute their results to reduce the impacts that result from data breaches [1]. The main databases include Privacy Rights Clearinghouse (PRC) [2], DATALOSS db [18], the Veris Community Database (VCDB) [21], and Web Hacking Incident Database (WHID) [20]. While the information in these databases was not directly applicable to this phase of the study, they can be valuable for validation of results once a computational model, based on the observations here, has been constructed [1].

V SECURITY APPROACHES

In this section, we examine some novel security approaches which are used in cloud computing organizations against data breaches.The primary issue is that with the presentation of the cloud; the cloud supplier has certain control over the cloud clients' information.

Information-centric security: For the ventures to oversee data in the cloud, it might be valuable to adopt a strategy of shielding information from within. This approach is called data driven security. This self-insurance procedure involves knowledge to be placed in the information itself. Data needs to act naturally portraying and ensuring, by the by of its environment. When got to, information checks its arrangement and tries to recreate a protected situation that is confirmed as dependable utilizing the structure of Trusted Computing (TC).

High-assurance remote server attestation: At present, absence of transparency is keeping organizations from moving their information to the cloud. Information proprietors wish to look at how their information is being controlled at the cloud, and to affirm that their information is not being abused or spilled, or possibly have an unalterable review trail when it does happen. Currently, cloud suppliers are utilizing manual evaluating methods like SAS-70 to fulfill their customers. A way to deal with address this issue depends on trusted computing. In a put stock in processing condition, a trusted screen is introduced at the cloud server to screen the activities of the cloud server. The trusted screen gives a proof of consistence to the proprietor of the information, ensuring that specific get to approaches have not been violated. To guarantee honesty of the screen, secure bootstrapping of this screen keep running next to the working framework and applications.

Privacy-enhanced business intelligence: A different approach to control data requires the encryption of all cloud data. The problem with this approach is that encryption restricts data use. Cryptographers have designed adaptable encryption proposals that take into account operations on the encrypted text. The cryptographic primitives, for example, homomorphic encryption (Gentry, 2009) and private data recovery (PIR) (Chor et al., 1998) perform calculations on cipher text without decrypting it. At the point when these cryptographic methods develop, they may open up new conceivable outcomes and directions for research for the development of cloud security algorithms.

Privacy and data protection: Privacy is a main issue in cloud computing environment. It includes the need to protect identity information, policy components and transaction histories. By migrating workloads to a cloud infrastructure, sensitive information of the customer faces the risk of unauthorized access and exposure. All cloud security solutions must be embedded with privacy-protection mechanisms**.**

Homomorphic encryption: This encryption scheme provides a mechanism to perform some specific type of computation on cipher-text which is not possible with any other encryption schemes. With this technique, data can be stored in the cloud as cipher-text format by the user. They can perform any necessary computation without the need to decrypt the cipher-text.

Searchable/ structured encryption: encryption is the base for this technique. It assures that the cloud does not know about the data and the computation which is performed on the data.
Proofs of storage: It is a service level agreement between the CSPs and its clients. It ensures the data stored in the CSP's servers would never be used by the CSP without the client's permission.
Server aided secure computation: This security mechanism offers a server and users to perform computation on the cipher-text without revealing the contents of the original data.
Tools: Tools encompass data loss prevention systems, unusual behavior pattern detection tools, format preserving and encryption tools, user behavior profiling, decoy technology, and authentication and authorization technologies. These tools provide functions such as real-time detection on checking traffic, audit trails recording for future forensics, and trapping malicious activity into decoy documents to reduce the data breach issues.

VI. SECURITY CHALLENGES

There are numerous security challenges associated with cloud computing. Some of them are as follows:
Privileged User Access If any of the confidential information of the client is accessed by an unauthorized user then the client should acquire a new membership to verify about the unauthorized access. Otherwise the leakage of information will be increased. The owner of the data is having full privilege rights over the data stored. All other users are having only certain set of privilege or access rights.
Regulatory Compliance Cloud provider perform internal audit to the cloud systems and processes, but never permit for any external auditing processes. Installing new security certificates to the network is also dropped by the cloud provider.
Data Location In cloud computing conditions the client of the cloud is ignorant of the storage areas of the information.
Investigative Support An exact request concerning the unlawful access to the customer information in cloud computing is troublesome. The unapproved access is finished by either inside (internal client) or remotely (external client).
Data segregation In cloud computing, the data from one client can be made available to other clients through sharing process. So more than one client can accesses the data in parallel with each other.
Recovery If the server or the data farm utilized by the cloud provider for putting away the customer information is flopped because of characteristic catastrophes or framework disappointments then it's the obligation of the cloud provider to advice about the status of the customer information to him.

VII. DISCUSSION

We have perceived a couple of research areas that are as yet unattended in cloud computing information security, for example, reviewing, and relocation of information starting with one cloud then onto the next where the data breaches are conceivable. The vast majority of the cloud scientists have their emphasis on quick execution and minimal effort services, yet the nature of service has not been genuinely considered. The core concern is related with data and its transmission. Data migration from one cloud to another is not achievable, due to the heterogeneous nature of clouds. Non availability of tools that ensure that user data has been deleted from the cloud if the contract has exhausted leads to serious concern on breach. Researchers have to pay attention on data privacy threats to provide some standards for permanent data deletion. In addition to this, mobile applications provide higher level of threat for data, as there is a less security on application's development. It is trusted that the cost reduction component in cloud computing will additionally experiment the acknowledgment of cloud computing in different fields of cloud applications. With the generous development in cloud computing worldview, the security pulled in the consideration of researchers but still has not received sufficient enhancement. In this study we found cloud security issues such as firewall, issues in configurations, malicious insiders, damaged binaries, multi-tenancy, side channels, weak browser security, and mobility. It is also underlined the deficiencies of security systems designed for cloud that contain the high communication and computation overhead and the detection efficacy and analysis. Furthermore the security against the data breach issues has the following short comings like lack of transparency, issues itself protection techniques, No proper technique for data leakage, searching and indexing in encrypted data, balancing between data privacy and provenance.

VIII. FUTURE RESEARCH DIRECTIONS

Since cloud is one of appealing technology for good business also, speculation, the analysts are spurred to take part in tackling the genuine issues of cloud security in view of data breach, all the more particularly, security and protection challenges of cloud servers and cloud clients. There are diverse cloud models proposed by researchers and various computations for data security, data availability, data integrity, securing from misuse, security audit thus on. We felt the need to characterize these security related researches and directions to motivate researchers to identify the research areas where the new proposals is expected to characterize the security especially in data breach issues for cloud computing. Following section outlines it.

Protect Critical Information

The privacy information of the user should be given higher priority and focus has to be given to secure them. More research is required to protect the critical information infrastructure by analyzing the legal background and involving all laws from all sectors. From the technical

viewpoint, the new methods are to be evaluated which threaten the security of critical information infrastructure.

Exploring computational calculators

A few researchers have attempted to give computational models to quantify the data breach cost, yet the methodologies create a generous connection amongst cost and probability which is difficult to approve. Along these lines, the probability computations gave by data breach cost adding calculators are required to be investigated in detail. Thus it is a dire need to explore computational calculators to study this topic further.

Third party authentication

User privacy breach is one of the major data breach issues. To solve the privacy issue, methods have been developed to protect the user data privacy and user querying privacy. However, these methods provide user level privacy control, which can be enhanced by providing security for data integrity. Third party authentication mechanism can provide a solid security infrastructure for user privacy and data integrity. Future research can be focused to develop a third party authentication framework which can interoperate between cloud service providers and users of the cloud services.

Regulation

Organizations have lost the significant amount of user data due to data breaches. Industries have tried to provide regulations which can avoid them. The industries have examined different procedures, each with its own method to addressing information security. Some procedures can reduce losses due to data compromise, but there is no indication that an increase in procedures would result in fewer compromises. It has been proved that following the regulations can avoid data breaches to some extent. Further research is needed to investigate and develop regulation which will avoid data breaches.

Socio-technical approach

The social aspects related to cloud computing needs to be studied that takes a balanced method to cloud computing data breaches and incorporates the end-user. Users will provide their information to various web sites and thus making data breaches easier. So there is a need to study and balance the struck between social, technical and environmental aspects covered in finding a practicable solution to security breaches.

Security monitoring mechanisms

Security monitoring mechanisms can help to avoid data breaches and analyze security issues. Organizations use different security mechanisms to inspect any suspicious behavior. eg. Cloud Watch by Amazon. The development of new security mechanisms face several obstacles due to different cloud environments used by cloud provider. Therefore there is a requirement to study the different components of the cloud and offer a cross platform solution to prevent data breaches**.**

Service Level Agreement

The data breach risk will be changing based on security SLAs as well as based on client's needs. The existing models can be extended as additional monitoring tools become available. It allows a better evaluation among multiple cloud providers, allowing an evaluation by a user. More research is required to find models which can help user to select a cloud provider with low security risk.

Cryptographic Algorithms

Cryptography relies on encryption and decryption processes of messages by the use of unique keys. Various cryptographic algorithms are used in security methods. Organizations have used ECC (Elliptic Curve Cryptography) over RSA algorithm to protect the user data. However, ECC cannot be used in all circumstances. But it is more crucial to select the appropriate cryptographic algorithms. Hence further research is required in this regard.

Scheduling Algorithms

Scheduling Algorithms of green IT to find the possibility of giving suitable systems to DIDS which stops the data breach challenges for heterogeneous clouds might be a fascinating exploration research area.

Mobile computing

The mobile platforms gangs restricted memory, low processor speed and higher computational prerequisites make obstacle in the endeavors to give best execution on these stages. It is another research issue to investigate in planning the frame work to incorporate cloud infrastructure with mobile computing challenges without data breach issues.

IX. CONCLUSION

The security issue has turned into an obstacle limiting the applications of cloud computing in various fields. This paper concentrates on the significance of data breach issues in cloud computing. The research advance of issues of encryption, access control, and authentication et cetera as for data breach in cloud computing information security has been contemplated. Based on the study, we figure out the key technologies and key challenges the cloud computing data breach issues should be concerned about. Moreover, the research of cloud computing data breach problem is at the early stage of research. In terms of data breach problems in cloud computing data security, there are still a large number of key issues to be studied in depth which has been pointed out in this paper.

REFERENCES

[1] Abdullah M. Algarni, Yashwant K. Malaiya, 2016 IEEE "A Consolidated Approach for Estimation of Data Security Breach Costs",2016.

[2] A Chronology of Data Breaches, Privacy Rights Clearinghouse. [Online]. Available: http://www.privacyrights.org/data-breach.

[3] AkshitaBhandari, Ashutosh Gupta, Debasis Das,2016, IEEE International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT),"A framework for Data Security and Storage in Cloud Computing",2016.

[4] Aryan TaheriMonfared, Martin GiljeJaatun, 2011 Third IEEE International Conference on Cloud

Computing Technology and Science, "Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments".

[5] D.Chandramohan,T.Vengattaraman,D.Rajaguru,R.Baskaran, and P.Dhavachelvan, "A Privacy Breach Preventing and Mitigation Methodology For Cloud Service Data Storage",2013 3rd IEEE International Advance Computing Conference (IACC).

[6] Cloud Security Alliance,Top Threats Working Group,"The Notorious Nine Cloud Computing Top Threats in 2013".

[7] David Kolevski, Katina Michael,2015 IEEE 2015 International Conference on Green Computing and Internet of Things (ICGCIoT)" Cloud Computing Data BreachesA socio-technical review of literature".

[8] FarzadSabahi, "Cloud Computing Security Threats and Responses", 2011 IEEE 3rdInternational Conference on Communication Software and Network (ICCSN), pp. 245-249,May 2011.

[9] http://www.uniassignment.com/essay-samples/information technology/abuse-and-nefarious-use-of-cloud-computing-information-technology-essay.php

[10] http://www.insidecounsel.com/2013/12/06/technology-a-lack-of-due-diligence-still-a-top-thr

[11] https://www.techopedia.com/definition/29863/data-loss.

[12] Ida Madieha Abdul GhaniAzmi, Sonny Zulhuda,SigitPuspitoWigatiJarot," Data Breach on the Critical Information Infrastructures: Lessons from the Wikileaks".

[13] Jitender Grover, Shikha, Mohit Sharma, 2014,IEEE 5th ICCCNT, "Cloud Computing and Its Security Issues – A Review".

[14] Justin LeJeune, Cara Tunstall, Kuo-pao Yang, IhssanAlkadi, 2016 IEEE "An Algorithmic Approach to Improving Cloud Security: The MIST and Malachi Algorithms",2016.

[15] Mark L. Huson, Barbara Hewitt, 2016 49th Hawaii International Conference on System Sciences"WouldIncreased Regulation Reduce the Number of Information Breaches?"

[16] MounaJouini, Latifa Ben ArfaRabai, 2014,IEEE 10th International Conference on Computational Intelligence and Security, "Surveying and Analyzing Security Problems in Cloud Computing Environments",2014.

[17] Nina Pearl Doe, Suganya V., 2014 International Conference on Computer Communication and Informatics (ICCCI -2014)," Secure Service to prevent Data Breaches in Cloud".

[18] Open Security Foundation's formerly Attrition.org. [Online].Available:http ://datalossdb.org.

[19] Qi Zhang, Lu Cheng, RaoufBoutaba,"CloudComputing: State-of-The-Art and ResearchChallenges", Journal of Internet Services andApplications, Vol. 1, No. 1, pp7-18, April 2010.

[20] The Web Hacking Incident Database (WHlD). [Online]. Available:http ://projects.webappsec.orglw/page/13246927/FrontPage.

[21] VERIS.VERIS Community Database (VCDB).[Online].Available:http://veriscommunity.netlvcdb.html.

[22] VivekShandilya, SajjanShiva,The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013),IEEE,2013, "Security in the Cloud Based Systems: Structure and Breaches".

[23] www.cyberriskhub.com/breach

[24] YogachandranRahulamathavan,MuttukrishnanRajarajan, Omer F. Rana,Malik S. Awan,PeteBurnap, and Sajal K. Das, 2015 IEEE 7th International Conference on Cloud Computing Technology and Science,IEEE,2015," Assessing Data Breach Risk in Cloud Systems".