International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Revisiting Cloud Security Threats: Repudiation Attack

Vaishali Singh, S. K. Pandey

Abstract: ***Analysis of security threats and examining of existing mitigation techniques are considered as the major dimensions that need to be focused by next-generation cloud technology. These securities and privacy-based challenges are affecting most of the quality services and online data storage having huge network infrastructures and applications for information management. However, still the variant advantages are the success key of emerging cloud, but poses new security issues and reliability challenges for the users and their service applications. The main concern is an application-based cloud threats, which are not tracked properly and no user action logs are maintained for the evidences. This specially leads to the forging of identifications and manipulation in system actions. Nowadays the most common action observed by malicious attacker is to execute repudiation, where one of the parties involved in communication, denies that actually they have executed the particular conduct. Repudiation attack leads to the major legal actions on massive financial losses, which are not even legitimately proved due to the lack of evidences. Thus, the paper presents a broad indication of repudiation attack through analysis of prior security issues in a cloud environment. Wide-ranging reviews on the same have been presented. The study has tried to figure out the root cause of repudiation attack in order to come up with more suitable and satisfactory counter measures. The study also focuses on a variety of dimensions for future research study in the domain of repudiation based on the previous published works and industry /organization reports.***

Keywords: ***Repudiation Attack, Threats, Audit Log, Timestamp, Digital Signature, eSign, Non-Repudiation***

I INTRODUCTION

The Cloud has a huge, varied and extremely comprehensive ecosystem, which is handling large amount of data [1]. Most of the beneficial applications of cloud platforms focus on the aspect of data storage [1]. Even though with more practicality and flexibility, these service models bring challenges to data security [1]. Introducing emerging features like elasticity, scalability and agility through allowing data access anywhere, on any platforms had responded to challenges and threats [2] [5].

Manuscript published on January 30, 2020.
* Correspondence Author
Vaishali Singh*, Research Scholar-CS, Jagannath University, Asst. Prof., St. Xavier's College, Jaipur, Email: vaishalisingh@stxaviersjaipur.org
S. K. Pandey, Dept. of Electronics & Information Technology, Ministry of Communications & IT, Govt. of India, New Delhi, India, Email: santo.panday@yahoo.co.in

The vulnerabilities in data storage are presented through various threat classification models [3] [4]. STRIDE is the main mnemonic for events happening wrong in security [6]. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege are considered as the main threats [6].
LINDDUN (Likability, Identifiability, Non-Repudiation, Detectability, Disclosure of information, Content Unawareness Policy and consent Non-Compliance) is another important element of STRIDE threat modeling as the main security measures [7].

The present paper focuses on the repudiation attack in which the system and applications are unable to manage the control logs properly and allows the malicious attacker to manipulate the identity and actions of the user [8]. The attacker logins through inappropriate data for accessing log files by changing the authorized identifications [9]. Thus, system logs need to be secured effectively for the security of information and to find preceding actions [9]. In such cases repudiation attack acts as an important aspect where the user claims that nothing has being done wrong regardless of whether done or not by him/her. The system needs to ensure that the logs are secure and preserve while addressing repudiation [10].

If the companies had not maintained any logs for investigating such actions or attempts for repudiating, there is no means of proving anything without evidence [11]. These logs are more susceptible to threats while sending over the network and designed by gathering various data from different sources to different destination with security privileges [12]. Repudiation attack claims that the sender or receiver had not done anything malicious and was not responsible for any loss [13]. Repudiation attack violates non-repudiation objective of security [13].

Through the repudiating attempt, attacker notices the user sessions login's, even if no logs are maintained or if logs are maintained, then the attacker embeds the malicious logs, with the main logs with the help of log reading code [14]. In such cases, the attacker is main fraud entity but the identity, which was executing malicious attempt, is of the user, therefore with innocence user claims to have "not clicked" and "not received receipt" [14].

Since user is not the attacker who has used someone else's payment account without any authorization [14]. Thus, repudiate is not often the attacker that is why is called as someone rather than the attacker who may have failed by process or technology. In such cases, due to avoidable satisfactory auditing and recordkeeping, it becomes hard to provide evidence for repudiation attacks [14].

Technologies like digital signatures, fraud preventions, timestamps, logs maintenance, hash trees, cryptography and audit trails are the security measures for repudiation challenges but these measures are not platform provided but are implemented by the users [15].

Therefore, use of single security measures alone is not sufficient for the non-repudiation objective. Multiple security measures are required at a time to maintain non-repudiation. Sender's non-repudiation security measure cannot deny with this fact that they are the originator of the information sent [16]. Likewise, receiver's non-repudiation security measure cannot deny with this fact that they are the recipient of the information received [17].

Therefore, the research on repudiation attack in cloud will represent broad prospects through revisiting the related literature. The paper on repudiation attack in cloud includes a variety of conclusive results based on the available works, industrial reports and surveys. This may perhaps support in the improvement of a processes to examine the repudiation attack and provide countermeasures.

Beyond this **"*Introduction*"** on the background details, the rest of this paper is organized as follows. The section II defines "***Methodology***" and section III **"*Root Cause Study*"**. Section IV highlights **"*An outline of related work*"** and Section V determines **"*Results*"**. Finally, **"*Conclusion and the Future Work*"** have been reported in section V.

II METHODOLOGY

In order to achieve the research study aims, the research is based on a comprehensive review of journal articles, conference papers, books and edited volumes.

III ROOT CAUSE STUDY

Root cause analysis focuses on the main loopholes and weaknesses causing repudiation attack in the cloud system. This research study supports the experts to investigate the exact sectors of vulnerabilities to improve security development. Chief reasons for the occurrence of the repudiation attack are given as under:

1. **No adoption of appropriate track controls mechanism. [17]:** There are no rules and regulations for the server owners and application users to keep track of the software inventory. These responsibilities are limited with the installed security appliances.
2. **No logs maintenance of each identity [18]:** Weak control setup is provided by the IDMS to implement and maintain the service customer event logs. This leads to no evidence existence and accountability of a particular action. Due to no activity logging technique and real time, tracking the malicious attacker takes an advantage to repudiate the customers easily. This leads to major losses like unauthorized use of data and identity forgery of the user's credentials.
3. **Inadequate audit strategies for cloud application services [21]:** Inadequate audit strategies with unskilled training for addressing the audit issues are the major reasons for repudiation. The audit questionnaires incorporated in regulatory requirements are not automated with updated tools. IT audit approach does not meet the security requirements and objectives of cloud.
4. **Lack of planning for protection of audit information [21]:** Cases, where no plan is implemented to protect information created by auditing decisions leads to unauthorized access and inadvertent deletion of valuable data through repudiation. If the audit information is not secure than it can affect the legal exceptions of consumer's identity protection and the standards of company.
5. **Unknown and untrusted access permission to data logs [20]:** Data logs are generally exploited through untrusted and unknown access permissions. These unknown permissions lead to negative consequences in the domain of countermeasures configuration and results in complete erasing of significant evidence through the unauthorized activities**.**
6. **Weak authentication and security objectives in protocols of application layer [22]:** The application layer is directly connected to Internet and is also known as the SaaS interface layer. The user through this layer utilizes all the applications, thus the major management responsibility is on the application layer for the installation, removal and update of databases and software's. Therefore, the security challenges and issues related to the web application is directly a concern for application layer security.
7. **Limitation of a role-based authorization model [17]:** The major complex affair is role explosion and unmanaged numerous real-world roles based on their privileges and permissions in limited number of users that creates non-scalability and repudiation issues.
8. **Enable anonymous access but authenticate every principle [23]:** According to the least privilege principle, one can be granted anonymous access with minimum privileges as specified in the security guidelines for completing the task. Still it is important to secure the data by all the users and even authenticated users by limiting their scopes to read and analyze the application on the Internet.
9. **Use of weak granular authorization model in order to produce precise logs at all tiers [24]:** The basic problem occurs when the granular authorization needs to incorporate into the application layer. This increases the cost and complexity of application development but still not appropriate to get granular authorization results.
10. **No log actions during capturing any sensitive data in logs [19]:** Whenever the hacker is able to fetch out the sensitive information from the logs like personally identifiable information (PII) or credentials stolen from the platform, no action logs are created to get an alert message for security. Separate action log commands should be applied to the secret data files.
11. **Wireless links between nodes are unreliable in mobile ad hoc network [25]:** As there exists various types of nodes mobility with limited energy power source creates unreliable wireless medium due to which extensive number of packets are lost.

Thus, security of these nodes during communication and transmission ensures the reliability and decreases the repudiation threat.

12. **Persistently change in topology [26]:** One reason due to which repudiation occurs is frequently changing topologies. These topologies do not remain stable because of mobility of nodes and wireless channel has limited bandwidth, which results in unreliability form.
13. **Deficiency of security features integration in configured wireless routing protocol [27]:** Absence of security features and lack of investigational quantitative study creates deficiency in wireless routing protocols due to which more attacks are focused in the routing infrastructure.
14. **Lack of security in transport layer and network layer for preventing the nodes in network [22]:** Repudiation occurs due to the improper security measures employed for mitigating the attacks in accessible routing protocols for wireless networks. Use of these compromised nodes in network results in repudiation and transfers the valuable information to unauthorized network nodes.
15. **Traditional encryption mechanisms are insufficient for providing security network layers [28]:** The traditional encryption standard is not sufficient for the privacy and security of processing state of data as all the operations are managed by the cloud provider and needs the decryption mechanism simultaneously
16. **Email protocol does not verify that the indicated sender is indeed the real sender [29]:** Less efforts are made while tuning the data with email confidentiality for security purpose. The scripting languages and other auto-execute/download features on the hyperlinks and attachments, which are mailed as the part of content, require more focus.
17. **Non-repudiation is mostly concerned with dishonest behavior of the participants [30]:** The diversity of user's and their behavior is one of the major issues that creates the security problems in cloud platforms. The dishonesty in the behavior of the user shows the abnormal privacy and access to the data. Moreover, the diversity of cloud users and user's behavior makes the security problems of the cloud platform more prominent.

IV A SURVEY OF RELATED WORK

Nowadays, every individual need evidence for proving their identity and their work authenticity. Even each user wants to store their documents for a long period electronically. For storing the documents blindly on network, the objective which is most focused is non-repudiation.

The current literature survey on non-repudiation presents a comprehensive overview. There are varieties of undergoing research work focusing on repudiation attack in diverse domains of Cloud applications and examine some of the trendsetting research involvement are given as under:

1. **Analysis of Integrity Vulnerabilities and a Non-repudiation Protocol for Cloud Data Storage Platforms [31] -** This paper has analyzed the vulnerabilities of the available cloud storage platforms and focused on the problem of repudiation. The paper has proposed a non-repudiation protocol specifically for cloud computing environment, which can prevent applications from cloud threats and attacks in the network relations.
2. **Continuous Certification of Non-repudiation in Cloud Storage Services [32] -** This paper has proposed a certification model in the cloud storage services whose objective is to sustain non-repudiation. This NR certifying model was based on continuous monitoring. The model has been defined on the approach of CUMULUS. This model relates to same as level three-maturity certification with reference to certification scheme of CSA.
3. **A fair non-repudiation framework for data integrity in cloud storage services [33] -** This paper has exposed few of the marketable vulnerabilities in cloud storage services which are the cause of conflicts between the service provider and the user of the cloud storage. The research has proposed a framework which is without risk of contention and will support the procedure for fair data transmission. This study has presented multi party non-repudiation protocol and two-party non-repudiation protocol for securing the cloud storage from the network attacks.
4. **A fair multi-party non-repudiation scheme for storage cloud [34] -** This research study has focused on the commercial vulnerabilities found in the services of cloud storage domain. This study has analyzed in depth the problem in cloud environment due to repudiation. Moreover, this research work has projected a new multi-party non-repudiation scheme for resolving non-repudiation problems. The paper has provided description of the new schemes and its operations. The paper has also focused on the prevention mechanism of the scheme against the network threats.
5. **On the Security of Fair Non-repudiation Protocols [35] -** This study on security domain has revisited on two of the non-repudiation protocols. The results have presented some new attacks related to the termination property and fairness objectives of these protocols. The paper has proposed preventive measures which intensify the strength of the design and the way of implementing non-repudiation protocol. Through a novel approach, a fair non-repudiation has been developed in the applications for mitigation techniques.
6. **Fairness in Non-Repudiation Protocols [36] -** This research work has highlighted few of the problems related to the specification of fairness in non-repudiation protocol. The first problem focused in the paper was on perfect information having implicit assumptions. Another problem was the shortage of possible effectiveness. The paper has proposed solutions to these problems by re-defining fairness. This paper has also created a hierarchy of several fairness definitions and indicated various consequences of the present work.

7. **An Intensive Survey of Fair Non-Repudiation Protocols [37] -** This work has defined the characteristics of fair non-repudiation protocol. The paper has examined the survey of majority of significant non-repudiation protocols with the third trusted party and in absence of the trusted party.

   This paper has also discussed about the development of trusted third-party participation and described the latest protocol having transparent trusted third party. The paper has also highlighted few of the ad-hoc issues in the management of non-repudiation verifications.

8. **Security Analysis of (Un-) Fair Non-repudiation Protocols? [38] -** Variants of fair non-repudiation protocol was demonstrated, based of protocol analysis via simple homomorphism verification tool and asynchronous product automata. New attacks based upon these protocols were presented and enhanced version of the Fair Non-repudiation protocol was proposed.

9. **Evolution of Fair Non-repudiation with TTP [39] -** This manuscript has reviewed the earlier research studies based on the development of fair non-repudiation protocol and its techniques especially related to Trusted Third Party (TTP) to propose a securely well-organized novel version of fair non-repudiation protocol.

10. **Towards Verification of Non-repudiation Protocol [40] -** The paper has focused on the Cryptographic protocols and the failures related to the design objectives. The research study has formalized their goal towards the non-repudiation services with the use of SVO logic for the requirements for verifying non-repudiation protocols.

11. **Probabilistic Non-Repudiation without Trusted Third Party [41] -** This manuscript has planned a novel hypothetical generic protocol for non-repudiation services. The paper has aimed to present the ability to achieve fair non-repudiation services in the absence of third party. For this, the paper has proposed actual implementation motivated by this generic protocol.

12. **Formal analysis of a non-repudiation protocol [42] -** This manuscript was functional in applying and communicating sequential theories for the modeling and exploratory of non-repudiation protocol according to the formal analysis by the paper authentication and key exchange protocols differs from non-repudiation protocols therefore the study depicted different kinds of properties required to model this protocols with a distinct standard approach. Hence the basic non-repudiation protocol framework proposed by Zhou Gollmann was studied within this new framework for finding novel considerations.

13. **Analyzing the security of a non-repudiation communication protocol with mandatory proof of receipt [43] -** This paper has examined the mandatory proofs of receipts in the non-repudiation communication. The study has proposed modal logic based on knowledge with verification technique and tried to prove the protocol correctness. Further undergoing the analysis, the deductive reasoning has been used on the desired protocols for deducing the goals using axioms sets, inferences rules, theorems on the assumptions and messages exchanges. When the protocol was assumed to act in accordance with the goal it was accurate and secured.

14. **An efficient non-repudiation protocol [44] -** The manuscript has focused on a particular variant of fair non-repudiation protocol by means of the trusted third-party mechanism. This study has involved the trusted third party only in such a case that if one party would not obtain the probable non-repudiation confirmation from the front party. This efficient variant presented in this study would help the two parties to resolve such a communication problem in an environment.

15. **Long-term integrity and non-repudiation protocol for multiple entities [45] -** This paper has focused on the unsolved issues of privacy and security faced in the development of innovative applications and improved quality of architectures in smart cities. Another problem focused in the paper was the latest development of quantum computing in which public key infrastructure-based solutions were not able to maintain the objectives of non-repudiation and continuous data integrity. Therefore, the paper has proposed a new lightweight non-repudiation protocol which can be applied on various entities using hash functions and Merkle tree. The study has also proposed an efficient demonstration of the presented approach through the parameters like message overhead, continuous ability to maintain data integrity, low transmission rate and non-repudiation.

16. **Fulfilling mutual non- repudiation for cloud storage [46] -** This study has proposed ways to obtain mutual non-repudiation among the service providers and users in the absence of client's workstation for exchanging the messages in cloud storage in such case client only needs to secure the last confirmation it has received. The study has pinpointed on the parallel accessible files needs to be prohibited, if the attestations required to be chained together as one. This paper has also proposed concurrent files access to multiple chains in a peer account. This research paper has further proposed the mechanism to present the applicability of hash tree for elimination of stored attestations. These proposed experiments have demonstrated the feasibility of scheme and provided the guarantee of mutual non-repudiation in the service level agreement (SLA).

17. **How to achieve non-repudiation of origin with privacy protection in cloud computing [47] -** This manuscript has focused on the security challenges of cloud computing particularly on privacy and security on message originator at non-repudiation of origin (NRO). The paper firstly described NRO-I and NRO-II, the actual goals of non-repudiation of origin which can easily be taken using customary handwritten signatures as the confirmation of origin. The result depicted by the study was that empirical persistent digital signatures could provide NRO-I but not constantly NRO-II using counterexample. Further, the study work contributed in communication protocol for achieving privacy of message originator and accepting non-repudiation of origin. The proposed protocol has satisfied the NRO-II and I. The core of present protocol was the secured verifier signature scheme.

18. **Non-repudiation and digital signature [48] -** This study has focused on the non-repudiation property and explained ways to achieve this property using digital signatures. Further, the study has focused on defining the problem of repudiation for digital document and their correctness while transmitting the document to the authenticated receiver.
19. **Is non-repudiation really non-reputable with digital signatures? [49] -** The study has focused on Repudiation problem explaining its legal concept used in information security. The study and security communities has raised problems related to non-reputability with digital signature really exist. The research has also focused on the difference between authentication and non-repudiation. Further, in detail the paper has discussed the importance of eIDAS and Qualified Electronic Signatures (QES).
20. **Securing digital signatures for non-repudiation [50] -** Disagreement of transactions is a general trouble that could fail the objective of the business. The paper focuses on the conventional approaches that were inefficient to attain non-repudiation in e-commerce. This manuscript presents a scheme to secure digital signatures as non-repudiation evidence with an adjustable degree of risk.
21. **Non-repudiation in digital environment [51] -** This paper has focused on the following issues related to non-repudiation legal definition and crypto methods underlying non-repudiation. The research has also explained the technicalized vulnerabilities or weakness adoption in terms of legal aspects in article 13 and even focused on the Common Law positions for trusted system. This paper has also lighted on the UNCITRAL Model Law and the onus of proof issue under article 13. This research paper has focused on the lawmaker and researchers' problems who are confused with the terms on non-repudiation while dealing with crypto and legal domain. The study of the paper has clarified the fundamental definitions and main problems of the signer while incorporating trust objective in electronic communication.
22. **Digital Signing and Non-Repudiation [52]** - This paper has focused on the standards used in advanced electronic signatures generations and validation. The paper has also provided a detailed study about the processes implemented in generation and validation of signature. Further, the research also focused on defining the needs of complaint applications while generating and validating advanced electronic signatures.
23. **Enhancing the reliability of digital signatures as non-repudiation evidence under a holistic threat model [53] -** The research has highlighted the reliability enhancement of digital signature for ensuring the non-repudiation. The paper has depicted that the present technology does not have a satisfactory level of trustworthiness for a reliable evidence based on non-repudiation and digital signature. This study also finds and motivates the security experts by explaining the digital signature facts with legal policies under legislations. The paper has provided an opinion that these security threats are challengeable to the reliability of evidences based on repudiation needs to be dignified and categorized. Therefore, the study proposed taxonomy for digital signatures attack and threats planned for systematic classification. The study has also focused on a new approach, which is more trustworthy, and robust full in enhancing the digital signature reliability. The paper presents the two new approaches as extended e-signature policies and signature environment division process. The core of paper is to develop the new fair exchange protocol for enhancing the reliability of non-repudiation and digital signature.
24. **Implementing Nonrepudiation [54] -**The study has focused on the overview of nonrepudiation. The research has explained the role of digital signatures, secure timestamps and secure audit logs in achieving non-repudiation in business-to-business engine. The paper has in depth focused on the digital signature support provided to business protocols. Furthermore, the study has also progressed to implement and explain the configuration of secure timestamp services and secure audit log service. This study has also described the service provider interfaces for the non-repudiation services mainly secure audit log and timestamp.
25. **How Digital Signature Works in India [55] -** This article has defined the digital signature definition with respect to different domains in India. According to the study, digital signature has been considered as mathematical method for indicating legitimacy of documents, it is a standard for cryptographic protocols suite, used as electronic signature, in general employed for asymmetric cryptography and used to achieve the non-repudiation objective. The paper has also focused on the Indian Law, which is an important governing aspect for security services specially while dealing with digital signatures. The paper has highlighted the important points of Section 3 of the IT Act with subject to digital signature used as authenticity objectives for electronic documents.
26. **Effective design of a parametrical security model for digital signatures using cryptography [56] -** The paper has studied on the digital signature authentication for secure communication and focused on the non-repudiation aspects of security. The study has discussed different methods to secure the communication during transactions and provided guidance to prevent from fraudsters, simultaneously detecting the tampering of electronic data.
27. **What is Aadhar Sign? [57] -**This study has focused on the Aadhar Sign technique, which has ensured authentication, integrity and non-repudiation considering the core function of digital signature in India. The paper has elaborated the benefits of Aadhar Sign as a new method of digital signing technology, which will ensure the non-repudiation aspect between two parties. The paper has described the Aadhar Sign features, which explained that it is completely law compliant method and was provided by the regulator of certifying authorities, ministry of electronics & IT, Govt. of India through third party mediators as eSign service providers, UIDAI and application service providers.

The study explained that, each time for transaction request, the Aadhar Sign would be used. Know your customer authentication will process concurrently through the Aadhar KYC. After which, one-time use digital signature certificate will be issued for signing the transaction request document using servers of UIDAI, ASPs, CCA and ESPs.

28. **eSign [58] -** This article has focused on Open API integration with eSign for achieving the non-repudiation feature of security for the online service provider in their existing services.

This study has focused on the use of eSign objective, which is an electronic signature connected with Aadhar. The study has further focused on the features of eSign, which is considered to be easy, secure online, legally valid, flexible to implement, user privacy maintained, and after usage, the key destroys immediately. The research also focused on the basic benefits like paperless method, no key storage and key protection, user ease, based on integrity, non- repudiation and authentication objectives, reduced cost and save time. The study also represented the working of eSign through a pictorial diagram.

V RESULTS

Research experts have done significant hard work in the area/s of Repudiation attack, although there is still a necessity of additional effort on the mitigation techniques more imperatively. Based on above mentioned prior research and survey, a variety of area/s has been recognized as given below and a pictographic representation of the same is given.

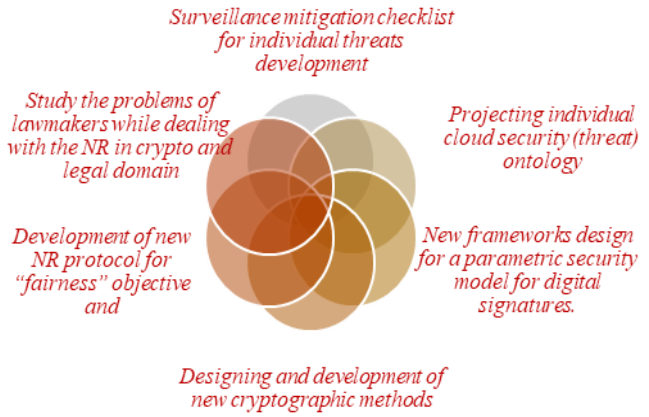

Figure 1 Conclusive Findings in the field of Non-Repudiation

S. No.	Problems	Conclusive Findings (Results)
1	No Updating in existing mitigation technique	The need is to re-examine the existing countermeasures on the initial stage according to the user's perception for inculcating non-repudiation objective, for the reason that after executing many existing mitigating frameworks, still Repudiation is a major issue for cloud.
2	Lack of overall Identification of weakness	Repudiation is considered as in top ten threats, therefore needs to identify the in-depth weakness or loopholes from the front end as well as back end of the cloud service.
3	Unstructured approach towards vulnerability domain	There is need to conduct a structured approach towards the vulnerability domain for expose the cloud threats at their initial levels.
4	No ontological explanation of individual threat	Another method for resolving the repudiation issue is projecting individual cloud threat ontology for provider and consumer in cloud [4] [5].
5	No inclusive global observance of threat	By focusing on the issue of repudiation in cloud and top ten threats, companies will meet all-inclusive global observance, which will provide best ways for mitigation techniques requirements.
6	No mitigation checklist for individual threats	The society and user needs approach to understand repudiation and non-repudiation in their simplest way. Therefore, requires a surveillance mitigation checklist for individual threats development for helping in applying privacy protections for user and its organization.
7	No in-depth study to focus on the vulnerabilities	The future study requires to focus and analysis on the vulnerabilities existing in the cloud storage platform and the reason for repudiation
8	Outdated certification models	New certification models need to be proposed in the cloud storage services whose purpose is to maintain non-repudiation.
9	More focus on the "fairness" objective	New non repudiation protocol needs to be developed to support "fairness" objective between the user and service provider in cloud storage to eliminate the risk, threats and conflicts between two parties.
10	Lack of comparative study of existing protocols	The future research needs a comparative study of existing protocols on the basis of designing and implementing the non-repudiation protocol
11	Lack of updating existing preventive measures and framework	The study also requires a novel preventive measures and framework for designing and implementing the non-repudiation protocol after the comparative study finding.

12	Awareness campaigns required for threat study	The future study can focus on the awareness campaigns for the use of Aadhar Sign and increase the objective of non-repudiation and trust in organizations.
13	Less cryptographic and effective methods	Designing and development of more cryptographic and effective methods for securing the digital signature, eSign, e-certificate and electronic documents as the evidence for non-repudiation.
14	Inefficient parametric security model	New frameworks design for a parametric security model for digital signatures.
15	Old schemes used for security services	Development of new schemes, important for governing aspects for security services in Indian Law.
16	More focus on ICT for authenticity	Future study can focus and analysis the Information Technology Act 2000, which deals with the use of eSign, digital signature and e-certificate authenticity.
17	Less secured timestamp services	There is a need of new structural designs and implementation of more secured timestamp services for achieving non-repudiation objective.
18	Updation in fair exchange protocol	There is a need to develop the more secure and preventive fair exchange protocol for analyzing the user's trust measure, reliability of non-repudiation.
19	Less significance of complaint applications requirements	There is a need to look in depth about the significance of complaint applications requirements for generating and validating new electronic signatures and certificates.
20	Problems of lawmakers	The need is to study the problems of lawmakers while dealing with the key points of non-repudiation according to crypto and legal domain.
21	Struggle in incorporating trust objective models	The study needs to focus on the foremost struggle of the signer and organization during incorporation of trust objective in digital communication.

VI CONCLUSION AND FUTURE WORK

There are major needs for high cloud adoption rate and for smooth operation execution for deployed businesses to abide by legal, secure and compliance policy for restricting the threats in cloud. These computing concepts are only required to create a public package of resources, which comprises of various services, application, servers, data storages and network connectivity for the user at one place. Cloud is considered as one of the basic pillars of emerging computing paradigm on Internet. On demand effective services and rapid development of huge infrastructures, is the achievement keys of emerging cloud.

Nevertheless, the adoption and pervasiveness in cloud environment is blocked-up due to security issues and challenges to an immense level. There are many trust parameters-based clarifications for cloud but on the same time all, the security issues are not addressed individually in cloud threat domain. Therefore, this paper has addressed on the security issue related to a specific cloud threat "Repudiation Attack". The study has focused to develop or present detailed analysis of various unsolved challenges associated with repudiation attack threatening the cloud implementation, deployment and affecting the various stakeholders associated with it.

The future study may be to outline the repudiation attack in one of the individual cloud threat ontology with considering different factors of mitigation techniques and security requirements. Accordingly, new satisfactory countermeasures may be structured and developed for repudiation attack that may provide a suitable security service to the user and provider. Moreover, the future work may be to embed the countermeasure on the cloud security ontology for more scientific ways. Another future work is to create Surveillance Mitigation Checklist (SMC) for repudiation attack, which may be used to examine the mitigation techniques and will result in reduction of failure actions to an extent. SMC will also pinpoint the crucial area/s for more detailed study in any organizations. The research work will help cloud to create an enhanced confidence and trust among the stakeholders of the services and applications.

REFERENCES

1. Vaishali Singh & S. K. Pandey, "Research in Cloud Security: Problems and Prospects", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) Vol. 3, Issue 3, Aug 2013, pp. 305-314.
2. Vaishali Singh & S. K. Pandey, "Revisiting Cloud Security Issues and Challenges", International Journal of Advanced Research in Computer Science and Software Engineering Vol.3.Issue7, July-2013, pp. 1-10.
3. Vaishali Singh & S. K. Pandey, "Cloud Security Related Threats", International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 pp. 2571.
4. Vaishali Singh & S. K. Pandey, "Revisiting Security Ontologies", International Journal of Computer Science Issues, Vol 11, Issue 6, No. 1, November 2014 Pg150-159.
5. Vaishali Singh & S. K. Pandey, "A Comparative Study of Cloud Security Ontologies" 2014 IEEE 3rd International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), Pg. 797-803.
6. Jiang Li, Chen Hao, Deng Fei and Zhongqiu sheng, A Security Evaluation Method Based on Threat Classification for Web Service, Journal of Software, Vol. 6, No. 4, April 2011, page no.595
7. Linddun privacy threat modeling - official website, https://distrinet.cs.kuleuven.be/software/linddun/index. php

8. Umme Habiba, Rahat Masood, Muhammad Awais Shibli and Muaz A Niazi, Cloud identity management security issues & solutions: a taxonomy, Complex Adaptive Systems Modeling 2014, 2:5 http://www.casmodeling.com/content/2/1/5
9. S. Muthu raj kumara, S. Ganapathy, M. Vijayalakshmi and A. Kannan, Secured Temporal Log Management Techniques for Cloud, International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science 46 (2015) 589 – 595
10. Fundamental Security Concepts, Describe Principles of Information Security, https://cryptome.org/2013/09 /infosecurity-cert. pdf
11. Shams Zawoad, Amit Kumar Dutta and Ragib Hasan, SecLaaS: Secure Logging-as-a-Service for Cloud Forensics, https://arxiv.org/pdf/1302.6267.pdf
12. Cloud Security Alliance, The Treacherous 12 - Top Threats to Cloud Computing and Industry Insights,2017, https://downloads.cloudsecurityalliance.org/assets/research/top-threats / treacherous-12-top-threats.pdf
13. Karsten Brauer, Authentication and Security Aspects in an international multi-user network, Thesis (UAS) Information Technology, European Computer Science, 2011, https://www.theseus.fi/bitstream/handle /10024/30738/Karsten_Brauer.pdf
14. Sanchika Gupta, Padam Kumar, Taxonomy of Cloud Security, International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.3, No.5, October 2013
15. Ahmed E. Youssef and Manal Alageel, A Framework for Secure Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012
16. Yang, Xiaoyu, Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing, IGI Global, 31-Jan-2013
17. Davit Hakobyan, Authentication and Authorization Systems in Cloud Environments, Master of Science Thesis Stockholm, Sweden 2012 TRITA-ICT-EX-2012:203
18. Ahmed Lounis. Security in cloud computing. Other. Université de Technologie de Compiègne, 2014
19. A Study on Cloud Computing Security Challenges, Master Thesis Software Engineering Thesis no: MSE-2012:82 01 2012, https://www.diva-portal.org/smash/get/diva2:830115/FULLTEXT01 .pdf
20. Umme Habiba, Rahat Masood, Muhammad Awais Shibli and Muaz A Niazi, Cloud identity management security issues & solutions: a taxonomy Complex Adaptive Systems Modeling**2**:5 Springer. 2014
21. William Aiken, John Kissell, Jungwoo Ryoo, Syed Rizvi, Cloud Security Auditing: Challenges and Emerging Approaches Mar 08, 2015, https://www.infoq.com/articles/cloud-security-auditing-challenges-and-emerging-approaches
22. Safiriyu Eludiora, Olatunde Abiona, Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime and Lawrence Kehinde, A User Identity Management Protocol for Cloud Computing Paradigm, Int. J. Communications, Network and System Sciences, 2011, 4, 152-163
23. Raja Shree S., Secure Substantiation in Cloud Computing Environment, International Journal of Modern Engineering Research (IJMER), National Conference on Architecture, Software systems and Green computing (NCASG), Pp-42-46 ISSN: 2249-6645
24. Cloud Security Alliance's, Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 is https://cloudsecurityalliance .org/download/securityguidance-v4/., 2017
25. CH.V. Raghavendran, G. Naga Satish and P. Suresh Varma, Security Challenges and Attacks in Mobile Ad Hoc Networks I. J. Information Engineering and Electronic Business, 2013, 3, 49-58, September 2013, MECS
26. Ivana Kostadinovska, Cloud security - An approach with modern cryptographic solutions Master's Thesis The 2nd Cycle Masters Study Programme Computer And Information Science,2016
27. Sumati Ramakrishna Gowda and P.S Hiremath, Review of Security Approaches in Routing Protocol in Mobile Adhoc Network IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 2, January 2013, ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814
28. JaydipSen, Security and Privacy Issues in Cloud Computing, In book: Architectures and Protocols for Secure Information Technology Infrastructures, Edition: First Edition. September, 2013, Chapter: 1, Publisher: IGI-Global, USA.
29. NunoMota, Email Security with Digital Certificates (Part 1), MAY 31, 2016, http://techgenix.com/email-security-digital-certificates-part1/
30. Mahendran D, Jothi Prakash V, S. Manikandan, K. Karthiban, A Study on Effective Methods for Ensuring Privacy in Cloud Computing Environment, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, March 2015
31. Jun Feng, Yu Chen, Wei-Shinn Ku, Pu Liu, Analysis of Integrity Vulnerabilities and a Non-repudiation Protocol for Cloud Data Storage Platforms, 39th International Conference on Parallel Processing, ICPP Workshops 2010, San Diego, California, USA, 13-16 September 2010 https://www.researchgate.net/publication /220270055_Analysis_of_Integrity_Vulnerabilities_and_a_Non-repudiation_Protocol_for_Cloud_Data_Storage_Platforms
32. Maria Krotsiani, George Spanoudakis, Continuous Certification of Non-repudiation in Cloud Storage Services, 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, 24-26 Sept. 2014
33. Jun Feng and Yu Chen, A fair non-repudiation framework for data integrity in cloud storage services, Int. J. Cloud Computing, Vol. 2, No. 1, 2013
34. Jun Feng, Yu Chen, Douglas H. Summerville, A fair multi-party non-repudiation scheme for storage clouds, 2011 International Conference on Collaboration Technologies and Systems (CTS), 23-27 May 2011
35. Sigrid G¨urgens, Carsten Rudolph, Holger Vogt, On the Security of Fair Non-repudiation Protocols, http://sit.sit. fraunhofer.de/smv/publications/download/IJIS-2004.pdf
36. Wojciech Jamroga, Sjouke Mauw, and Matthijs Melissen, Fairness in Non-Repudiation Protocols, https://pdfs. semanticscholar.org/c3b8/ac2c587e444469f08bad690c19443f64fa23.pdf
37. Steve Kremer, Olivier Markowitch and Jianying Zhou, An Intensive Survey of Fair Non-Repudiation Protocols, http://www.lsv.fr /Publis/PAPERS/PDF/comcom02.pdf
38. Sigrid G¨urgens and Carsten Rudolph, Security Analysis of (Un-) Fair Non-repudiation Protocols, http://citeseerx. istpsu.edu/viewdoc/[150download?doi=10.1.1.86.2406&rep=rep1&type=pdf
39. Jianying Zhou, Robert Deng, Feng Bao, Evolution of Fair Non-repudiation with TTP, Australasian Conference on Information Security and Privacy, ACISP 1999: Information Security and Privacy pp 258-269
40. Jianying Zhou, Dieter Gollmann, Towards Verification of Non-repudiation Protocols, In Proceedings of 1998 International Refinement Workshop and Formal Methods Pacific.
41. Olivier Markowitch and Yves Roggeman, Probabilistic Non-Repudiation without Trusted Third Party, http://citeseerx. ist.psu.edu/viewdoc/download?doi=10.1.1.93.9279&rep=rep1&type=pdf
42. Steve Schneider, Formal analysis of a non-repudiation protocol, https://pdfs.semanticscholar.org/2bb0/bf7c772e74cf964018a85777b3cda6e2b289.pdf
43. Tom Coffey, Puneet Saidha, Peter Burrows, Analysing the Security of a Non-repudiation Communication Protocol with Mandatory Proof of Receipt, https://pdfs.semanticscholar.org/4bd3/81caf466af676be065d0a712bffacea18180.pdf
44. Jianying Zhou, Dieter Gollmann, An Efficient Non-Repudiation Protocol, Proceeding CSFW '97 Proceedings of the 10th IEEE workshop on Computer Security Foundations Page 126
45. Mohamad Badra and Rouba Borghol, Long-term integrity and non-repudiation protocol for multiple entities, Sustainable Cities and Society, Volume 40, July 2018, Pages 189-193
46. Gwan-Hwan Hwang, Wei-Sian Huang, Jenn-ZjonePeng and Yu-Wei Lin, Fulfilling mutual nonrepudiation for cloud storage, Concurrency and Computation: Practice and Experience, (2014) Wiley Online Library
47. Wei Wu, Jianying Zhou, Yang Xiang and LiXu, How to achieve non-repudiation of origin with privacy protection in cloud computing, Journal of Computer and System Sciences Volume 79, Issue 8, December 2013, Pages 1200-1213
48. Non-repudiation and digital signature, Posted in General Security on January 9, 2014
49. Is non-repudiation really non-repudiable with digital signatures? Stefan Hansen on 14. June 2017
50. J. Zhou and K. Y. Lam, Securing digital signatures for non-repudiation, Computer Communications Volume 22, Issue 8, 25 May 1999, Pages 710-716
51. Adrian McCullagh, William Caelli, Non-repudiation in the digital environment, First Monday, 1995-2018. ISSN 1396-0466, Volume 5, Number 8 - 7 August 2000
52. Andy Truscott, Graham Jack and John Whiteside, Digital Signing and Non-Repudiation, July 2007,

https://developer.nhs.uk/wp-content/uploads/2016/12/Digital_Signature_and_Non_Repudiation.pdf
53. Jorge L´opez Hern´ andez-Ardieta and Prof. Dr. Ana Isabel Gonz´alez-Tablas Ferreres, Enhancing the reliability of digital signatures as non-repudiation evidence under a holistic threat model, February 2011, https://e-rchivo.uc3m.es/bitstream/handle/10016/11882/Tesis_Jorge_Lopez_Hernandez_Ardieta.pdf
54. Implementing Nonrepudiation, e-docs, Web Logic Platform, WebLogic Integration, B2B Security, https://docs.oracle. com/ cd/ E13214_01/wli/docs70/b2bsecur/nonrep.htm
55. Simmi Setia, How Digital Signature Works in India, 2017, http://www.iamwire.com/2017/02/digital-signature-india/149093
56. B. Ananda Priya and Ananthi Shesha saayee, Effective design of a parametrical security model for digital signatures using cryptography 2016 International Conference on Communication and Electronics Systems (ICCES)
57. Shivam Singla, what is AadhaareSign? April 12, 2018, The Leegality Blog
58. eSign Online Electronic Signature Service, May 2018 http://cca.gov.in/cca/?q=eSign.html

AUTHOR PROFILE

Ms. Vaishali Singh, is presently working as an Assistant Professor in the Department of Computer Science, St. Xavier's College, Jaipur, India. Research Scholar of Computer Science from Jagannath University, Jaipur, India. She has an excellent academic background right from the school level. Under the Institute-Industry linkage program, she delivers expert lectures on various areas of Computer Science. She has contributed three research papers in reputed International journals and national conferences. Her research interest includes: Cloud Security, Cloud Security vulnerabilities, threats and countermeasures, Access control, Identity measurement etc.

Dr. Santosh K. Pandey, is presently working as Scientist 'C' with the Ministry of Electronics & Information Technology, Government of India New Delhi. Before joining Deity, he was a Faculty of Information Technology with Board of Studies, The Institute of Chartered Accountants of India (Set up by an Act of Parliament) New Delhi. Prior to this, he worked with the Department of Computer Science, Jamia Millia Islamia (A Central University) New Delhi and Directorate of Education, Govt. of NCT of Delhi. He has a rich Academics & Research experience in various areas of Computer Science. His research interest includes: Software Security, Requirements Engineering, Security Policies and Standards, Formal Methods, Cloud Computing, Security Metrics, Vulnerability Assessment etc. He has published around 46 high quality research papers and articles in various acclaimed International/National Journals (including IEEE, ACM, CSI) and Proceedings of the reputed International/ National Conferences (including Springer). Out of these publications, most of them have good citation records. He has been nominated in the board of editors/reviewers of various peer-reviewed and refereed Journals. In addition, he has also served as a Program Committee Member of several reputed conferences in India as well as abroad. He has also been designated in various academic/research committees by the government organizations as well as software companies as a subject expert.