ISSN:2231-0711

Rakesh Kumar et al | IJCSET(www.ijcset.net) | 2017 | Volume 7 Issue 7, 62-68

Cloud Computing PAVD Security System: A Survey

Rakesh Kumar[1], Shubhdeep[2]
Department of Computer Science & Engineering
Guru Nanak Dev University,Amritsar, India

Abstract:-Cloud computing is the best solution for providing a flexible, on-demand, and dynamically scalable computing infrastructure for many applications. In case of private cloud environment access is limited to a group of users or an organization. Even though there are many aspects in cloud environment. The data security, confidentiality and privacy plays a major role in cloud deployment model. Lot of investment is made in cloud based research by MNCs like Amazon, IBM and different R & D organizations. Inspite of these the number of stakeholders actually using cloud services is limited. The main hindrance to the wide adoption of cloud Technology is feeling of insecurity regarding storage of data in cloud, absence of reliance and comprehensive access control mechanism. For the protection of data, we do have a existing technique called PAVD technique. A three security issues of privacy, data security and data verification. Hence it is called as PAVD system.

In this paper, we extended the existing PAVD technique, by adding group signature based verification and adding AES Encryption to it. The issue of protection on device or protection on cloud has found to be the major challenge and survey to provide secure cloud computing environment. In this paper, we mentioned the gap of survey and objectives of thesis work.

Keywords: Member, cloud computing, Security problems, Data security, Signature, DH, RSA.

I. INTRODUCTION

Cloud computing concerns all the feature of creating cloud computing safe. Several of these features are not exclusive to the cloud setting: data is at risk to attack irrespective of where it is kept. Therefore, cloud computing security includes all the theme of computing security, including design of security design, minimization o attack surfaces, defenses from malware, and implementation of access control. But there are some features of cloud computing security that look to be explicit to that area. There are some aspects of cloud computing security that appear to be specific to that domain.

1. Cloud computing security or, more simply, cloud security is an developing sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. The cloud is typically a shared resource, and other sharers (called tenants) may be attackers.
2. Cloud-based data is usually intentionally widely accessible by potentially insecure protocols and APIs across public networks.
3. Data in the cloud is vulnerable to being lost (e.g., accidentally deleted) or incorrectly modified by the cloud provider.
4. Data in the cloud can be accessed by the cloud provider, its subcontractors and employee.

In this report we mention the security mechanism PAVD system. PAVD Means Privacy authentication verification of data. Hence PAVD program utilize two various server's viz. Encryption sever and storage server. It perform three responsibilities, firstly key exchanging and secondly, assess SHA-1 code for the original files for verifying digital signature at the time of downloading and lastly encryption user data using algorithm.

Working of PAVD System

The context level diagram is also referred to as zero level Data Flow Diagram, which describes the system at lowest level of the system. From the Figure it is clear that the PAVD security system consist of two different servers, which are not in contact with each other. Encryption & Storage servers provide encryption and storage services respectively.

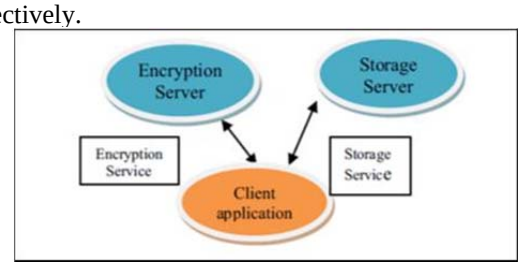

Figure :Working of the PAVD System

II. LITERATURE REVIEW

After the problem was identified the second phase is to review the state of the art. It is important to understand the basic and expertise regarding Cloud computing and the security challenges, issues involved in cloud computing. It is also important to understand the basic and research regarding group based signature and PAVD security system. The study starts by identifying cloud computing security challenges and their mitigation strategies from the literature. To identify cloud computing security challenges group based signature and PAVD cloud be used. Literature study is conducted to develop a solid background for the re-search. Various simulation tools and their functionality are studied. Literature Review (LR) helps to identify state of art in a study and Cloud computing helps to revisit into references used in the article and information related to the current study. The rationale for selecting better security technique cryptography algorithms and group based signature and PAVD security system and literature review is as follows:

1. The topic of choice (cloud computing) is new and using other techniques might result in a few papers.
2. The LR helps to identify articles that are relevant to the study.

1. SURVEY OF DEFINITIONS OF CLOUD COMPUTING

There is no one single definition of cloud computing. Experts and industry players have attempted to de ne cloud computing in various ways. Below is a survey of cloud computing definitions:

(Mell and Grance 2011) NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management e ort or service provider interaction" [2].

(Youseff et al. 2008) According to youseff "cloud computing can be considered a new computing paradigm that allows users to temporary utilize computing infrastructure over the network, supplied as a service by the cloud-provider at possibly one or more levels of abstraction" [3].

(Armbrust et al. 2009) Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds" [51].

(Buyya et al. 2008) Being grid computing scholars, Buyya et al. postulate a more technical focused approach, regarding cloud computing as a kind of parallel and distributed system, consisting of a collection of virtualized computers. This system provides resources dynamically, whereas Service Level Agreements (SLA) are negotiated between the service provider and the customer [1].

(Vaquero et al. 2009) They claim that clouds are a large pool of easily us-able and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs" [1].

(Gens 2008) The market research company IDC for example defines cloud computing very general as an emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet" [4].

(Plummer et al. 2008) Another example of a market research company's declaration is Gartners definition of cloud computing as a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies" [5].

2. SURVEY ON SECURITY TECHNIQUES

A number of studies showing the need of security in cloud computing and the various proposed techniques to enhance security [6].

(Rongxing et al. 2010) According to author it gave a new security and provenance proposal for data forensics and post examination in cloud computing. According to them their proposed system can provide the privacy and security on secret documents/files that are piled up in the cloud. It also provides secure authentication mechanism to control unauthorized user access, and provides track mechanism to resolves disputes of data. Their proposed secure provenance scheme is working on the bilinear pairing methods [7].

The strength of their work is the proposed secure provenance system and limitation of their work is that their proposed scheme is di cult to implement as it is based on complex mathematical model which is very di cult to understand.

(LaQuata Sumter et al. 2010) says: The rise in the scope of cloud computing has brought fear about the Internet Security and the threat of security in cloud computing is continuously increasing .To assure users that there information is secure, safe not accessible to unauthorized people, they have proposed the design of a system that will capture the movement and processing of the information kept on the cloud. They have identified there is need of security capture device on the cloud, which will definitely ensure users that their information is secure and safe from security threats and attacks. The proposed implementation is based on a case study and is implemented in a small cloud computing environment [8].

The advantage of their work is assurance of security to the end users of cloud. The limitation of this study is there proposed framework is not feasible for large scale cloud computing environments.

(Mladen 2008) states that Cloud computing is a recent field, which came into existence after years of research in networking and different types of computing. It uses a SOA, that minimized the information technology operating and maintenance cost for the clients, it offers greater flexibility, reduces capital costs, provides required services are along with many other characteristics. This study discusses issues associated with cloud computing along with Virtualization, Service oriented Architecture and end users. The study ranked security as the primary challenge in cloud computing. Service providers must assure the availability and reliability of services to the consumers available anytime, anywhere using internet, plus security, safety, data protection and Privacy is also exercised [9].

The benefit of this study is the identification of issues related with security and implementation. The drawback of this work is that study is based on theoretical concepts nothing practical found in this study.

(Wenchao et al. 2010) It have explored the security properties of secure data sharing among the applications hosted on clouds. They have proposed a new security platform for cloud computing, which is named as Declarative Secure Distributed Systems (DS2). In DS2, the network protocol and security policies are specified Via

Secure Network Data log (SeNDlog) a language which is normally rooted in Data log that merges declarative networking and logic-based access control specifications .They have added provenance support to the DS2 platform be-cause they believe that the distributed Provenance is significant step towards a secure cloud data management infrastructure [10].

The strength of their work is the proposed tool for data centric security which provides secure query processing, seamless integration of declarative access control policies, system analysis and forensics, efficient end-to-end verification of data. Limitation is that there work has not been validated from cloud computing vendors.

(Soren et al. 2010) It have mentioned that benefits of clouds are shadowed with the security, safety and privacy challenges and due to these challenges the adoption of cloud computing has been inhibited to a great extent. In this paper an approach has been presented for analyzing security at client side and server side. Amazons Elastic Compute Cloud (EC2) has been chosen for this assessment. The primary aim is to focus on the accessibility, vulnerabilities in the entire cloud infrastructure. They have implemented the security analysis model & weigh up it for realistic environments. Security assessment has been implemented in Python and weigh up was calculated on Amazon EC2 [11].The advantage of this work is their proposed tool which provides strong analysis of security attacks and vulnerabilities, this analysis helps vendors to improve their security policies and the drawback is that their proposed framework is specific to Amazon.

(Flavi and Roberto 2010) It stated that clouds are being targeted increasingly day by day. In this paper integrity protection problem in the clouds, sketches a novel Architecture and Transparent Cloud Protection System (TCPS) for improved security of cloud services has been discussed. To address the integrity issues, they have proposed a system, and the system is named as Transparent Cloud Protection System (TCPS) for increased security of cloud resources. According to them their proposed system, TCPS can be used to keep the transparency and virtualization [12].

The strength of their work is their proposed tool which provides improved security, transparency and intrusion detection mechanism. The limitation of their work is that they haven't validated their work nor they have deployed in professional cloud computing scenario.

(Wayne 2011) In this paper benefits of cloud computing are highlighted along with the basic security issues that are still associated with cloud services. Shaping the security of critical systems is very important. This research brings primary problems in terms of cloud security, which are alleged to cloud computing security and privacy issues. Key security issues identified and addressed in this paper are end user trust, Insider Access, Visibility, Risk Management, Client-Side Protection, Server-Side Protection, Access Control and Identity management.

The strengths of their work is identification and discussion on cloud computing security issues which educates end users about security and private risks associated with cloud services. The weakness is that they haven't proposed any tool or framework to address identified issues [13].

(Jinpeng et al 2009) said that Cloud computing poses many new security threats. In this paper they have evaluated these threats in depth from an image repository side. They have also analyzed the risks faced by the system administrators and end users of a cloud's image repository. An image management system design has been presented to address the associated risks and according to them the proposed design is implementable and proficient. The filters of the system in first step finds malicious stuff and in next step sensitive information like passwords etc are removed [14].

The strength of their work is the proposed image management system which provides image filters and scanners to detect malicious images. The weakness is that image filters are not accurate and sometimes legitimate images may also be detected as malicious image and their virus scanner is also not efficient. The scanner is not capable to detect all types of viruses, virus scanner validation is not provided by the authors.

(Miranda and Siani 2009) In this paper states that most important obstacle to wide acceptance of cloud computing services security and privacy issues in cloud computing, users have serious concerns about confidential data seepage. Privacy is not observed while critical data is being processed in the public accessible cloud. Some practical scenarios has been discussed in this paper, based on these scenarios it is recommended strongly that use of sensitive information must be minimized when data is processed on clouds and privacy to end users must be assured. To address this issue, a client based privacy manager tool has been proposed in this paper. The proposed reduces security issues, and provides added privacy features. The tool has been tested accordingly in different cloud computing environments [15].

(Dan and Anna 2010) Cloud computing provides highly scalable resources accessed via Internet. Data protection problems in the cloud computing have not been tackled currently. In the cloud, users of cloud services have serious threat of losing confidential data. To address data privacy issues of users, they have pro-posed data protection framework. According to them the proposed data protection framework addresses the challenges throughout the cloud services life cycle [16]. The advantage of this work is that their proposed tool provides Correctness, Time-Efficiency, Scalability, Security, Robustness and Reliability. The weakness is that their proposed model is not validated.

(Farhad et al. 2013) [17] This paper explain security issues in cloud computing. According to this paper, if the cloud computing services are going to be global, it should be taken care that they work in a better way everywhere like on mobile phones also as the mobile phones have applications to access everything. In MCC technology considering the hardware limitations of the device such as mobile phones, tablets and smart phones can be connected to a cloud environment and the opportunities that this environment provided benefit. To provide secure and reliable services in cloud computing environment is one of the most important issues in this technology. MCC is

emerging as a new phenomenon in the world of information technology and business is considered highly, so that the promise to deliver and provide a wide range of advantages to their followed. This paper, study only mobile technology and MCC security challenges. Its approach is only limited to keep the data on mobile devices which are related to cloud platform and hence there is a much modified work required in his approach.

(VahidAshktorab et al. 2012) This paper discussed the advantages of the cloud platform and the security risks of keeping the data on a cloud server. This paper, mainly focus over the major security threats of cloud computing systems while introducing the most suitable countermeasures for them. After that some effective countermeasures are listed and explained. The limitation of this paper is that they have just provided basic information about the security thefts of cloud server like sql injection problem, dos attacks and others. This paper does not discuss about any kind of solutions to these problems in its result approach [18].

(Mr. D. Kishore Kumar et al. 2012) This paper mainly discussed the security against the DDOS attack on the cloud server. The DDOS attack is a attack in which the server gets a number of request at the same time and due to which the server feel uncomfortable in responding to all of them simultaneously. As a result the server results into a long queue of jobs which has to be completed and this increase the waiting time of the jobs into the queue. To prevent from such kind of attack , the author has presented a third party mechanism in which the data and the query can be validated from a third party to check whether the results or the query is ne or not. It further focuses on the available security measures which can be used for the effective implementation of cloud computing [19].

(K. S. Suresh et al. 2012) This paper discusses about the basic cloud features like Iaas , Paas and SaaS and also provided information that if data is kept at any cloud sever , then it can be kept in encrypted form so that when someone even tries to access the data base , then hacker should not get the data directly . For the encryption mechanism three good encryption algorithms namely AES ,MD5 and RSA are discussed. The problem with this approach is that, this paper doesn't taking about any combinational algorithm for encryption which is quite feasible these days [20].

(Dr.A.Padmapriyaet al. 2013) This paper have discussed about cloud computing security mechanisms and presented the comparative study of several algorithms .After discussing the general problems of the cloud computing server application,introduces a heterogeneous mode algorithm which is a combination of two or more security algorithms.This paper talks about the RSA and DES algorithm and provides information that they can be combined to create a new algorithm for the encryption part [21].

(LeenaKhanna et al. 2013) This paper deals with various issues associated with Security and focus mainly on the data security and methods of providing security by data encryption. Various encryption methods of block cipher algorithms such as RSA, Blow fish are discussed for providing solutions to cloud security. This paper has provided a detailed information about the blow fish algorithm and the architecture of other algorithms also like RSA and DES algorithm. It also discusses the drawback of each algorithm and the comparative study of the results of these three algorithms [22].

(Mandeep Singh Sandhu et al. 2013) This paper uses a distributed frame-work architecture to make data secure on the cloud platform. The mail service using the SMTP services has been used to make the data content secure from the unauthorized access .It proposes a more effective and flexible distributed verification scheme to address the data storage security issue in cloud computing. As it rely on the cryptography algorithms [MD5] and [DES] to be used.

(Priyanka Gupta et al. 2013) This paper explores a new method which is a combination of role based access control with advanced encryption algorithm (a combination of RSA and two fish),signature verification to enhance security when storing text, image ,audio ,video les onto cloud server [23].

(M.Sudha et al. 2010) This paper implements a simple security framework using cryptographic algorithm. The data protection is optimized by incorporating both public and private key cryptosystems for various cloud applications. Enhanced data security has been achieved using AES, RSA and SHA algorithm with the minimal cost and e ort [24].

(Neha Jain et al. 2012) This paper presented a data security system in cloud computing using DES algorithm. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. There is no danger of any data sent within the system being intercepted, and replaced. The system with encryption is acceptably secure, but that the level of encryption has to be stepped up, as computing power increases [25].

(Rejoice Paul et al. 2012) In this paper, the various security risks of Cloud Computing are analyzed and presented. They explain different types of security issues. The limitation of this is paper is that it don't gave solutions for security threats [26].

(Ashish Sharma et al. 2013) This paper focus on the security of the multimedia data using two enhanced algorithms namely UTF8 encoding and DES. Paper also focus on keeping the data on multiple servers rather than keeping the entire structure at one server. The evaluation of decryption is based on time to decrypt the data [27].

(Ashutosh Kumar Dubey(2012) This paper proposed a trusted cloud environment which is controlled by both the client and the cloud environment admin. Their approach is mainly divided into two parts. First part is controlled by the normal user which gets permission by the cloud environment for performing operation and for loading data. Second part shows a secure trusted computing for the cloud, if the admin of the cloud want to read and update the data then it take permission from the client environment. For the above concept RSA and MD5 algorithms is used. Cloud user sends a secure key with a message digest tag for updating data. If any outsiders perform a change in the key,

the tag bit is also changed indicating the key is not secure and correct [28].

3. CRYPTOGRAPHIC ALGORITHMS

(NehaJain) presented a data security system in cloud computing using DES algorithm. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. There is no danger of any data sent within the system being intercepted, and replaced. The system with encryption is acceptably secure, but that the level of encryption has to be stepped up, as computing power increases [29].

(N.Saravanan et al.) Presented a data security system in cloud computing using RSA algorithm. They have implemented RSA algorithm in Google App engine using cloud SQL. From the results they proved that RSA gives protection for the data, which is stored in cloud. Only authorized user can retrieve the encrypted data and decrypt it. Even if anyone happens to read the data accidentally, the original meaning of the data will not be understood [30].

(M. Sudha, Dr. Bandaru Rama Krishna Rao) implement a simple Data Protection framework which performs authentication, verification and encrypted data transfer, thus maintaining data confidentiality. Programming is performed using Java platform. Cloud environment is created using wired and wireless LAN networks. An Advanced Encryption Standard security algorithm is implemented for ensuring security framework [31].

(Jian Zhang, Xuling Jin) solve the data security problem by developing a mixed DES andSHA-1 encryption system based on VC++ environment. The system on the one hand encrypt data using Triple DES and RSA and on the other hand, SHA-1 algorithm validate the integrity of data [32].

(M.Sudha, M.Monica) Implemention simple security framework using cryptographic algorithm. The data protection is optimized by incorporating both public and private key cryptosystems for various cloud applications. Enhanced data security has been achieved using AES, RSA and SHA algorithm with the minimal cost and effort [28].

(AmanjotKaur, ManishaBhardwaj) shows a concern on the security element in cloud environment. It suggests a technique to enhance the security of cloud database. This technique provides the flexible multilevel and hybrid security. It uses RSA, Triple DES and Random Number generator algorithms as an encrypting tool [33].

(G. Jai Arul Jose et al.) Propose to produce RSA public key and Private Key for public and private access to overcome the situation of data security .Binary record can be used inside get a control on node setup record to create sure cloud data flow securely. The get a control on node deliver data through protected Socket Layer after activation. Ultimately AES algorithm is use for encryption .this unique mixture makes this answer best to prevent different types of attacks. The strength of their function is solid data security against different assault. if consumers is attempt to login wrongly for often, the device automatically slowing the services and temporarily end the account services for this consumer [34].

There are many examples of homomorphic commitments. Homomorphic cryptosystems such as [35] [36] [37] [38] or Linear Encryption [39] can be seen as homomorphic commitment schemes that are perfectly binding and computationally hiding. Commitments based on homomorphic encryption can be converted into computationally binding and perfectly hiding homomorphic commitments, see for instance the mixed commitments of Damgard and Nielsen [40] and the commitment schemes used by Groth, Ostrovsky and Sahai [41], Boyen and Waters [42], Groth [43] and Groth and Sahai [43]. Even in the perfectly hiding versions of these schemes the size of a commitment is larger than the size of a message though. This length increase follows from the fact that the underlying building block is a cryptosystem whose cipher texts must be large enough to include the message.

(Girault et al. 1998) [22] Investigates notion just like in which of key insulation associated with a digital signatures while context of cards research. Nonetheless, this particular initial function doesn't have any formal unit with no proofs associated with security. E orts on key-insulated public-key encryption were thought to be simply by **(Tzeng et al. 2002)** [44] and also (Lu et al. 2002) [45](but simply next to a weak non-adaptive adversary). Key-insulated public-key encryption was first formalized, as well as strategies with extensive proofs of security given, inside the current function associated with **(Dodis et al. 2002)** [46].

(Kanika et al. 2010) In Cloud computing, we have issue like security of data, documents process, backups, Network traffic, host security .They have proposed a idea of digital signature with RSA algorithm, to encrypt the data while moving it within the network. This approach solves the dual issue of authorization and security. The strength of their work is the structure proposed to address security and privacy issue [8].

(Hatem S. Abdelkader et al. 2012) Cloud computing moves the application software and listings to the large data centers, where the administration of the data and solutions may not be fully trustworthy. This excellent feature, but, increases many new security challenges. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. Therefore their report investigates the essential issue of cloud computing data security. They presented the data security model of cloud computing on the basis of the study of the cloud architecture. They executed software to improve perform in a data security model for cloud computing. Eventually they used that software in the Amazon EC2 Micro example for evaluation process [59].

(Ayush Sharma et al. 2012) claims a fresh method called cloud networking which gives networking functionalities to cloud computing and helps flexible placement of virtual assets crossing provider borders. This enables several types of optimization, e.g., lowering latency or network load. This report presents a security architecture that allows an individual of cloud networking to de ne security requirements and enforce them in the cloud networking infrastructure [57].

(Deyan Chen et al. 2012) from the consumers perception, cloud computing security concerns are specially data

security and privacy defense problems which remain the primary inhibitor for use of cloud computing services. They provided a concise but all-round analysis on data security and privacy defense problems related with cloud computing across all phases of data life cycle. Chances are they proposed to protect data using different scheme and procedures like airavat etc. This method can reduce privacy loss without authorization in Map-Reduce computing process. The weakness is that it just a concept which depends on other scheme and procedures because of its implementation [56] [6].

Feasibility of structure-preserving signatures on group elements was first shown by Groth [43], who presents a construction based on the decision linear assumption (DLIN) [47]. While it is remarkable that the security can be based on a simple standard assumption, the scheme is not practical as signatures consist of hundreds of thousands of group elements. Based on the q-Hidden LRSW assumption, Green and Hohenberger [48] presented an efficient scheme that provides security against random-message attacks. An extension to chosen message security is not known.

(Cathalo, Libert and Yung 2009) gave a practical scheme based on a combination of the hidden strong Di e-Hellman assumption, the flexible Diffie-Hellman assumption, and the DLIN assumption. It was the first structure preserving sig-nature scheme to sign single group elements. However, it cannot sign its own verification keys and signatures on vectors grow linearly in their length [49].

III. GAP OF SURVEY

The literature survey presented in the previous chapter found gaps in cloud computing security.

1. The use of group based signature in PAVD security system has been ignored.
2. The majority of secured data storage has neglected. The login overhead has been neglected.
3. The member freedoms to upload and download data have algorithms ignored in existing research.

IV. OBJECTIVES

To evaluate the upload and download time.

(a) Amazon cloud Drive
(b) Box
(c) Drop box
(d) Google Drive
(e) Sky Drive

2. To improve the PAVD security system by using the group based digital sig-nature in cloud environment.
3. The group based signature also provide freedom to group member to send and receive data directly which will reduced the authentication overhead.
4. To draw comparison between PAVD security system and Proposed group based digital signature PAVD system based upon the following parameters:

(a) Download time
(b) Upload time
(c) Overheads
(d) Response Time
(e) Execution Time

V. CONCLUSION AND FUTURE SCOPE

This paper has offered Cloud Computing PAVD security system A Survey. Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services and from huge number of applications, number of systems for secure data transmission have been proposed in recent years. In this work, we had ex-tended one of the existing technique called PAVD to group signature based PAVD. A protocol in which the group digital signature is generated using the strong RSA algorithm. In this method the freedom of the member is sacrificed by sending the message through the group manager.

In this paper the survey has shown various limitation in the some well-known cloud computing security techniques. In this work, we conduct a study on the recent cloud security issues and the state-of-the-art security results. We classify 28 cloud security issues such as firewall misconfigurations, malicious insiders, tampered binaries, multi-tenancy, side channels, weak browser security, and mobility. Then, we categorize these issues into five security categories, namely: security standards, network, access, cloud infrastructure, and data. We also identify nine attack classes that target the clouds and present variable incidents of each attack such phishing, fate sharing, botnet, and malware injection.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, 2008.

[2] P. Mell and T. Grance, “The nist definition of cloud computing," 2011.

[3] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youse , and D. Zagorodnov, “The eucalyptus open-source cloud-computing system," in Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on. IEEE, 2009, pp. 124-131.

[4] F. Gens, “Defining cloud services and cloud computing," IDC exchange, vol. 23, 2008.

[5] D. C. Plummer, T. J. Bittman, T. Austin, D. W. Cearley, and D. M. Smith, “Cloud computing: Defining and describing an emerging phenomenon," Gartner, June, vol. 17, 2008.

[6] F. B. Shaikh and S. Haider, “Security threats in cloud computing," in Inter-net technology and secured transactions (ICITST), 2011 international conference for. IEEE, 2011, pp. 214-219.

[7] R. Lu, X. Lin, X. Liang, and X. S. Shen, “Secure provenance: the essential of bread and butter of data forensics in cloud computing," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010, pp. 282-292.

[8] R. L. Sumter and C. Computing, “Security risk classification, acmse 2010."

[9] M. A Vouk, “Cloud computing-issues, research and implementations," CIT. Journal of Computing and Information Technology, vol. 16, no. 4, pp. 235- 246, 2008.

[10] W. Zhou, M. Sherr, W. R. Marczak, Z. Zhang, T. Tao, B. T. Loo, and I. Lee, “Towards a data-centric view of cloud security," in Proceedings of the second international workshop on Cloud data management. ACM, 2010, pp. 25-32.

[11] S. Bleikertz, M. Schunter, C. W. Probst, D. Pendarakis, and K. Eriksson, “Security audits of multi-tier virtual infrastructures in public infrastructure clouds," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010, pp. 93-102.

[12] F. Lombardi and R. Di Pietro, “Transparent security for cloud," in Proceedings of the 2010 ACM symposium on applied computing. ACM, 2010, pp. 414-415.

[13] W. Jansen et al., “Cloud hooks: Security and privacy issues in cloud computing," in System Sciences (HICSS), 2011 44th Hawaii International Conference on. IEEE, 2011, pp. 1-10.
[14] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, “Managing security of virtual machine images in a cloud environment," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 91-96.
[15] M. Mowbray and S. Pearson, \A client-based privacy manager for cloud computing," in Proceedings of the fourth international ICST conference on communication system software and middle ware. ACM, 2009, p. 5.
[16] D. Lin and A. Squicciarini, “Data protection models for service provisioning in the cloud," in Proceedings of the 15th ACM symposium on Access control models and technologies. ACM, 2010, pp. 183-192.
[17] F. S. Gharehchopogh, R. Rezaei, and I. Maleki, “Mobile cloud computing: Security challenges for threats reduction," International Journal of Scienti c & Engineering Research, vol. 4, no. 3, pp. 8-14, 2013.
[18] V. Ashktorab and S. R. Taghizadeh, “Security threats and countermeasures in cloud computing," International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 1, no. 2, pp. 234-245, 2012.
[19] D. K. Kumar, D. G. V. Rao, and D. G. S. Rao, “Cloud computing: An analysis of its challenges & security issues," International Journal of Computer Science and Network (IJCSN) Volume, vol. 1, 2012.
[20] K. Suresh and K. Prasad, “Security issues and security algorithms in cloud computing," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 10, 2012.
[21] D. A. Padmapriya and P. Subhasri, “Cloud computing: Security challenges & encryption practices," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 3, pp. 255-259, 2013.
[22] L. Khanna, “Prof. anant jaiswal cloud computing: Security issues and description of encryption based algorithms to overcome them," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 3, pp. 279-283, 2013.
[23] P. Gupta and A. K. Brar, “An enhanced security technique for storage of multimedia content over cloud server," International Journal of Engineering Research and Applications (IJERA), vol. 3, no. 4, pp. 2273-2277, 2013.
[24] M. Sudha, D. B. R. K. Rao, and M. Monica, “A comprehensive approach to ensure secure data communication in cloud environment," International Journal of Computer Applications (0975-8887) Volume, 2010.
[25] N. Jain and G. Kaur, “Implementing des algorithm in cloud for data security," VSRD International Journal of Computer Science & Information Technology, vol. 2, no. 4, pp. 316-321, 2012.
[26] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, “Security issues for cloud computing," Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies, p. 150, 2012.
[27] A. Sharma and V. Gupta, “Multimedia data security enhancing des &utf8 parameterizing time constraint," International Journal of Computer Science and Communication Engineering, vol. 2, no. 4, pp. 47-51, 2013.
[28] M. Sudha, “Enhanced security framework to ensure data security in cloud computing using cryptography," Advances in Computer Science and its Applications, vol. 1, no. 1, pp. 32-37, 2012.
[29] S. Selvi, S. S. Vivek, C. P. Rangan, and N. Jain, “Cryptanalysis of li et al.'s identity-based threshold signcryption scheme," in Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference on, vol. 2. IEEE, 2008, pp. 127-132.
[30] T. J. Neela and N. Saravanan, “Privacy preserving approaches in cloud: a survey," Indian Journal of Science and Technology, vol. 6, no. 5, pp. 4531- 4535, 2013.
[31] K. V. Kumar, D. N. C. S. Reddy, and B. S. Reddy, “Preserving data privacy, security models and cryptographic algorithms in cloud computing," Inter-national Journal of Computer Engineering and Applications, vol. 7, no. 1, 2015.
[32] J. Zhang and X. Jin, “Encryption system design based on des and sha-1," in 2012 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science. IEEE, 2012, pp. 317-320.
[33] A. Kaur and M. Bhardwaj, \Hybrid encryption for cloud database security, "International Journal of Engineering Science & Advanced Technology, vol. 2, no. 3, pp. 737-741, 2012.
[34] G. J. A. Jose, C. Sajeev, and C. Suyambulingom, “Implementation of data security in cloud computing," International Journal of P2P Network Trends and Technology, vol. 1, no. 1, pp. 18-22, 2011.
[35] T. ElGamal, “On computing logarithms over finite fields," in Advances in CryptologyCRYPTO85 Proceedings. Springer, 1986, pp. 396-402.
[36] T. Okamoto and S. Uchiyama, “A new public-key cryptosystem as secure as factoring," in Advances in CryptologyEUROCRYPT'98. Springer, 1998’p.p 308-318.
[37] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes," in Advances in cryptologyEUROCRYPT99. Springer, 1999, pp. 223{238.
[38] D. Boneh, E.-J. Goh, and K. Nissim, “Evaluating 2-dnf formulas on cipher-texts," in Theory of cryptography. Springer, 2005, pp. 325-341.
[39] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586-615, 2003.
[40] I. Damgard and J. B. Nielsen, Perfect hiding and perfect binding universally composable commitment schemes with constant expansion factor. Springer, 2002.
[41] J. Groth, R. Ostrovsky, and A. Sahai, “Non-interactive zaps and new techniques for nizk," in Advances in Cryptology-CRYPTO 2006. Springer, 2006, pp. 97-111.
[42] X. Boyen and B. Waters, “Compact group signatures without random oracles," in Advances in cryptology-EUROCRYPT 2006. Springer, 2006, pp. 427-444.
[43] J. Groth, “Simulation-sound nizk proofs for a practical language and constant size group signatures," in Advances in Cryptology-ASIACRYPT 2006. Springer, 2006, pp. 444-459.
[44] W.-G. Tzeng and Z.-J. Tzeng, “Robust key-evolving public key encryption schemes," in Information and Communications Security. Springer, 2002, pp. 61-72.
[45] L. Cheng-Fen and S. W. Shieh, “Secure key-evolving protocols for discrete logarithm schemes," in Topics in CryptologyCT-RSA 2002. Springer, 2002, pp. 300-309.
[46] Y. Dodis, J. Katz, S. Xu, and M. Yung, “Key-insulated public key cryptosystems," in Advances in CryptologyEUROCRYPT 2002. Springer, 2002, pp. 65-82.
[47] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures," in Advances in Cryptology{CRYPTO 2004. Springer, 2004, pp. 41-55.
[48] M. Green and S. Hohenberger, “Universally composable adaptive oblivious transfer," in Advances in Cryptology-ASIACRYPT 2008. Springer, 2008, pp. 179-197.
[49] J. Cathalo, B. Libert, and M. Yung, “Group encryption: Non-interactive realization in the standard model," in Advances in Cryptology-ASIACRYPT 2009. Springer, 2009, pp. 179-196.
[50] Y. Pawar, P. Rewagad, and N. Lodha, “Comparative analysis of pavd security system with security mechanism of different cloud storage services," in Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, April 2014, pp. 611-614.
[51] A. Fox, R. Gri th, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, ”Above the clouds: A berkeley view of cloud computing," Dept. Electrical Eng. and Computer Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, p. 13, 2009.