IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-3 E-ISSN: 2347-2693

A Secure Cloud Environment

P. Indu[1*], S. Bhattachryya[2]

[1*] School of Computers ,Inspiria Knowledge Campus, Maulana Abul Kalam Azad University of Technology, Siliguri, India
[2] Department of Computer Science and Engineering, University Institute of Technology, The University of Burdwan, Burdwan, India

[*]*Corresponding Author: pabakindu@yahoo.co.in*

Available online at: www.ijcseonline.org

Received: 17/Feb//2018, Revised: 25/Feb2018, Accepted: 11/Mar/2018, Published: 30/Mar/2018

Abstract— *Cloud Computing has been a one-key, cost-effective solution for many small I.T industries from past few decades in terms of storage, computation etc. It provides different kinds of services and infrastructural support. While cloud makes these services more appealing, it also brings some critical security threats to the cloud service users as well as to the cloud service providers. In this paper authors have tried to identify major security threats faced by different models of cloud in current day scenario and providing with some suitable solutions addressing those threats like One-time password, Homomorphic encryption technique, Access control and Data Recovery mechanism in different cloud deployment models.*

Keywords— Third Party Auditor, One-time password, Homomorphic encryption technique, Access control and Data Recovery mechanism, Cloud Service User (CSU), Cloud Service Provider(CSP).

I. INTRODUCTION

NIST(National Institute of Standards and Technology) had described cloud computing as "the 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 or service provider interaction"[1] in other words it is the cost effective and zero tolerance model which delivers almost everything as a service for different start-up IT industries.

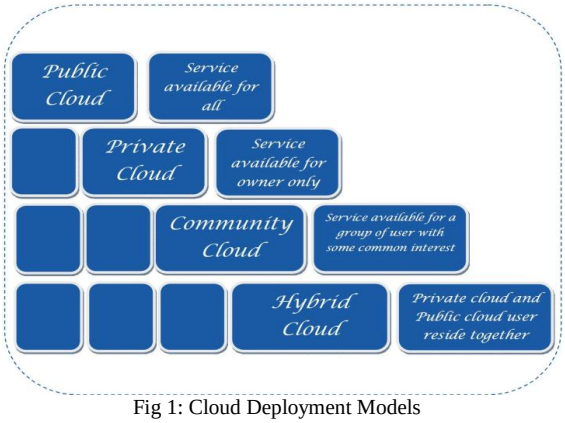

Fig 1: Cloud Deployment Models

Depending on the different types of services and the accessing types, the cloud can be broadly categorized in four deployment models [2] and three service models [2] as

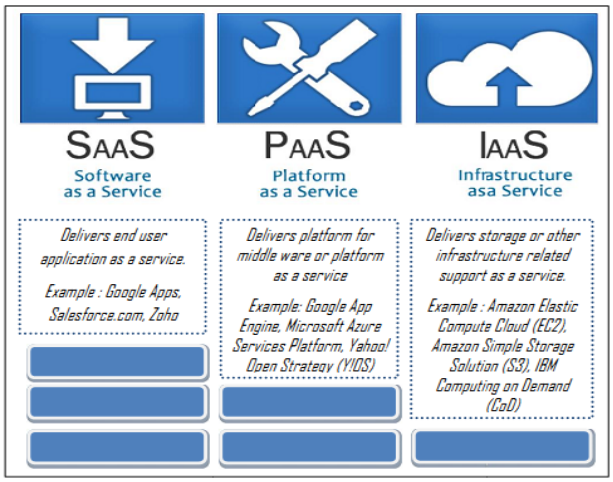

Figure 2: Cloud Service Models

shown in figure 1 and figure 2 respectively.

A. The Cloud Service Models:

Software-as-a-Service (SaaS) : This model [2] offers on demand applications or software as a service to the users. All the cloud service users (CSU) share a single instance of the software service. Users need not to spend any extra money to maintain the software. User pays according to the usage. The entire software service is maintained by the cloud service providers (CSP), like maintaining future version of the

software, license agreement, patches etc. Some examples of SaaS model are described below

- *Google Apps* provides web-based office tools; such as e-mail, calendar and document management tools etc.
- *Salesforce.com* provides customer relationship management (CRM) applications.
- *Zoho* provides web-based large suite of applications, mostly for enterprise use.

Platform as a Service (PaaS): This paradigm of cloud [2] supports the development of applications by providing a higher level application development platform. Users develop their suitable and useful applications in this development arena. Below there are some examples of PaaS providers.

- *Akamai Edge Platform* provides large distributed computing platform for web application deployment (focus on analysis and monitoring of resources).
- *Force.com* provides a platform to build and run applications and components bought from App Exchange or custom applications.
- Google App Engine:
- This is an application development platform and these applications run on Google's infrastructure.
- *Microsoft Azure Services* platform provides windows Azure based on-demand compute and storage services along with a development platform.
- Yahoo! Open Strategy (Y!OS):
- The platform is used to develop web based applications.

Infrastructure as a Service (IaaS): This is basically an infrastructural support [2] based model. It provides storage and computational support to the client over the network. Various types of infrastructural equipments are shared over the network, like Servers, storage systems, networking equipment etc. Examples of IaaS Providers are discussed below.

- *Amazon Elastic Compute Cloud* (EC2) provides a special virtual machine (AMI) [3] that can be deployed and run on the EC2 infrastructure deployed.
- *Amazon Simple Storage Solution* (S3) provider provides users access to dynamically scalable storage resources.
- *IBM Computing on Demand* (CoD) provider provides users' access to highly configurable servers, plus value-added services such as data storage.

B. The Cloud Deployment Models

Cloud deployment models define the benchmark for accessing, protecting data and applications. Depending on these benchmarks cloud is classified into four types as described below.

- ***Public Cloud:*** This Cloud model [2] is made available to all the CSU and is owned by CSPs like, Amazon, Google and Microsoft Azure. In this model CSU refers general public or a large industry.
- ***Private Cloud:*** This Cloud model [2] is entirely accessed by a single organization. It may be managed by that company or a third party. This third party may be part of that organization or it can be a different organization. Like Attenda RTI.
- ***Community Cloud:*** This Cloud model [2] is shared by several CSUs from different backgrounds (like organizational support for a specific community) with similar interests. Like G-Cloud of UK.
- ***Hybrid Cloud:*** This cloud paradigm [2] is a composition of two or more previous cloud models, which has some distinct properties, but they are bound together by some standard rules that maintains their distinctness and data-application portability. This is the most popular cloud delivery model.

Section I contains the Introduction of the basics of cloud computing, where as Section II tells us about some of the existing security issues followed by the security solutions proposed by other researchers, are discussed in Section III. The Section IV describes about the mathematical formulation for the proposed method. Section V draws the solution methodology followed by the algorithms of the proposed method. Section V succeeding with Section VI and VII draws the comparison between the proposed methods and some existing approaches followed by the conclusions at the end.

II. SOME EXISTING SECURITY ISSUES

Success of cloud lies in the term "multi-tenancy". This is curse in bliss for the cloud, because, multiple organizations share the same infrastructure provided by a different organization. As a result protection of the outsourced data lies entirely under the management of a different organization. This is the one of major reasons behind data vulnerability in the cloud.

In the year 2008 and 2009 International Data Corporation (IDC) [4] had conducted a survey on Cloud Services, illustrated in Figure 3. This shows the rapid increasing requirement of strong security mechanisms for smooth and uninterrupted execution of cloud.

In this section authors have identified some existing security issues as guided by the International Standards Organization (ISO) 7498-2 [5].Figure 4 describes the different security threats faced by different types of cloud service models [6]. In Fig 4 "Y" means mandatory requirement and "N" means optional requirements.

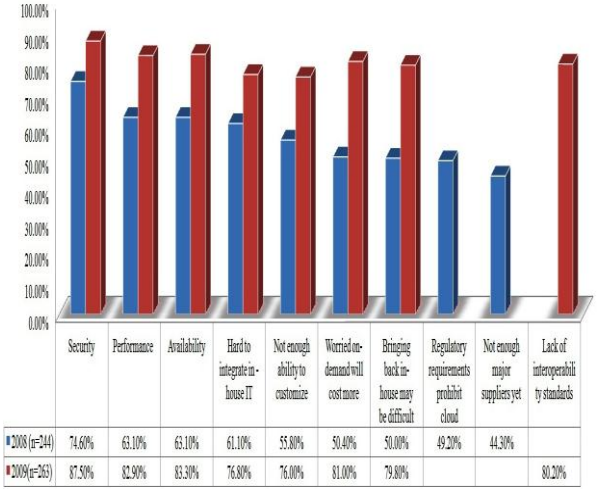

Figure 3: Cloud challenges/issues survey 2008 and 2009 (in courtesy International Data Corporation (IDC) [4]

The security requirements are described below in the context of cloud data security.

- ***Identification & Authentication***

This phenomenon [5] ensures the access control of the cloud by authenticating CSUs. This authentication can be done using User-id, password, MAC address, IP address, firewalls or any other mechanism.

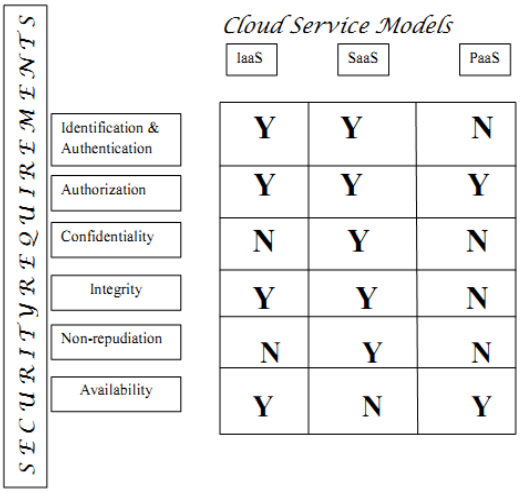

Figure 4: Cloud Computing Security Requirements

- ***Authorization***

It deals [5] with the referential integrity. It controls the process flow or service flow in a cloud. This security requirement is basically maintained by the cloud service providers (CSP).

- **Confidentiality**

Confidentiality [5] is a vital phenomenon to maintain the multi tenancy as well as the security of a cloud. It ensures unauthorized users are prevented from accessing private information. Virtual accessing of data allows maintaining the confidentiality to some extent.

- ***Integrity***

The integrity [5] ensures the protection for components of cloud system from intentional and unauthorized harm or changes. Integrity requirements can be classified in data integrity, hardware integrity and software integrity. In many of the cases it is achieved by service level agreements [21].

- ***Non-repudiation***

Non-repudiation [5] provides protection against repudiation of communication between two communicating parties. Repudiating interactions are often counteracted by some authorizing protocols. These techniques are therefore often used for access control. Amongst others, the exchange of public keys, certificates or digital signatures are included.

- ***Availability***

Success of cloud lies in the types of services it provides[5]. So for a cloud, availability of the services and data are key factors. This is can be dealt with, some service level agreements (SLA) between CSP and CSU but now a day's many researchers have found only SLA is not enough to maintain availability. So they have developed some

mechanism to maintain the availability of the services as well as data.

III. SOME EXISTING SECURITY SOLUTIONS

Md.Tanzim Khorshed et al. [7] proposed an attack detection mechanism with the help of machine learning techniques. The proposed model detects and identifies the pattern of the attack and both the CSU and CSP are informed about the attack. Afterwards necessary attack prevention steps are taken. Figure 5 illustrates the method.

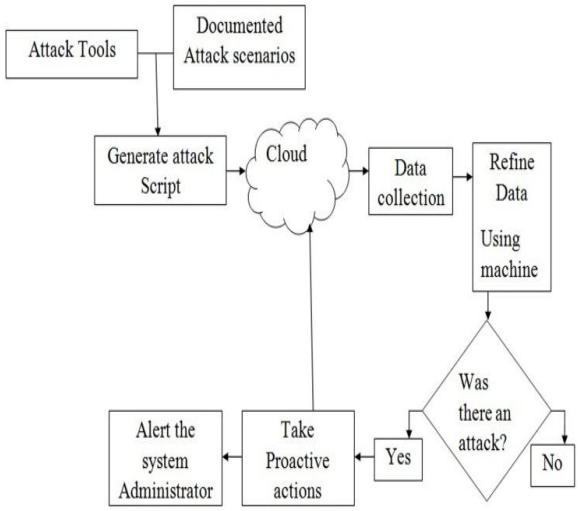

Figure 5: Attack detection and proactive resolution
(In courtesy Md.TanzimKhorshed et al. [7])

A. *IaaS service model*

- Cong Wang et al. [8] used an external auditor which audits the user outsourced data over the cloud environment on behalf of CSU and returns some data consistency parameters. This model also supports batch auditing. Third Party Auditor (TPA) also supports auditing for different users at any instance of time.

- In Xiaojun Yu et al.'s model [9] authors have described different phases of the data process. Among these phases only data storing phase is considered for the security protection. The CSU uses asymmetric key cryptography before uploading the data into the cloud. Figure 6 shows the working principle of the model.

- Uma Somani et al. [10] have derived Digital Signature from some mathematical formulas. This Digital Signature is embedded into the data for authentication purpose. The authentication mechanism is guided by "hashing algorithm" which converts the data into the message digest. RSA is used for secure transmission of data over the network

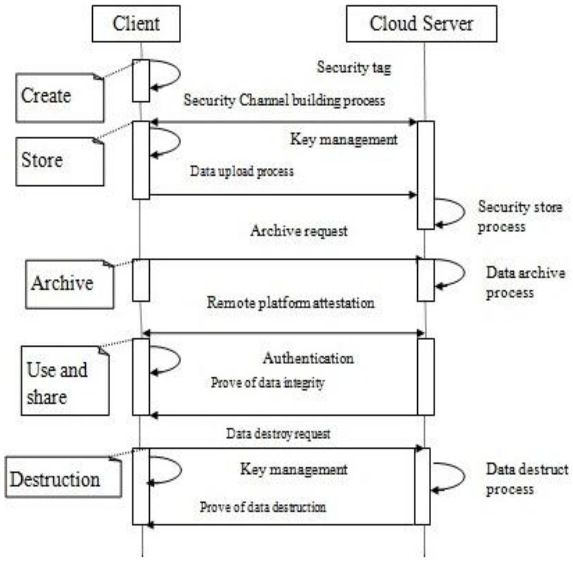

Figure 6 : Data security process in data life cycle
(in courtesy Xiaojun Yu et al. [9])

- P. Syam Kumar et al. [11] have designed a model which uses an effective and flexible distribution to achieve a successful verification protocol. This model incorporates pre-computed erasure code to the data to achieve availability and reliability. Some utilization tokens are generated by pre-computation of erasure data over the sobel sequence to maintain data integrity. For better availability the entire data is distributed among several sites. If some sites fail to respond the system can regenerate the entire data from the remaining sites. This phenomenon makes the system fault tolerant.

B. *SaaS and PaaS service models*

In Xi Cao et al.'s [12] proposed model has two way security protocols.

Step 1: This part requires CSU's digital signature and this digital signature is provided to the CSP to launch the cloud services.

Step 2: Software provider counts the number of deployed services by obtaining the digital signature from the CSP.

Figure 7 describes the working principle of the model.

Junli Zhu et al. [13] have designed a security system over the UCON model. Subject, subject attributes, object, object attributes, rights, authorization, obligations and conditions, these are eight components of the system. Figure 8 shows the uses of UCON models in a SaaS environment.

Kiyoshi Nishikawa et al.'s [14] model achieves security through information gateway. Every Cloud Service is enabled using this gateway. This gateway maintains the confidentiality of the system operating location which is changed and controlled dynamically.

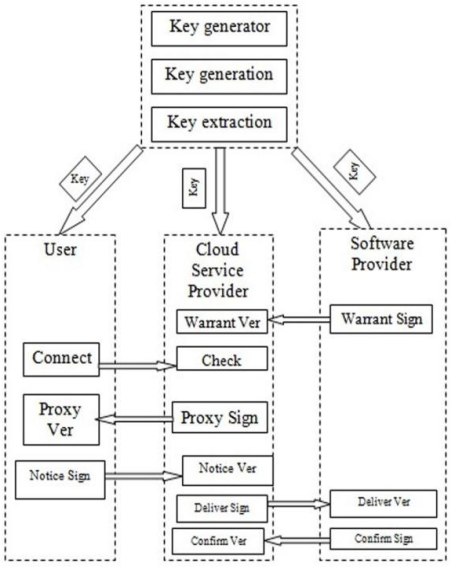

Figure 7: Id-based proxy Signature Model for cloud service in Saas(In courtesy Xi Cao et al. [12])

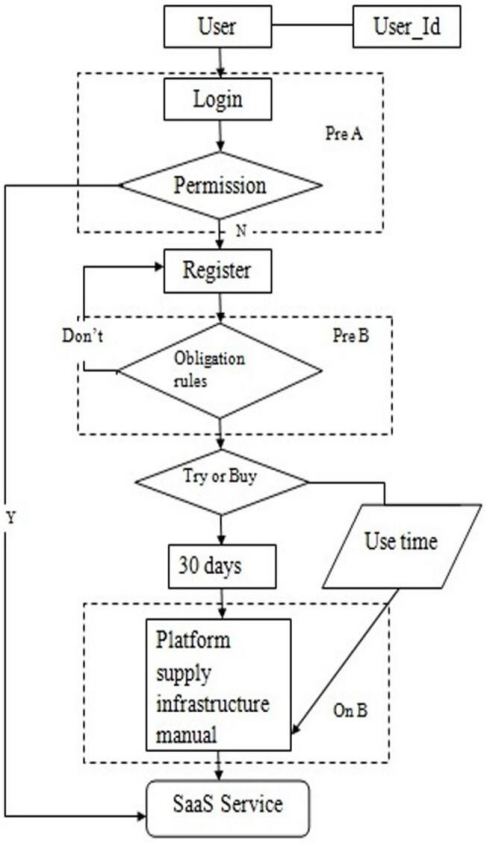

Figure 8: UCON Combined with SaaS Access Flow (In courtesy Junli Zhu et al. [13])

C. Some more security approaches

- Jinpeng Wei et al.[15] designed a security model through management of virtual machine in a cloud environment.

Disadvantage: The image filters cannot be accurate so that system does not eliminate the risk entity.

- Miranda Mowbray et al. [16] Proposes a client based privacy manager for reducing the misuse risk of the CSU's private data and also assists the CSP to ensure the privacy law.

Disadvantage: The CSPs have to provide honest services with the privacy manner otherwise it's not an effective one.

- Flavio Lombardi et al. [17] proposed a Transport Cloud Protection System (TCPS) based model. The TCPS acts as a middleware whose core is situated between kernel and Virtualization layer.

Advantage: Effective in detecting most kind of attacks.

Disadvantage: This model is not generalized. It cannot be implemented in all scenarios.

- F. A. Alvi et al. [18] have designed a security access control service (SACS) model for better security of cloud data.

Disadvantage: Unidentified killer application cannot be avoided.

- Shantanu Pal et al. [19] designed a trust based agent model. This model provides security at service provider level and user level in a cloud environment.

Disadvantage: It cannot handle many security threats.

IV. MATHEMATICAL REPRESENTATION OF THE PROPOSED METHOD

The authors have identified that SaaS, PaaS and IaaS have separate security issues and they also require separate security solutions. These security solutions are represented in terms of mathematical formulation.

A. For SaaS and PaaS cloud environment

The authors have introduced a One Time Password generation mechanism to achieve security. Here 'κ' and 'β' are two arbitrary computed real number values computed randomly and assigned to 'x' and 'y'.

$$x = \kappa, where \kappa \in \Re$$

$$y = \beta, where \beta \in \Re$$

'e' is the key parameter for generating essential factor, ,of one time password(OTP).

n is the length of the OTP

$$\phi_1 = celling\left(\left|\log_2\left(e^x \otimes y^x\right)\right|\right)\ldots(1)$$

x, y are computed 'n' times(i.e. till the number reaches to the length of OTP)and depending on equation 1 is generated.

$$\phi = \sum(\phi_1, \phi_2, \cdots, \phi_n)\ldots(2)$$

B. For IaaS cloud environment

For IaaS environment security a strong encryption mechanism is required. To provide security as well as data integrity authors have implemented a unique homomorphic encryption [20] technique.

ω is the user' s personal encryption key of length 'n'.

χ is user data.

ξ is the derived encryption key.

"i" is an arbitrary suffix from 1 to n.

$$\delta = \sum_{i=1}^{n} \omega_i \ldots(3)$$

In equation 3 ASCII of the each character of the user's personal key are added with each other.

$$\xi = e^{\delta} \ldots(4)$$

In equation 4 exponential of equation 3 is computed to provide an extra layer of security.

After applying equation 3 and 4, ψ is generated, this is the encrypted version of the out sourced data.

$$\psi = \chi \otimes \xi \ldots(5)$$

Now to audit the integrity of data user enters the audit key, θ of length 'n'.

$$\gamma = \sqrt{\sum_{i=1}^{n} \theta_i} \ldots(6)$$

Similar to equation 3 "γ" is computed through equation 6.

After applying the logarithmic function shown in equation 7 "τ" is computed.

$$\tau = celling\left|\log_e \gamma\right|\ldots(7)$$

$$(\rho, \sigma) = \psi \otimes \tau \ldots(8)$$

TPA uses equation 6,7 and 8 and generates some security parameters 'ρ', 'σ' as a proof of data integrity. User might store these parameters for future reference.

For data recovery CSP transmits entire data to a separate location where access of user is fully restricted.

For decrypting data 'δ', 'ξ' are regenerated from equation 3 and 4. And using equation 9 original data is retrieved.

$$\chi = \psi / \xi \ldots(9)$$

C. Homomorphic Encryption

This kind of encryption technique is used to perform some operation on the encrypted data without having access to the actual data or the private key [20]. This operation returns the same value as it would have been if the operation is done on the actual data. So by using this technique TPA is unable to access the actual data but it returns the same parameter values. So this reduces the vulnerability of data [21] and ensures the integrity of the out-sourced data. Here is a very simple example of homomorphic encryption scheme in terms of cloud computing:

- Organization ASD has a vital organizational data (VOD) that consists of the numbers 25 and 100. To encrypt the data set, ASD multiplies each element in the set by 4, creating a new set of data whose values are 100 and 400.Now this becomes the new VOD.
- Organization ASD outsources the encrypted VOD to the cloud for secure storage. After some time some business organization contacts organization ASD and requests the sum of VOD elements.
- Organization ASD asks the CSP to perform the operation. The CSP, who only has access to the encrypted version of the data, finds the sum of 100 + 400 and returns the answer 500.
- Organization ASD decrypts the cloud provider's reply and provides the organization with the decrypted answer, (500/4) =125.

V. SOLUTION METHODOLOGY OF THE PROPOSED MODEL

Figure 9 shows the solution window for preserving access control and confidentiality using username and password and segregating users into ordinary user and organizational user.

Figure 10 shows the users' access restriction window for PaaS and SaaS services and fig 11 shows the users with full access over the PaaS and SaaS services.

Figure 12(a) and Figure 12(b) shows the deployment window of the SaaS and PaaS service models. Figure 13 shows the deployment window of IaaS service model.

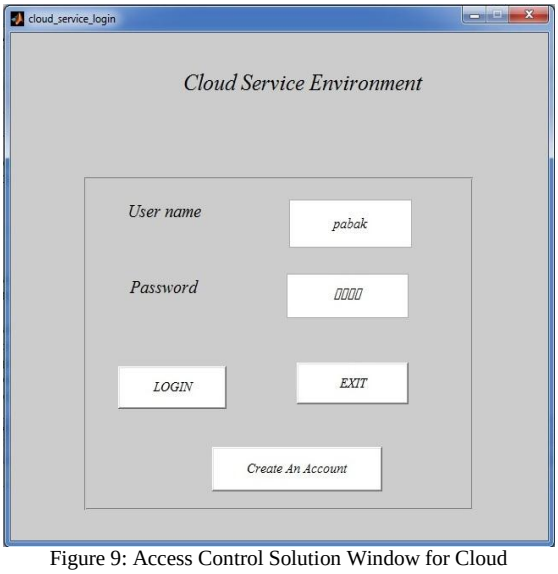

Figure 9: Access Control Solution Window for Cloud

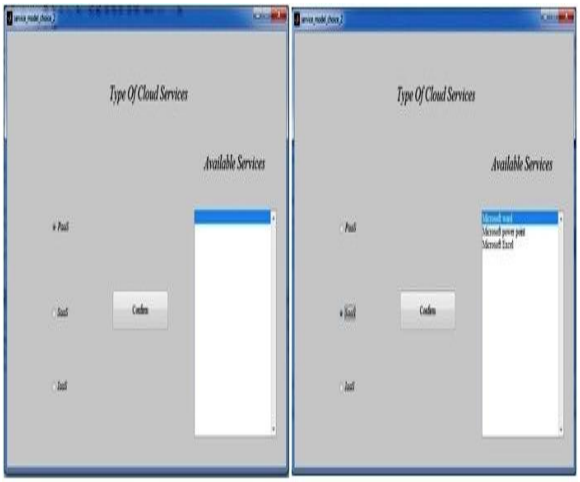

Figure 10: Users access restriction window for PaaS and SaaS services

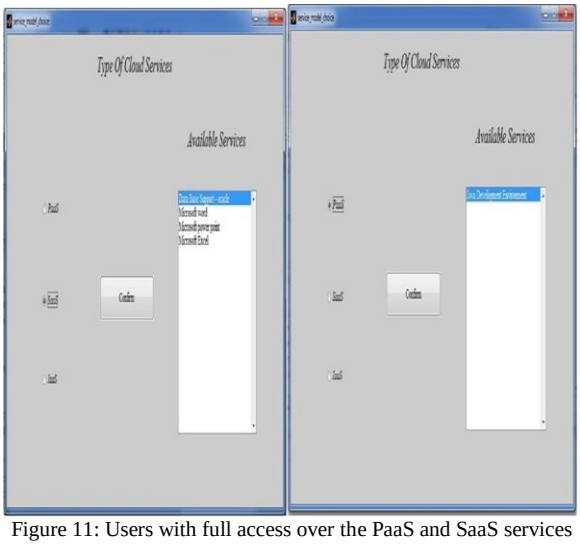

Figure 11: Users with full access over the PaaS and SaaS services

Figure 12(a): The deployment window of SaaS service model.

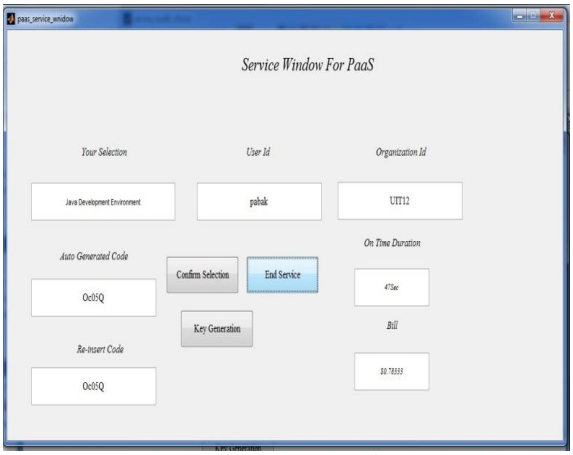

Figure 12(b): The deployment window of PaaS service model

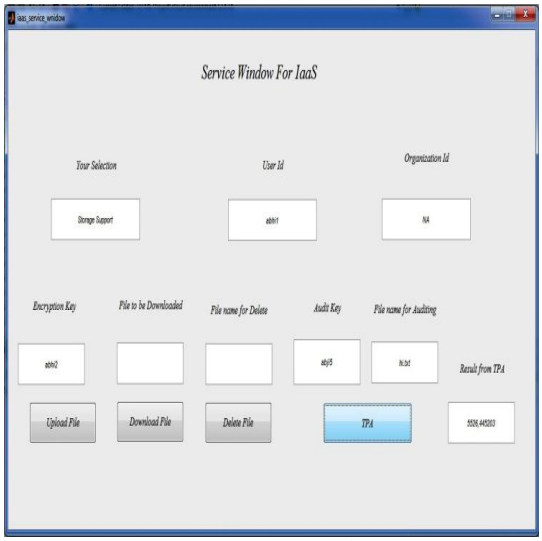

Figure 13: The deployment window of IaaS service model

A. Algorithm of the Proposed Model

- ***For SaaS and PaaS Cloud Service Models***

Let "X" be a user, "Y" be an System generated One Time Password (OTP) for "X" and "Pass" is a Onetime password (OTP) entered by the User. "X" is distributed among two groups one is "organizational group" and one is "non-organizational group", "Full-Services" are available only to the organizational group and "Restricted Services" are available for "Non-organizational groups". "R",is computed to ensure user access.

Step 1: Services are provided to "X" according to the type of User.
Step 2: X Choose the service
Step 3: Y is generated and send to user.
Step 4: IF (Y==Pass)
Step 5: Start Service.
Step 6: End Service According to X.
Step 7: Generate R.
Step 8: End of IF
Step 9: End
Figure 14 shows the working principal of the model.

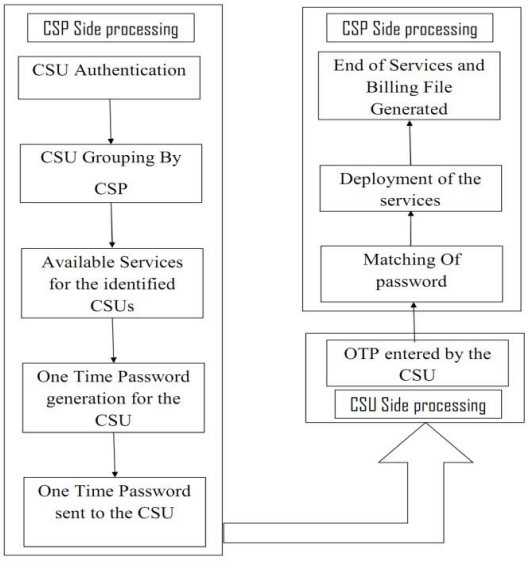

Figure 14: Block diagram of SaaS and PaaS security models

- ***Algorithm for OTP***

The generation of One Time Password depend upon Equation no 2.

Let "ϕ" is a ASCII value. "L" is the length of the One Time Password. "Final" is the ultimate generated one time password. "C1" is characterization of the " ". "i" and "C" are the arbitrary variables where "i" is initialized to 1 and "C" to NULL.

Step 1: Generate ϕ .
Step 2: i=i+1
Step 3: C1= characterize "ϕ"
Step 4: C=merge (C,C1)
Step 5: repeat Step 1 to Step 4 until (i== L)
Step 6: Final = C
Step 7: Send 'Final' to the use for deployment of service.

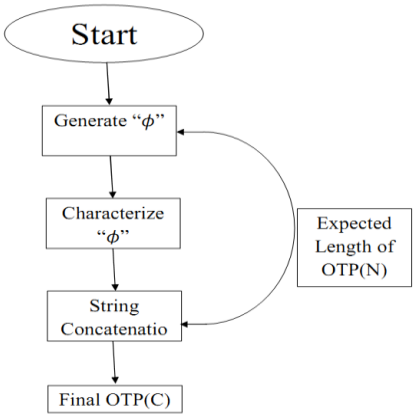

Figure 15: Shows the OTP generation block diagram.

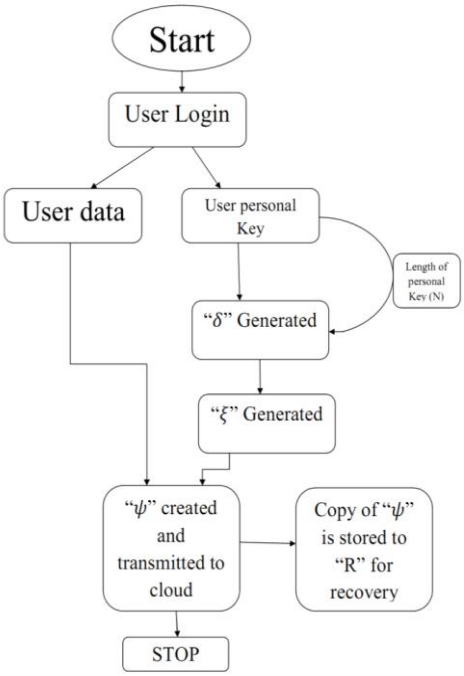

Figure 16: The working principal for out sourcing data to the cloud

Figure 15 shows the OTP generation block diagram.

- ***For IaaS Cloud Service Models***
- ***Algorithm for Encryption***

Let 'x' is the organizational private data to be outsourced. 'y' is the user key for encryption. Length of 'y' is 'N'. 'R' is a recovery file situated in a remote location. Neither CSU nor CSP have direct access to R. C is an arbitrary variable which contains the value of 'x' temporarily. The

encryption is done according to equation 3, 4, 5. 'i' is an arbitrary variable.

Step 1: C := x
Step 2: for i=1:N
Step 3: generate "δ"
Step 4: End of loop
Step 5: generate "ξ"from "δ"
Step 6: generate "ψ"from "ξ" and 'x'
Step 7: R: = "ψ"
Step 8: END

Working principal for out sourcing data to the cloud had been shown in Figure 16.

- ***Algorithm for Auditing***

Let "ψ" be the data to be audited. 'y' is the auditing key. R is the remote location which is not accessible by the CSU and CSP, contains a copy of "ψ". 'N' is the length of 'y'. 's' is the status of the availability of "ψ". 's=1' denotes "ψ"is found and's=0' denotes "ψ" is not found. ρ and σ are two parameters which are generated after a successful auditing. 'i' is an arbitrary variable. Equation 6,7 and 8 are used to generate ρ and σ.

Step 1: user requests for TPA and enters the key 'y'
Step 2: IF s==1
Then
Step 3: for i=1: N
Step 4: γ is computed
Step 5: End Loop
Step 6: τ is computed from equation 7depending on γ.
Step 7: ρ and σ are computed from ψ and τ.
Step 8: if s==0
Step 9: ψ : =R
Step 10: repeat step 3 to step 7
Step 11: End

Figure 17 shows the Auditing Mechanism for the outsourced data.

- ***Algorithm for Retrieving Data***

Let ψ be the outsourced data and 'x' is the original data. 'y' is the encryption key. R is the remote location which is not accessible by the CSU and CSP, contains a copy of ψ. 'N' is the length of 'y'. 's' is the status of the availability of ψ. 's=1' denotes is found and's=0' denotes ψ is not found. 'i' is an arbitrary variable. Equation 3,4 and 9 are used to generate 'x'.

Step 1: user requests for data and enters the key 'y'
Step 2: IF s==1
Then
Step 3: for i=1:N
Step 4: generate "δ"
Step 5: End of loop
Step 6: generate "ξ" from "δ"
Step 7: generate 'x' from "ξ"and "ψ"
Step 8: if s==0
Step 9: ψ :=R
Step 10: repeat step 3 to step 7
Step 11: End

Figure 18 shows the block diagram of the retrieving outsourced data form cloud.

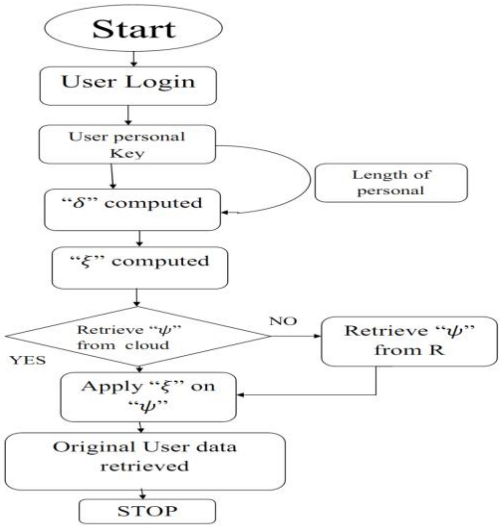

Figure 17: The Auditing Mechanism for the outsourced data.

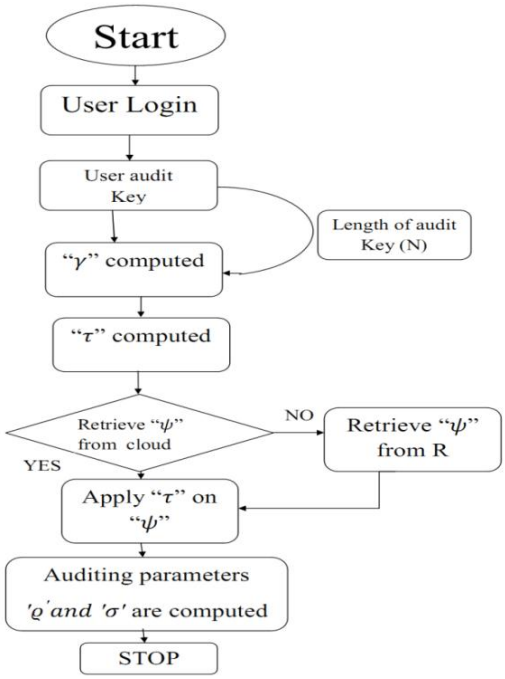

Figure 18: The block diagram of the retrieving outsourced data form cloud

VI. COMPARISON BETWEEN THE PROPOSED MODEL AND SOME EXISTING APPROACHES

Table 1 draws the comparison between some existing SaaS and PaaS security models with the proposed model. For better understanding of the comparison authors have referred the title of the papers in a smaller form, like "Identity-based proxy signature for cloud service in SaaS" by Xi cao et al.[12] referred as IBPS, "SaaS Access Control Research Based on UCON" by Junli Zhu et al. [13] referred as SACUCON, "SaaS Application framework using information gateway enabling cloud service with data confidentiality " by Kiyoshi Nishikawa et al. [14] referred as IGW.

Table 2 shows the comparison between the existing IaaS security models with the proposed model. Similarly like the previous methods titles of the following method's are also abbreviated.

"Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing" by Cong Wang et al. [8] referred as PPADS, "A view About Cloud Data Security from Data Life Cycle" by Xiaojun Yu et al. [9] referred as CDSDLC, "Implementing digital signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" by Uma Somani et al. [10] referred as IDSRSA, "Ensuring data Storage Security in Cloud Computing using Sobol Sequence" by P. Syam Kumar et al. [11] referred as EDSS.

Table 1: Comparison between existing SaaS and PaaS security models with the proposed model

Existing Solutions	Operating environment	Concerned attacks	Method description	Detail discussion
IBPS by Xi cao et al. **[12]**	SaaS	Denial Of Services	This method uses a key generator to generate different keys for User, CSP and Software Provider. The user uses its key to make a service request to the CSP and CSP takes the permission, for providing the service, from the software provider using its own key.	i. Three stage key generators and both way key transmission results high computational and network overhead. ii. Maintenance overhead is high for the CSPs as there are two different sites i.e. CSP site and Software Provider site.
SACUCON by Junli Zhu et al. [13]	SaaS	Access Control	This method uses UCON model for authentication purpose. This model consists of total eight component subject, subject attributes, object, object attributes, rights, authorization, obligation and conditions.	i. Simple authentication process. ii. No other security aspect is covered.
IGW by Kiyoshi Nishikawa et al. [14]	SaaS	Confidentiality	In this method security is achieved through information gateway in the cloud environment and the executing location is dynamically controlled. This results the confidentiality of data.	i. Due to dynamical change of executing location the communication overhead may increase.

Proposed model	All cloud	Authentication, access control, Confidentiality, Denial Of Services	Authentication and Access control is achieved by authentication of the user details, user name, and password. Confidentiality is achieved by restricting the services for different users Denial Of Services is achieved for SaaS and PaaS by key generator at the CSP site.	i. Sub grouping the users by their details helps to achieve access control and unique user ID, password achieves the authentication of the users. ii. Key generation procedure is based on randomize process between CSP and CSU, which helps to counter DOS attack. It uses simple and one way communication through a single onetime key so computation and communication cost is very low.

Table 2: Comparison between existing IaaS security models with the proposed model

Existing Solutions	Operating environment	Concerned attacks	Method description	Detail discussion
PPADS by Cong Wang et al. [8]	IaaS	Data security	This mechanism uses an external auditor which audits outsourced data in the cloud on behalf of the user depending upon some authentication key.	i. This mechanism also supports batch auditing facility. ii. As the auditing is done using an encryption key, the TPA can get the access the actual user data. This increases the security risk of the data.
CDSDLC by Xiaojun Yu et al. [9]	IaaS	Data security	This mechanism uses a symmetric key cryptography at the storing phase of data.	i. No auditing facility. So to verify the data integrity the users need to download the entire data from the cloud, resulting high communication overhead.
IDSRSA by Uma Somani et al. [10]	IaaS	Data security, authentication	In method digital signature is used for authentication purpose and RSA is used to secure the data in the cloud.	
EDSS by P. Syam Kumar et al. [11]	IaaS	Data security, availability	This mechanism uses erasure code for data availability, reliability. Utilize tokens are pre-computed using Sobel sequence to verify	i. Adding extra erasure codes increases the space overhead.

			integrity of erasure coded data rather than pseudo random data in exiting system.	ii. If any part of the file went missing the computational expense is high to retrieve the original data.
Proposed model	All cloud	Authentication, access control, Confidentiality, Data Security, Availability	Authentication and Access control is achieved by authentication of the user details, user name, and password. Confidentiality is achieved by restricting the services for different users Data Security is achieved using strong homomorphic encryption techniques Availability of data is maintained by keeping multiple copies at different locations. This location and copies of data are confidential.	i. Sub grouping the users by their details helps to achieve access control and unique user ID, password achieves the authentication of the users. ii. Use of TPA ensures the data integrity. iii. As Homomorphic encryption is used, the CSPs never have the actual data rather than they get an encrypted version of the user data. So there is no chance of data leakage. iv. And keeping multiple copies of data ensures the user data availability.

VII. CONCLUSION

Cloud has an ability to provide a distinct elevation to the current days IT industries. But like as any other technology's cloud also has some drawbacks and due to its complex nature, providing a single security solution is hard, but with a set of proper security solutions cloud could be invincible.

In this paper authors have tried to identify the existing security threats faced by cloud service provider, users and provided both the stake holders with a set of solutions in contrast with the existing solutions to make it safe and secure in all three service models. The Table 1 and Table 2 give us a deferential overview between the existing security solutions and the proposed security solutions. The existing researches mentioned in this paper have tried to focus only on one part of the cloud service model where as the authors have proposed security solutions for all the major cloud service models.

REFERENCES

[1] P. Mell, T. Grance, NIST definition of cloud computing. National Institute of Standards and Technology, October 2009

[2] GTSI Group, "Cloud Computing - Building a Framework for Successful Transition," *White Paper, GTSI Corporation, 2009.*

[3] Grace A. Lewis Research, Technology and Systems Solutions (RTSS) Program "Architectural Implications of Cloud Computing", May 18, 2011

[4] Gens F, 2009,' New IDC IT Cloud Services Survey: Top Benefits and Challenges', IDC eXchange, viewed 18 February 2010, from <http://blogs.idc.com/ie/?p=730>.

[5] ISO. ISO 7498-2:1989. Information processing systems- Open Systems Interconnection. ISO 7498-2

[6] Dlamini M T, Eloff M M and Eloff J H P, 'Internet of People, Things and Services – The Convergence of Security, Trust and Privacy', 2009

[7] Md.TanzimKhorshed,A.B.M.ShawkatAli,SalehA.Wasimi,"As urveyongaps,threatremediationchallengesandsomethoughtsforp roactive attack detection in cloud computing", *School of Information and Communication Technology, CQ University QLD4702, Australia*

[8] Cong Wang, Qian Wang, and Kui Ren Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", *IEEE INFOCOM 2010*

[9] Xiaojun Yu, Qiaoyan Wen, "A View About Cloud Data Security From Data Life Cycle", *IEEE ,2010*

[10] Uma Somani, Kanika Lakhani, Manish Mundra , "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" ,*2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010),IEEE*

[11] P. Syam Kumar, R. Subramanian and D. Thamizh Selvam, "Ensuring Data Storage Security in Cloud Computing using Sobol Sequence", *2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC – 2010) ,IEEE.*

[12] Xi Cao, Li Xu, Yuexin Zhang and Wei Wu, "Identity-based Proxy Signature for Cloud Service in SaaS", *Fourth International Conference on Intelligent Networking and Collaborative Systems, 2012,IEEE*

[13] Junli Zhu, and Qiaoyan Wen, "SaaS Access Control Research Based on UCON*", Fourth International Conference on Digital Home, 2012,IEEE*

[14] Kiyoshi Nishikawa, Kenji Oki and Akihiko Matsuo, "SaaS Application Framework using Information Gateway Enabling Cloud Service with Data Confidentiality", *19th Asia-Pacific Software Engineering Conference,IEEE, 2012.*

[15] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala,peng Ning. "Managing Security of virtual machine images in a cloud environment." *CCSW'09: Proceedings of the 2009 ACM workshop on Cloud computing security, November 2009, pp 91-96.*

[16] Miranda Mowbray, Siani Pearson "A Client –based privacy Manager for Cloud Computing*". OMSWARE '09: Proceedings of the Fourth International ICST Conference on communication system software and middle ware, June 2009 ACM.*

[17] Flavio Lombardi, Roberto Di Pietro. "Transparent Security for Cloud". *SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing, March 2010, pp 414-415.*

[18] F. A. Alvi, B.S Chaudhary, "review on cloud computing security issues & challenges".

[19] Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security", *Annals of Faculty Engineering Hunedoara International Journal of Engineering (Archived copy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.*

[20] "IBM's homomorphic encryption could revolutionize security" was originally published at InfoWorld.com.

[21] Pabak Indu, Souvik Bhattacharyya and Gautam Sanyal,"Different Aspects in Cloud Computing: A Comprehensive Review" Elixir Inform. Tech. 71 (2014) 24594-24602,June 2014.

Authors Profile

Pabak Indu received his B.E degree in Information Technology and M.E in Computer Science and Engineering from University Institute of Technology, The University of Burdwan and his areas of interest are Database, Web Technology, Network Security and Computer Network. He has published 7 research papers in International and National Journals / Conferences.

Souvik Bhattacharyya received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. He has received Ph.D (Engg.) from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor and In-Charge in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. His areas of interest are Natural Language Processing, Network Security and Image Processing. He has published More than 65 papers in International and National Journals / Conferences.

