A Proficient 5C Approach to Boost The Security in the SaaS Model's Technical Architectural Components

Balasubramanian.R[1]and Dr.Aramudhan.M[2]

[1]Research Scholar, Department of Computer Science & Engineering,
ManonmaniumSundaranar University, Trinelveli, South India.
[2]AssociateProfessor, Computer Science & Engineering Department,
PerunthalaivarKamarajar Institute of Engineering & Technology, Karaikal, South India.

Abstract

For anything that involves delivering hosted services over the internet is cloud computing.These services are classified as: IaaS,SaaS,PaaS.This paper focuses on SaaS security measures. SaaS is a cloud based productivity suite that helps the business people to connect and work from anywhere on any device. The data solely dumped behind a corporate firewall and it is physically accessed by the people through VPN system or through online.The only hurdle while adopting cloud computing is the lack of security.It is a major issue in the cloud for data as well as application and the platform. This paper gives an efficient approach named 5C approach for applying security under SaaSmodel.Itmainly focuses on authentication and authorization for customer data under SaaS in the cloud. The 5C mainly uses initial user level security in the architecture of SaaS server by integrating the Visual Guard Web Admin Console with other controls.

Key words

Cloud Security; SaaS; IaaS; PaaS; Cloud Service Provider; VPN; Visual Guard Security.

1. INTRODUCTION

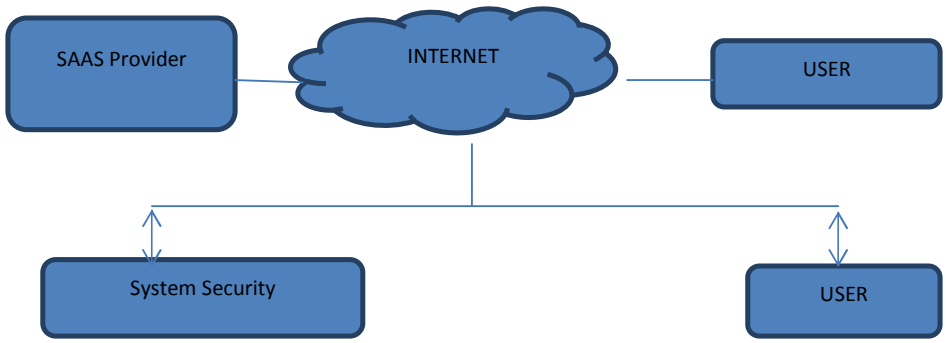
In Software-as-a-Service, the applications are one of the parts of cloud computing where the application is deployed centrally in the web based applications and it is offered to a large number of renters where each renter using several applications. From the renters' point of view, the cloud application with SaaS is outsourced in payment basis with billing system. From the service provider point of view, the Application Service provides is the earlier version for SaaS, and it is providing software facilities in less cost on large scale. The one and only ability for SaaS companies to deliver the huge amount of data to lot of places with high security access methods has had a profound impact on the ability for businesses to communicate, collaborate and achieve task [16]. Any enterprises of size small, medium can use the SaaS applications for non-core business. One example is salesforce.com-is a CRM based application. Currently the large enterprises are using SaaS for core business applications. Home based patient surveillance system is offered to health care institutions. These kinds of applications obviously need security challenges the importance of security. The SaaS with cloud computing can provide large enough advantages in terms of economic, security [19, 20, and 21]. SaaS also provides application level security with cryptography mechanisms, access limit control. The access limit control consists of 3 sub process like authentication, authorization and audit. Authentication confirms the stated

DOI : 10.5121/ijccsa.2013.3601

identity of a subject; authorization confirms that the user is allowed to do the desired activity after the authentication validated. SaaS is one of the cloud models, where core software is distributed to customers in pay-per-use method. In this model the end user no need to worry about running and securing the software. The customer provides their database and their business details to the SaaS and it will be deployed on the software. For example in Google Apps, Salesforce.com, the visibility and control afford to the IT manager is usually minimal.

The SaaS architecture is given in the following figure-1.

Fig:1SaaSArchitecture



The figure-1 depicts an additional dimension of responsibility and security. One advantage of physical security as a service is much like the traditional alarm companies in operation today they can serve both small and large companies across a very wide geography. The customer can use the SaaS provides' application, running in the cloud organization if they are capable. The functions are manageable from numerous client devices over a tinny client interface such as a web browser [18]. The end user does not succeed or control the principal cloud organization with network, servers, OS, storage space, or even separate application competences, with the conceivable exclusion of partial user-specific application structure settings.

The cloud is complete SOA, it provides amenity in many ways like SaaS, PaaS, IaaS etc. The customer is accessing the SaaS system over the internet. The SSL based security is available in Oracle cloud service accesses. The length of the encryption bit is least of 128 bit in the SSL connections. The oracle follows the SSL based security, with the private key, and it is used to generate the cipher key. This kind of security is recommended for all the browsers enabling the web based applications and these certified browsers for oracle applications are available in the Oracle support portal. There are many third party sites are integrated with the Oracle applications and it permits the HTTP connections additionally with the HTTP connections. The current survey conducted by Cloud Security Alliance (CSA IEEE) disclose that lot of companies are eager to adopt the cloud computing. But the security is necessary to accelerate the cloud is a wide scale and to respond to regularity drivers. Till now guaranteeing the security of corporate data in the "cloud" is difficult as they provide different services like SaaS, PaaS, and IaaS. Each service has its own security issues (Kandukuri et al., 2009). In SaaS, the client has to depend on the supplier for appropriate safety measure. The provider must do the work to keep multiple users' data. So it becomes difficult to the user to guarantee that right safekeeping measures are in place and also challenging to get promise that the application will be obtainable when needed. Hence this paper concentrated towards the security measures in technical architectural components of SaaS service delivery model.

The rest of this paper is structured as follows. Section 2 describes the related studies.Section 3 presents problem statement which includes the proposed 5C approach to improve security in SaaS components model. Section 4, we implement the 5C approach in Visual Studio .NET Framework 2010 for SaaS based application. Section 5 describes the results and discussion. The conclusion of this paper is presented in section 6. The extension of this work regarding PaaS and IaaS security measures are also mentioned here.

2. RELATED WORKS

Many of the Internet services require users to provide their sensitive information such as credit card number and an ID password pair. In these services, the manner in which the provided information is used is solely determined by the service providers. The work framed by article[1] permits the users to select the manner in which their information is protected. In their framework, a policy, which defines the type of information protection, is offered as a *Security as a Service*. According to their policy, users can incorporate the type of information protection into a program.

SaaS is an emerging Software service model providing application lease through internet. The majority of small and medium sized enterprises customers found that the costs of software applications are reduced and its maintenance is easier. In addition, for SaaS users, business data, especially financial data and customer information are core secrets for the company. These are new challenges which the SaaS model brings to the management to pay enough attention to data security. So to find out a new strategies to give guarantee the high quality of software service, Haitao Song and JingrongY_i[2] highlighted solution.

Most of the surveys show, security and privacy are the top concerns preventing firms from moving to SaaS.YuHuiWang[3] conducted a research survey regarding the Information Systems Continuance Model and adopts privacy and security compliance as a new construct of interest. In his study he aimed to contribute to a more sophisticated understanding of the role of privacy and security compliance for customer satisfaction and continued SaaS usage intentions.

A detailed survey, carried out by Rashmi[4], gave an analysis on cloud computing existing various security issues. Also they made an attempt to provide future security research directions in Saas model.

Regarding the tenants' requirements about enterprise data Security on SaaSYongjing A. Li*, Jiang B. Wu[5] proposed a data security protection strategy of the SaaS mode. The tenant can energetically select the security strategies at different levels. To support their SaaS security level they made SaaS security model test bed. For supporting their SaaS Security Level, they built SSM (SaaS Security Model) test-bed. On the SSM test-bed, they have done some experiments, which confirmed their SaaS Security Level is feasible and easy to use.

The one of the major hindrance for the growth of cloud computing is security issues. Improving features of a new model should not risk or threaten the other important features of current model. The cloud users need not be vigilant in knowing the risk of data breaches in the new environment. Subashini and Kavitha[6] conducted a survey regarding the security risks that create a threat to a cloud.

Cloud computing offers tenants to store their data on remote server and relieves tenants from the risk of storing and maintaining data locally. The off-premises cloud computing should make believe many security issues and challenges for user data since tenants does not have direct control on their data. Regarding this Mr. Hiren B. Patel and Mr. Dhiren R. Patel[7] have presented a review on various security issues and approaches in cloud computing.

Mohamed Almorsy, John Grundy, and AmaniIbrahim[8] have introduced a Tenant Oriented SaaS Security Management Architecture. Their paper facilitate i)every tenant to monitor the security of their cloud hosted assets ii) saaS provides to manage security isolation between their tenants iii) to promote security engineering from system oriented security to tenant oriented security. Also it permits multi-tenantSaaS application to easily catch the different tenant's security requirement.

Article [9] reveals on security regarding data storage for SaaS Applications or platforms that are built on multi-tenant architectures. Due to security reason here each tenant on cloud may be allotted separate database.But single database allocation is not cost effective. Hence single database allocation is shared. Since sharing of database leads to unauthorized access of tenants data by another tenant, they developed DPET (data partition encryption technique) in their paper.

As there is no frame work existing from logical level for secure planning of cloud services in article [10] the authors highlighted a clear idea about the business logic and security logic. In their paper a new model is proposed to write secured services without any burden to the developer of rewriting security routines.

In Security-as-a-service model the focus is on security provided as cloud services; i. e. security delivered through the cloud instead of on-premise security solutions.In the article [11] the authors provided the comprehensive analysis of security-as-a-service delivery model from various perspectives. They addressed various issues regarding security delivered as cloud service.

In a cloud computing environment, the entire data stored over a set of network resources. The different security and privacy challenges are to be addressed since the data centres may be available in any part of the world beyond the control of users. Hence to intricate and analyze many unresolved issues threatening the adoption of cloud computing a elaborate survey is presented in the article [12].

In Cloud Computing resources are shared among different user. Because of shared resources used in Cloud, user does not have control and permission to modify, delete or access of other user's data. So data integrity is one of the biggest security issues. To provide integrity of user data traditional integrity tools do not use because of dynamic nature of user data. Providing monitoring service will help data owners to ensure integrity. In this method client can check without downloading the file as well does not required a local copy. Another method which could be considered as improvement over PDP is Proof of Retrivebility(POR). This method detects data integrity as well as it recovers original data. Therefore in article [13] data integrity techniques have been surveyed by Parth D Shah.

In the article [14] the authors proposed multi-tenancy in SaaSarchitecture which introduces the concept of fully modular system, where the different modules may be implemented and configured according to the need of the users.

Because of the security issues the cloud computing has notgained wide acceptance. It is encircled by many security issues, data integrity etc. Article[15] is study of various security threats caused to the data stored in cloud and also threats concerned to both user and vendors in cloud computing. This is a literature survey of various key security threats associated with cloud computing.

3. PROPOSED STATEMENT OF THE PROBLEM

SaaS applications are succeeding the method of commissioning: the application distantly hosts and methods data essentially belonging to the tenant. Consequently, entree control in SaaS prototypes are mostly about defending the renter's data placed at the supplier's side. The renter controls the management and information about the operators of the solicitation and the correct to use control rules and policies. Hence it is the responsibility of the SaaS provider to give guarantee to data security for customer satisfaction. So to give enough attention to data security an efficient 5C approach to improve the security in SaaS model is presented in this paper.

3.1Proposed 5C approach

SaaS includes dozens of critical security features specifically designed for customers to keep their data very safe, secure and it should be under the customer's control. The data belongs to the customer, and the application tool (SaaS tools) enable the customer to control it, including who the customer share it with and how the customer share it. The data center in the SAAS network provides exceptional security and guarantees reliable access to the customer data. The security is provided in the following ways.

- Customer work is always backed up
- Customer can own and control your data
- Customer data security and reliability increased
- Customer data is encrypted and authenticated strong
- Customer Security is constantly improved by SAAS team

3.1.1 Customer work is always backed up

While the customer work, all the customer critical data is automatically backed up on SaaS servers. So when accidents happen, if customer computer crashes or gets stolen, customer can be up and running again in short time period.

3.1.2 Customer can own and control your data

When customer put their data in SaaS application, customers still own it, and it says just that in SaaS server contacts. SaaS Apps' powerful, easy-to-use tools help administrators manage things like users, documents and services, and keep track of usage and data via dashboards.

3.1.3 Customer data security and reliability increased

SaaS data centers are designed and built for SaaS applications and don't include unnecessary hardware or software. The number of potentially exploitable vulnerabilities are reduced by this. SaaS guarantee 99.9% uptime and built-in robust disaster recovery, so customer doesn't have to worry about natural disasters.

3.1.4 Customer data is encrypted and authenticated strong

SaaS Apps suggestions an additional layer of safety with two aspects based authentication, which significantly decreases the risk of hackers burglary the usernames and passwords. SaaS also spontaneously encode browser assemblies with SSL for Apps users without the necessity for VPNs or other expensive, cumbersome organization. This helps to safeguard customer's data as it journeys among the customer browser and SaaS data centers.

3.1.5 Customer Security is constantly improved by SaaS team

SaaS large information safety team continually screens SaaS worldwide network of data hubs. Many have progressive degrees ad are thought-leaders who are defining SaaS industry's info-security practices. SaaS Apps and SaaS data centers are also SSAE 16 / ISAE 3402 type of TPA [Third Party Auditors], they assesses the controls in place for safety, confidentiality, incident reply, and more. The 5C approach is elaborated and given in detail step by step below.

4. IMPLEMENTATION

- Customer work is always backed up
- Customer can own and control your data
  - Simple Internal Authentication by VGCP
  - Simple Federated Authentication [SSO – Single Sign On]
- Customer data security and reliability increased
- Customer data is encrypted and authenticated strong
- Customer Security is constantly improved by SAAS team

The 5C algorithm is implemented in VISAUL STUDIO DONTET FRAMEWORK 2010 for a SaaS based application and the efficiency of the security is compared with the existing SaaS security and the result is given. The 5C algorithm says a step wise procedure to make customer satisfaction more in SaaS service as well as in SaaS security.

The very first step in the SaaS computing, whenever the data of the Customer work is forwarded to and from customer's Hard disk to the cloud storage area it is always backed up by a synchronization methodology in cloud. The synchronization is updating the data in cloud storage and in customer's Hard disk in a periodical manner after login to the system.

The next step is to provide a provision to the customer; they can own their data and control themselves. For that the simple internal authentication can be provided by a dynamic password each customer on who registered in the SaaS. After receiving the dynamic key the user customer login with that key every time. The simple authentication dynamic key provide is implemented using Chinese Remainder Theorem, where It provides a method to uniquely determine a number S modulo k many relative prime integers

$$m_1, m_2, m_3 \ldots\ldots m_k \rightarrow S < \prod_{i=1}^{i=k} mi \qquad \text{--equation (1)}$$

Equation (1) provides a dynamic key for each customer according to the number.

The next one is the simple Federated Authentication, itis the strength and the flexibility also combined with the SaaS security. The system forte will promise application safety by

- Monitoring user entree inside the limits of their subscription
- Assuring data confidentiality between the users sharing the application
- Eliminating security breaches at protecting you from exterior attacks

And the system **flexibility** will contribute to the development to the professional by:

- Simplifying the development of your business model and the formation of your offer
- Answering to client needs related to user management

- Supporting scalability: Making best of the performance and abridging the management for large number of users and protected components.

Initially the SaaS server and the renters are integrated together. Due to the number of users increase, SaaS and the customers may wish to delegate certain management rights, so that clients are managing theirs users and accounts by themselves. For secured integration and management of renters the VG is integrated and it gives a management interface available to non-technical users, permitting you to delegate user management to local business leaders. Also this management interface comprises all usually mandatory entree control functions and proposals entree via the Internet shown in Figure-2a, Figure-2b.

Figure-2a: Visual Guard WebConsole Administration Dashboard

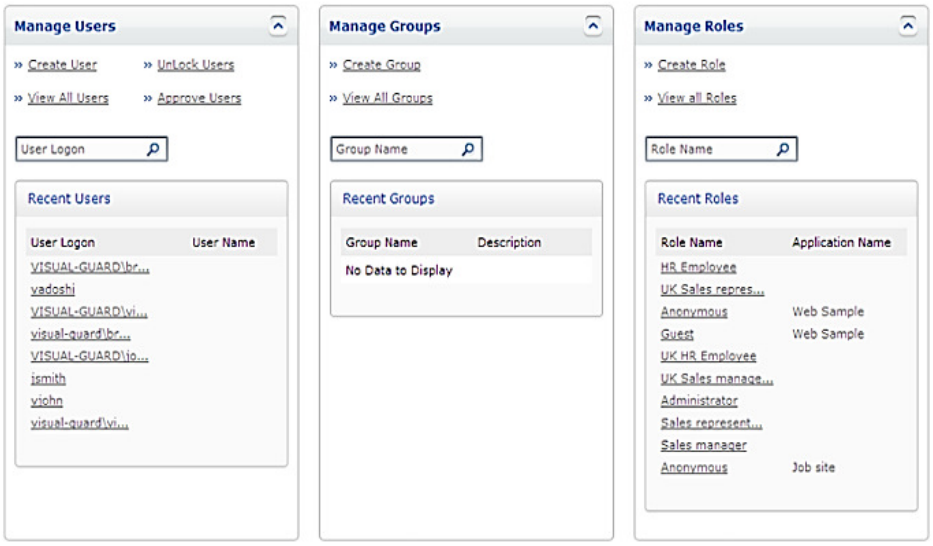
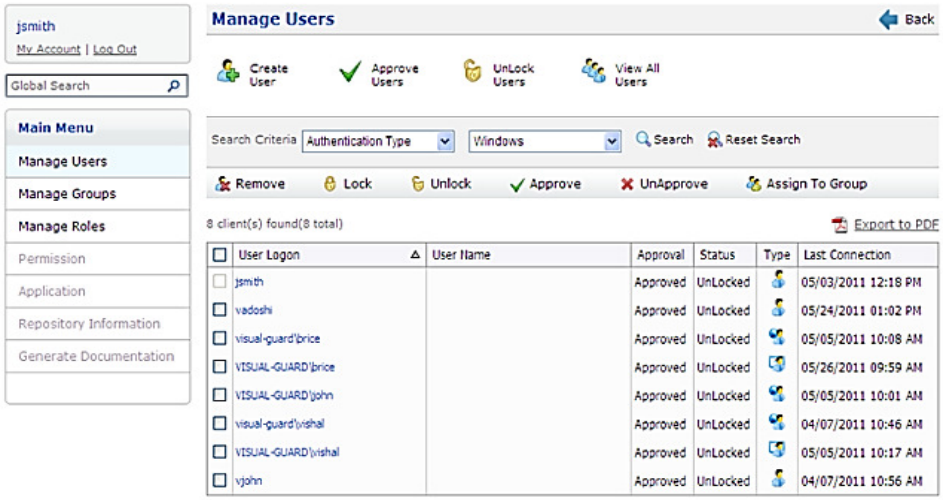


Figure-2b: Visual Guard WebConsole User Management



All renters acquires VG-WC [web console] panel for their operator management. Where the user can add, edit and delete their profile and administration account, administration operation, administration to certain applications are delegated. Merging these principles allows VG to cover numerous situations, entrusting numerous levels of management rights, according to your clients' association and necessities.

Single Sign On

The VG delivers the SSO feature to provide more user capability, and mostly do the user Session managing by recognizing the User, reconstructs their session for site official visit, and loads and smears the safety data like characteristics, nature of the work, authorization's etc., It has a tool to manage the safety tokens, and enhance the recital problems like page visited, number of time visited, request and response time with time out exceptions. Once the renter registered in SAAS, a user panel will be provided and the user account also can be managed, it is shown in the GUI in figure-3a, 3b for before login and after login.

Figure-3a: When the user attached to the first site, they will entree the login frame where they will select the type of account and enter their qualifications.

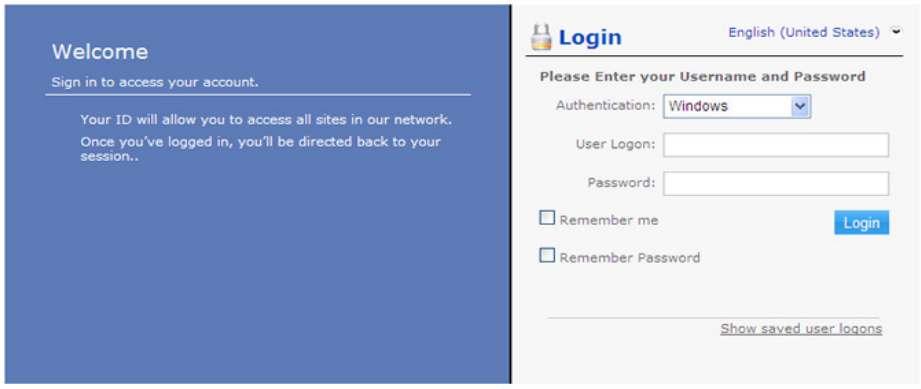
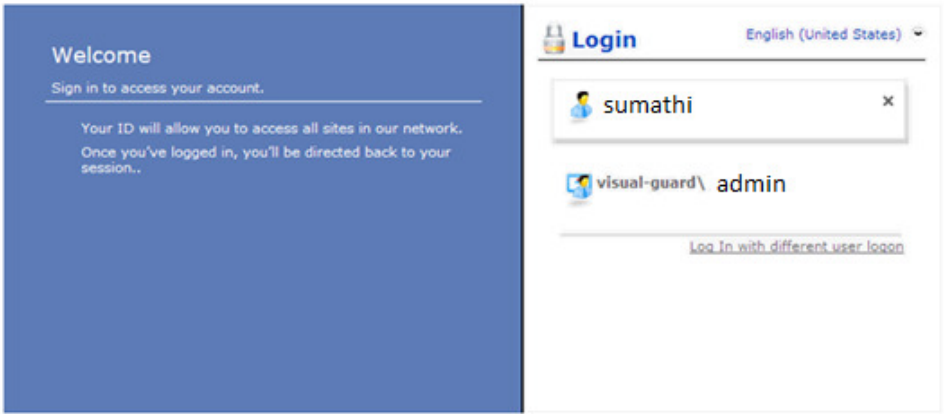


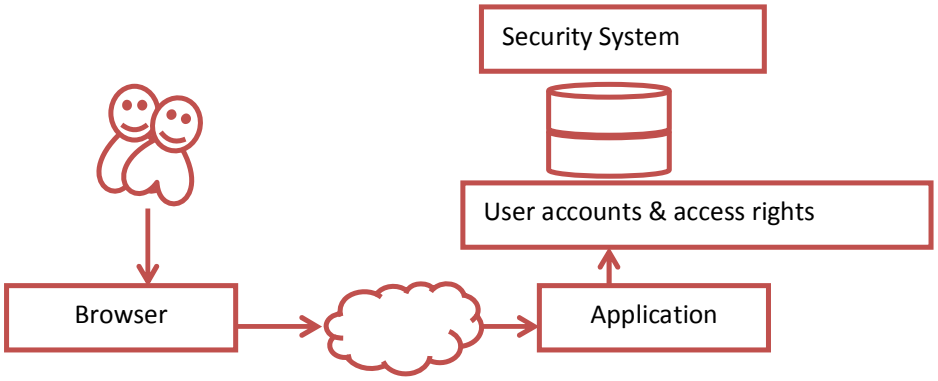
Figure-3b: The user can select to save assured credentials. On their subsequent visit, they can use the account remembered in the system.



The user can select to save assured authorizations. On their subsequent visit, they can use the account learn by heart in the system. Figure-3a provides the particulars formerly login to the

system, 3b demonstrates after login to the system. When login, the user should answer for what are all the credential listed in the window.

Figure-4: SaaS modelwith VG



The application is presented by the wholesaler with VG integrated. Users access it via the Internet. Clients pay to use your application on a time-limited, periodic basis. Software based businessmodel is the pay-per-use and the Softwaredistributionmodel is SaaS. From Figure-4, the users always communicate through the browser window to the application where the user accounts and access rights are applied from the security. The whole security solution can be provided by the VG integration with ASP by

- User Management
- User Authentication
- Authorization
- Static and Dynamic Permissions
- Auditing and Reporting

Since, VG is creating a system which provides safety for most of the common types of attacks; it is deployed with the SAAS applications.

Unauthorized access to security data:

- Safety data is not understandable by straight SQL access. VGI needs a secured association via the SAAS application or via the management interface to read and adjust this data.

- Subtle data like passwords is encoded.

Denial-of-service: VGI comprises guard in contradiction of attempts to make it unobtainable to customers by drenching it with recurrent logon requirements.

Illegal management operations: a user could learn how to entree the management interfaces or the APIs that accomplish access control. VG rejects the unlawfully delivers supplementary entree privileges to user accounts.

Capture of confidential information:

- Among the client browser and the web server: VG supports SSL/HTTPS protocols and encryption of transportations among the browser and the web server.

- Among the .NET mechanisms inside the SaaS application: VG trusts on the Microsoft Substitution System (Marshall) to accomplish and guard such transportations.

Password cracking: VG permits you to describe a classy Password Policy to guard against password cracking.

When a user is efficaciously accepted by the SaaS supplier's scheme, it is then essential to permit the user entree to only the data and purpose they are allowed to access. This is mentioned as approval. Given that a SaaS policy will established over time and may well alteration or add to its credential methods, it is essential to make sure the permission module is distinct from the confirmation module(s). The permission module should log each and every try at performing an action irrespective of the success of that try. The precise mechanism of permission is completely reliant on upon the SaaS software design. Recall, it is best to authenticate the requestor's permissions with every sole request. This will help to expurgated down on cross-scripting bouts etc.

Customer data safety and trustworthy enlarged can be completed by Packet inhaling**:** VG comprises a guard in contradiction of the imprisonment of data packs to find passwords or safety tokens in transportation over the network. A hacker could snip these tokens to create calls to the organization as though they were a genuine user. And one more way is by the SQL injection procedure, which is the VG Management console, comprises examination fields – for example, to discovery a user account. It is pre-armed in contradiction of SQL injections, which contain of inserting parts of SQL declarations in the search field, with the aim of referring trusted information, or illegally altering the safety data.

Customer data is encoded and legitimate powerfully by given that a key for the customer and using those keys the data is encoded and conveyed in SaaS.

Data – Encryption

In the best repetition three-tiered design, encryption keys are usually put in storage on the application tier. One separation method which has verified fruitful is to provide a dissimilar key for every customer. An unintentional cross-pollination of data owing to code flaw would consequence in the decoding of data and with a key that does not the same. It is essential to recollect the keys not from inside the database tier to include honesty to the procedure with "Defense in Depth". Defense in Depth is applied safety plan for accomplishing Information Pledge in today's extremely networked environs. It is a "best practices" plan in that it trusts on the intelligent application of methods and tools that occurs today. The aim is to present barriers at all conceivable level to avert an opening and to not trust on a sole tier or device to prevent illegal access. Therefore, sendoff the key with the data would be neglectful. Different keys should be used for Web to browser Meta data encoding in the similar way that data actuality deposited on the disk is encoded. Figure 3 exemplifies these thoughts. There are distinct key mechanism provides keys for the Web to web-application tier interaction and the solicitation to database tier communication. The advanced key is used to encode data upon the database server disk.

.

Encryption

```
FileStreamfsCrypt = new FileStream(cryptFile, FileMode.Create);
RijndaelManagedRMCrypto = new RijndaelManaged();
  CryptoStreamcs = new CryptoStream(fsCrypt,
   RMCrypto.CreateEncryptor(key, key),
   CryptoStreamMode.Write);
```

Decryption

```
FileStreamfsCrypt = new FileStream(inputFile, FileMode.Open);
RijndaelManagedRMCrypto = new RijndaelManaged();
CryptoStreamcs = new CryptoStream(fsCrypt,
RMCrypto.CreateDecryptor(key, key),
CryptoStreamMode.Read);
```

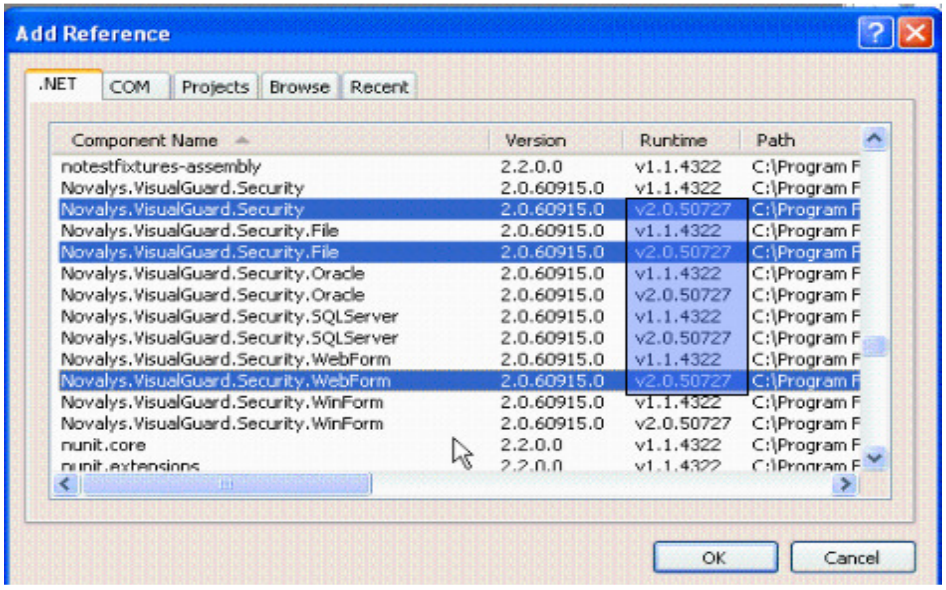
The encryption and decryption of the file or the data will be secured by two methods using the Rijndael Encryption procedure. They merely need that you pass them the full path to the original and target files. They both require the use of the System.Security, System.Security.Cryptography,System.Runtime.InteropServicesandSystem.

Text.Regualr.Expressions namespaces. The Rijndael encoding method has been deliberated to substitute the old DES procedure. Like DES, it is a block cryptograph. It uses 128-bit, 192-bit or 256-bit keys. This implementation encrypts 128-bit blocks.

5. RESULT AND DISCUSSION

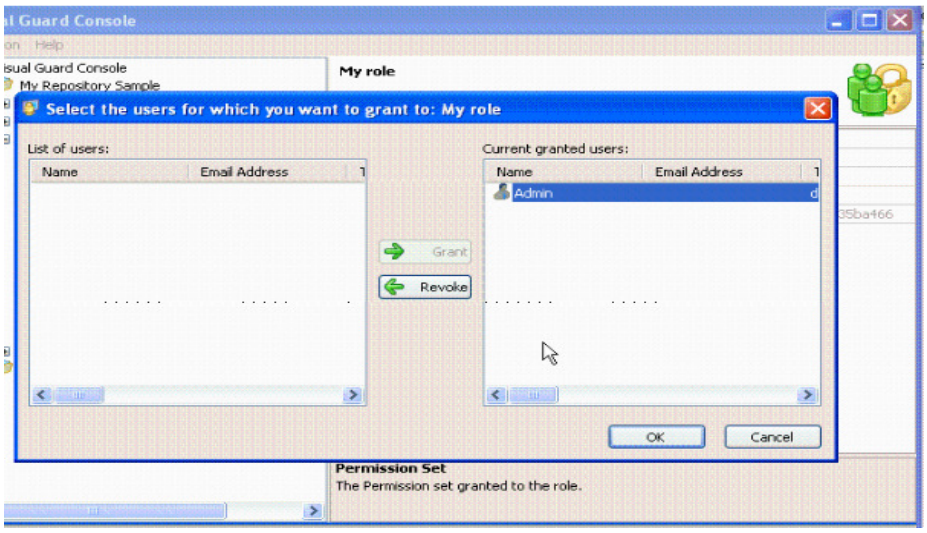
The SaaS result is shown in figure-2a, 2b, 3a and in 3b, where the security is applied in the software itself. But there are some more ways we can provide security for SaaS, and it is concluded from, a survey conducted among the various people using cloud and the conclusion is given in figure-5. The result says that the security can be applied in any way, like by the vendor, by the end-user or by uploading a crypt form data.

Figure-5: SaaS Security by Visual Guard



The complete security explained above 5C steps are integrated in VG, the third party tool which provides the sign on security, SSL security, and Certification security like all in one window. It can be integrated in the visual studio software and provide security in SAAS in depicted in figure-5.Designers use this module to install the Authorizations and Characters associated to their application. When new types of the application are released, the distribution module systematizes the update of the consents in the target sources (testing, QA, production…).

Figure-6: User Control in V-Guard



After integrating the VG in the VS-2010 software, the security mechanism can be getting activated while running any application on that. Generate and accomplish username/password interpretations with VG. Add your Dynamic Directory accounts with VG so that users can attach to your solicitations with their Windows accounts. Streamline user management with ranked

groups. Agent user management privileges to VG users. Limit the actions VG administrators can perform.

In the VG based administration, groups are used for user maintenance and each group divided into sub-groups. Even it is a group or sub group the user should login by entering the username/password in all the entrée. Each user is assigned with their own roles and the accounts about the user and the role is compared and validated in the virtual directory with the browser session values. This help to restrict the user in time, application access and so on.

Fig. 7a Granting Roles to Users

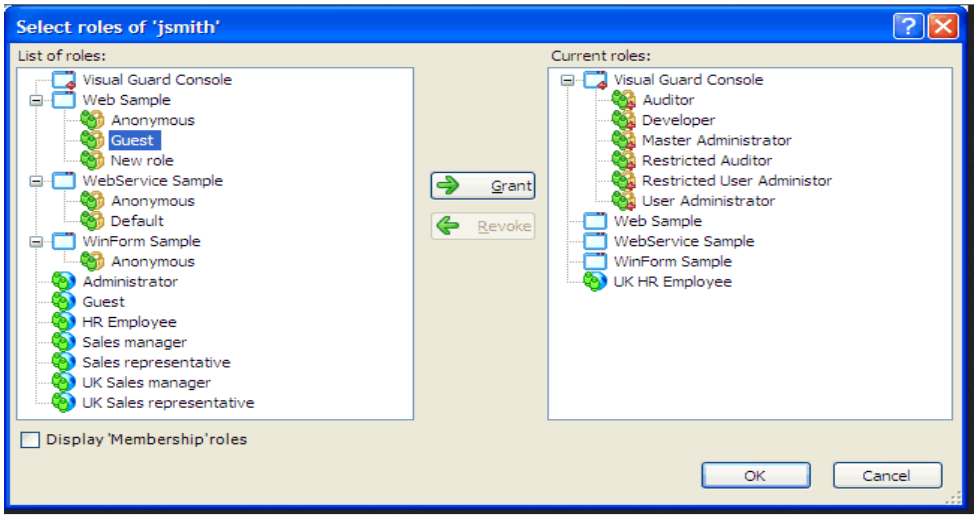


Fig. 7b Managing Roles

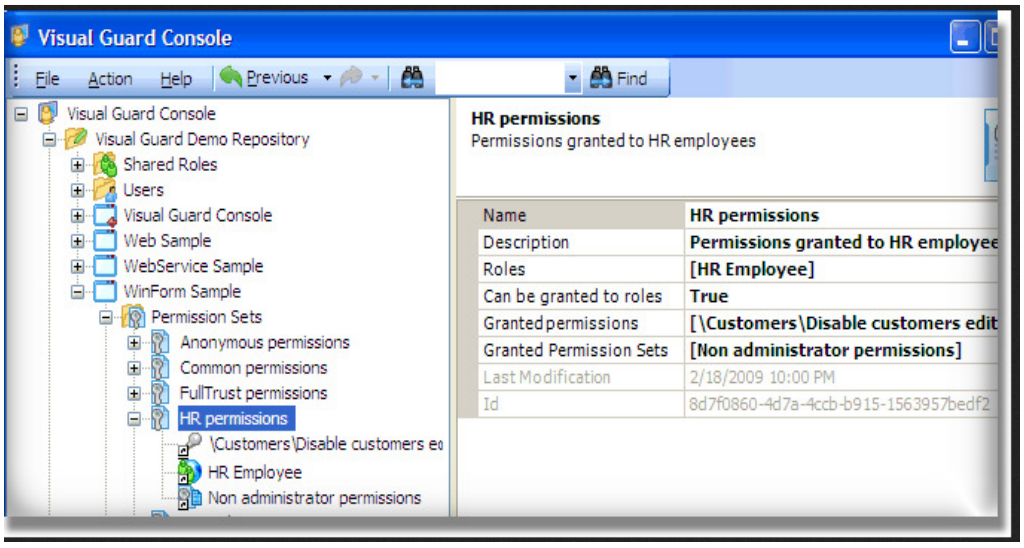
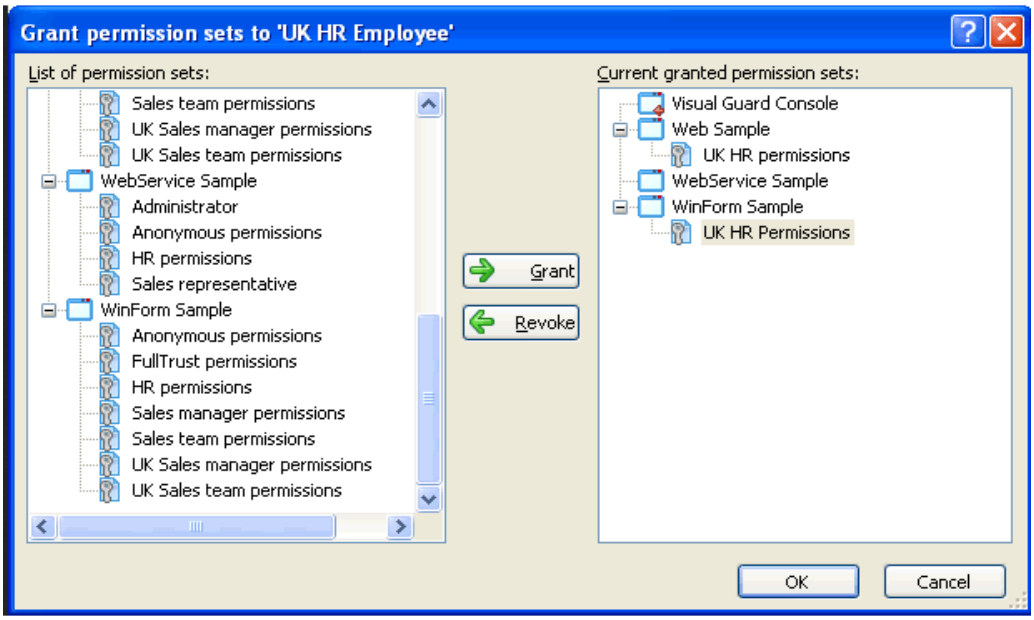


Fig. 7c Grouping Permissions Sets into Roles



When the user role is getting assigned the user's permission can be assigned for accessing multiple applications with either by username password or by using windows authentication mode. The validation of the user role can be verified by group wise or by sub group wise. All this accounts information with the role is stored in the virtual directory for each users

Fig. 8a Guarantee a security Report

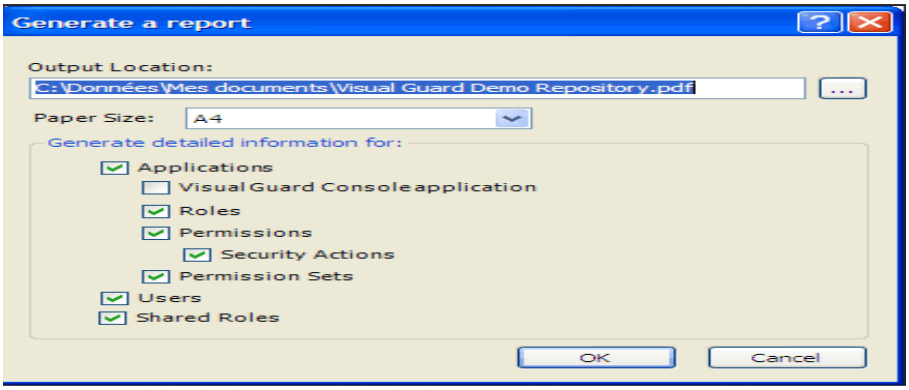
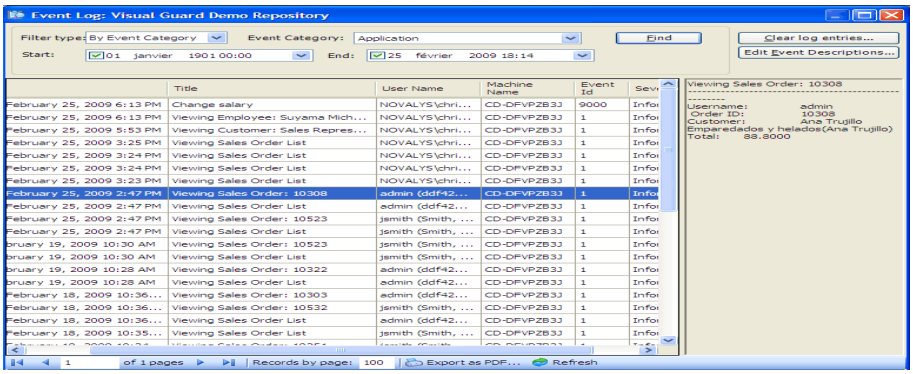


Fig. 8b Auditing – Event Viewer – Secured Applications



There are kinds of reports can be generated based on the data about the user, data about the groups, data about the roles and data about permissions. The operations performed by the users in the application also stored in the VG and it can be generated as the report form. Also the reports can be generated for the administrator performance on the applications.

6. CONCLUSION

This paper provides an architectural based security, where the end user will get the full benefit of the SAAS security. Since a huge number of customers are accepting the SAAS model, the vendor should provide at a low risk. Every new customer reaches SAAS service by the suggestions and advice from the existing customers experience and satisfaction with SAAS service.

As you've seen, successful companies offer a comprehensivevariety of services and use many different methodologies. What all the successful companies are having in commonmind is that they know how to measure and closely track their performance, they develop appropriate financial processes, and they have made the value of customer service an integral part of their companies' DNA to form the basis of every business area and to monitor every business decision

Future Work

Since the SaaS security talking about the physical or network level of security, the other PaaS can be implemented and connected with the SaaS security. Finally all the IaaS, SaaS and PaaS securities are integrated together and molded as a complete security solution to the cloud computing.

References

[1] Kenichi Takahashi&TakanoriMatsuzaki, "Security as a Service for User Customized Data Protection" Software Engineering and Computer Systems Communications in Computer and Information Science, 2011,Vol. 180,No.2, pp298-309.

[2] JingrongYi&HaitaoSong " Primary discussion on Data Security Management Under SaaS model" Applied mechanics and materials ,2011,Vols. 58-60, pp 441-446.

[3] YuHui Wang " The role of SaaS privacy and security compliance for continued SaaS use", NetworkedComputing and Advanced Information Management (NCM), 2011,pp303-306.

[4] SolutionsRashmi , " Securing Software as a Service Model of Cloud Computing: Issues and solutions" International Journal on Cloud Computing: Services and Architecture (IJCCSA),2013, Vol.3, No.4, pp01-11
[5] Yongjing A. Li*, "An SLA based SaaS Security Level", Telkomnika, Vol.11, No.7, July 2013, pp. 4111~ 4121
[6] Subashini n, V.Kavitha(2011), " a survey on security issues in service delivary models of cloud computing",Journal of Network and Computer Applications, Vol. 34, pp1-11.
[7] Mr. Hiren B. Patel and Mr. Dhiren R. Patel (2011), "A review on various security issues and approaches cloud computing" ,International Journal of computer science Engineering and Information Technology Research(IJCSEITR) vol. 1 , issue 2, pp 69-80.
[8] Mohamed Almorsy, 2012," TOSSMA: ",In proceedings of 5th IEEE Conference on Cloud computing, Waikiki, Hawaii, USA, pp24-29 .
[9] Prof.M.Padmavathamma" Multi-Tenant Data Storage Security In Cloud Using Data Partition Encryption Technique", International Journal of Scientific & Engineering Research, 2013,Volume 4, (7), pp 2229-5518.
[10] Sahar Mohammed Abduljalil, &Ehab E Hassanein,"A Novel Approach for Handling Security in Cloud Computing Services", IJCA, 2013,Vol.69, No.5 pp9-14.
[11] Deepak H Sharma, & Manish M Potey "Security-as-a-Service from Clouds: A Comprehensive Analysis", IJCA,2013 Vol. 67, No.3, pp15-18.
[12] RohitBhadauria&SugataSanyal,"Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques" International Journal of Computer Applications(IJCA) , 2012,Vol.47, (18),pp47-66.
[13] Parth D Shah &Amit P Ganatra, " Comparative Study of Data Possession Techniques for Data Storage as a Service (DSaaS)", International Journal of ComputerApplication(IJCA),2013, Vol. 80 , No.4, pp38-42.
[14] Sunil Kumar Khatri, &HimanshuSinghal," Multi-Tenant Engineering Architecture in SaaS", IJCA,2013,pp45-49.
[15] PrashantRewagad&YogitaPawar. Article," Security Threats - Main Hindrance to the Wide Acceptance of Cloud Computing Services", IJCA ,2012, pp21-27.
[16] Advanced SaaS Security Measures, Overview of BlueTie Security, SaaS Security White Paper, December 2012.
[17] Security Issues in Cloud Computing,Cloud Security Issues Jerry Scott 2011.
[18] Cloud Computing and SaaS, ASIS International (ASIS), 2010.
[19] Brunette, G.,&Mogull, R.: Security guidance for critical areas of focus in cloudcomputing v2.1. Tech. rep., CSA,December 2009.
[20] Catteddu,D.,&Hogben, G.: Cloud Computing: benefits, risks and recommendationsfor information security. Tech. rep., November 2009.
[21] Dean, D.,&Saleh, T.: Capturing the Value of Cloud Computing. Tech. rep., BostonConsultancyGroup,November 2009.
[22] Federatedauthorization for SaaS applications, Maarten Decat, Bert Lagaisse, WouterJoosen IBBT-DistriNet, 3001 Leuven, Belgium, ESSoS-DS 2012.
[23] www.codeproject.com/Articles/560900/Building-a-SaaS-Authentication-System-Using-the-AS

Authors

1.I, Balasubramanian.R, studied B.E(CSE) and M.E(CSE) at Regional Engineering College, Trichirappalli, TamilNadu, South India. I have more than 5 years of teaching experience and about 10 years of experience in Information Technology.

2.I, Aramudhan.M, studied B.E(CSE) and M.E(CSE) at Regional Engineering College, Trichirappalli, TamilNadu, South India. I completed my Ph.D in Computer Science and Engineering at IIT, Chennai, TamilNadu, and South India. I am working as Associate Professor at PKIE &Technology,Nedunkadu ,Karaikal,Pondy,India. I have more than15 years of teaching experience.