A Review of Data Security and Privacy Issues over SaaS

Rahul Kumar Pandey

Student, Master of computer Application , Galgotias university , Noida

Ekta Kumari

Student, Master of computer Application , Galgotias university , Noida

Aradhya Swaraj

Student, Master of computer Application , Galgotias university , Noida

Abstract—Cloud computing is a new internet-based computer technique. Cloud service providers offer service models that make the best use of available resources. Cost and services of cloud computing are quite popular with cloud users. Because of its reliance on a cloud provider, data security and privacy are a major concern. Although the SaaS service model offers numerous conveniences, it still lacks some security measures.We examine the lack of security mechanisms and feasible, current remedies in this study.. For in-depth research on SaaS security, vulnerabilities, and security risks, this article will be useful.

Keywords—Security,SAML(Security AssertionMarkupLanguage),SSL(SecureSocketLayer),TLS(TransportLayerSecurity).

INTRODUCTION

The most popular and cost-effective form of computing today is cloud computing, which offers three service models: SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Cloud computing, distributed computing, grid computing, scientific applications, military, governmental, and commercial systems and applications are all important security concerns [10].

A few of the many categories under which cloud computing security can be defined include physical security, network security, IT system (system security), information (data security), and application security. Security is the responsibility of both the client side and the server side. Physical security up to the hypervisor, environmental security, virtualization security, and environmental security are all handled by Amazon AWS EC2. The customer resource management (CRM) SaaS platform from Salesforce.com contains security requirements for managing physical and environmental security. Additionally, it ensures the data, applications, and infrastructure are secure. Many nations adhere to norms and regulations for data protection and information security all around the world. These nations, which use data protection legislation, include Japan, Australia, New Zealand, other Asian nations, and many more. They violate the OECD's privacy and security guidelines as well as those of APEC,the Organisation for Economic Cooperation and Development (OECD), and the European Economic Area [8].

LITERATURE REVIEW

From 2019 to 2022, research papers focused on data privacy and safety issues in Software as a Service (SaaS) environments. Key themes included data breaches and vulnerabilities, encryption and authentication, privacy concerns and compliance, trust and user perceptions, and third-party risks. Studies emphasized the need for robust security measures, proactive monitoring, and encryption techniques to protect data in transit and at rest. Privacy implications, such as data ownership, user consent, and compliance with regulations like GDPR, were discussed, highlighting the importance of transparency and user control. Building trust with users and addressing third-party risks were also key areas of investigation. Overall, the literature underscored the significance of comprehensive security measures, privacy-aware design, regulatory compliance, and user education to ensure data protection in the SaaS ecosystem.

CHALLENGES IN SaaS SECURITY

Clients completely rely on service providers in the SaaS model. Clients of cloud services are unaware of the technological security concerns and security measures required for data safety. Service providers ensure that client data is secure during multi-tenancy live migration and isolation and that no user will be able to see the data of another user. Client knowledge of appropriate security precautions and data availability in a secure manner when he needs it is crucial [3], [15]. Service providers offer the most recent updates to software that already exists. In addition to focusing on the portability of the application, the service provider is also improving the safety framework with data integrity [15], [20]. The cloud computing infrastructure service offered by a third-party provider (such as flipkart, Google, etc.) or the SaaS software vendor's own private server may be used to host the application. [3]. Moving applications and data onto a public cloud environment introduces a violation and raises the safety risk. The personnel of the provider of services or another customers who use SaaS services may or may not be the source of this danger [16].

DATA SECURITY AND BACKUP

The SaaS vendor shall guarantee to his customers that sensitive data is always regularly backed up with the option of speedy recovery in case of a disaster (intentional or unintentional). In order to guard against unauthorised fraud and unintentional theft of sensitive data, the provider also applies robust security measures such encryption on the backup data that is stored [3]. Sensitive data is defined by the Data Protection Act. Either the client or the service provider, or both, may define sensitive data. Apply the Act of Prohibition with legal law if the data is sensitive at that point. Although laws of protection are frequently highly helpful, they are frequently ineffective because laws change in response to the establishment of international borders [2], [8]. The three major objectives of ENSIA (European Network and Information Security Agency) are policy andorganisation, technical issues, and legal matters [39]. ENSIA is in charge of attaining network and information security. Instead of implementing a solution, NIST defines the type of services and works to understand internal cloud operations and dangers.

The amount of time necessary for it is a crucial parameter when a loss occurs that requires the recovery of operational data. When data is lost, steps are taken to ensure that either all or just the lost data is restored. The recovery of the full data file is what data recovery actually means [2]. Failures in the management of cryptography are currently the biggest issue with data protection. Key management and exchange between the user and the service provider. Only a few ways are actually practical, therefore there is still more work to be done on using cryptography to secure data [16], [17].

DATAINTEGRITY

Data integration ensures safe data transfer between sources and destinations and safeguards the data against unauthorised access, deletion, and change by outsiders. Data must always beaccurate while being transmitted and the service provider must ensure this [1], [13]. When performing integration operations,such as synchronising data between anon-site system and a SaaS system, data isalways managed and maintained in an identical manner [1].

To guarantee data integrity, data transaction systems must adhere to the qualities with respect to atomicity, consistency, isolation, and durability. To protect data transactions and ensure data integrity, the majority of databases use ACID characteristics. Amount of data accessibility varies depending on the SLA (Service Level Agreement) [3] for each SaaS service. Many standards and authorizations, such WS-Transaction and WS-reliability [6][7], are available to manage using web services. Open, standardised APIs are used by SaaS solutions to connect to on-site systems. This makes integrations easy, quick, and affordable [5].

DATA LOCALITY

The organization's most frequent compliance problem is data location. Clients demand specific information about where their database is actually kept, what security measures are in place to secure it, how they are certified, and where the data is relocated. Data protection becomes challenging whenever information crosses international borders since laws governing data protection vary depending on the location of the data [16]18],[19].

Currently, one of Amazon's EC2 facilities is in the United States and the other is in Europe. With 36 data centres worldwide, Google App Engine has locations in several nations, including the USA, China, and others [9]. Inquire with service providers about their commitment to processing and retaining data in particular jurisdictions and whether they will contractually obligate themselves to uphold a local's privacy laws representing their clients [14].

DATA SEGREGATION

Separation of data from many users are stored on the same server, preventing client intervention. Compromises in multi-user environments present the potential for data theft via application or client code access to SaaS systems [3].

SaaS providers must ensure that physical data and application-level data are separated separately. A SaaS service must be able to distinguish data from multiple users. For Amazon, the S3 API provides both bucket-level and object-level access control [15].

Cloud providers should offer encryption methods that have been extensively evaluated by experts [14]. In such situations, SaaS providers securely provide appropriate user rights and administrative tasks. User data may reside on a single physical system containing many VM instances. Data transmission and storage should be done in a controlled manner. For secure data transmission, the provider complies with applicable protocol and security standards. Service providers should use best-of-breed cryptosystems with pragmatic strategies for building trust with SaaS users [16], [17].

DATA ACCESS

The SaaS model is consistently adaptable enough to take into account the particular policies put forth by the organisation [3].

Data Access Control for Multi-Authority Cloud Storage, as proposed by Kan Yang and Bo Zhang, is known as DAC-MACS (Data Access Control for Multi-Authority Cloud Storage). Both are suggested as efficient and secure data access control policies for cloud storage environments with multiple tenants and authorities. By utilising a token-based decryption approach, both researchers suggested a multi-authority CP-ABE decryption scheme [11].

AVAILABLE DATA

The SaaS service providers guarantee uninterrupted data access twenty-four hours a day, seven days a week. When processing data, cloud architecture must use an efficient load balancing mechanism. To scale and make data accessible with a quick reaction time, architectural and infrastructure improvements are needed [4].

Amzon.in, a retail website, was hosted on Amazon AWS API. Amazon offers retail services to several clients while also offering a variety of features in a multi-tenant environment [3].

DATA CONFIDENTIALITY ISSUE

The safety of both deliberate and unintentional illicit access to information is referred to as confidentiality. Users have the right to expect that their information will be safe from theft. It's possible that another customer changed the security settings on purpose or illegally. SaaS service providers offer reliable security measures. A third party should certify this security method [15].[22]. The Regulation of Electronic Communications Act (ECPA) Act of 1986 offers defence against unauthorised access to user information, including electronic mail. The extensive privacy protection laws provided by the ECPA ensure the privacy and security of user data [3].

AUTHENTICATION

Application service is maintained outside of company firewall in a SaaS service. Users of the application service frequently share the same account with already-used Authenticated account. When an employee leaves a SaaS customer firm, the account must be deleted or disabled, and a new user ID and password must be provided [3]. Both WS (Web Service) Federation and SAML (Security Assertion Markup Language) are widely utilised SAML being what it,the more popular of the two.A SSO (Single Sign On) solution that is implemented using a secure VPN (Virtual Private Network) tunnel is anan alternative to WS Federation and SAML. In versions 1.1 and 2.2, the widely adopted SAML standard is frequently applied.Because several proprietary improvements have been incorporated into SAML 2.0, this standard should be implemented wherever possible because it allows for the addressing of a wide range of deployment circumstances [21].

AUTHORIZATION

The method that establishes a user's access level is called authorization. The service provider needs to have safe resources to validate the user's authorisation and confirm him using a safe mechanism in a controlled manner [13]. The management of Access management must be done in accordance with user roles. Authorization for access to secure data at various levels is based on client access policies, which are periodically evaluated. Generally speaking, Application of the least privilege model, with only users and CSP (Content Security Policy) administrators having access to the privileges necessary to carry out their duties [21].

OMB addressed various issues in February 2011 and made reference to the effective implementation of a commonality evaluation and authorisation cloud computing method [23]. A unique class of STS (Security Token Service) is offered by WS Federation and provides approval decisions. Internet-based identities could used as an identical authorisation method to the person's identity with the appropriate access. These identities may be based on an individual IP address or email address. A digital signature might potentially be an effective authorization method to identify the real user; this cryptography approach is the most appropriate one. [24].

NETWORK SECURITY

A network is a channel for SaaS services to be accessed from a cloud system. Due to network vulnerabilities, hackers are drawn to it and can use these flaws to attack cloud services and steal data from cloud storage [9].

VIRTUALIZATION

A cloud idea and element is virtualization. In addition to providing functionality for resources, data separation, server virtualization, and multi-tenancy management, it also serves as a middleman between the server and the users. Virtualization is made effective by a live migration, load balancing, and real-time issues , although these features also present a frontal assault attackers such VM escape, VM hopping, and scanning for or spoofing virtual networks [54]. These advantages expose security flaws and vulnerabilities that allow hackers to exploit VM middleware to gain access to data and resources or disable service functionalities.

It is challenging to enforce security features in virtual machines. A virtualized environment supports several instances running at once. On a single host computer, several guests can run various operating systems and applications and offer separation between the access of various users. Virtualization enables users to execute a variety of applications by allowing them to construct, copy, distribute, relocate, and roll back virtual computers [36],[37],[38].

The administration of the host and visitor operating systems is the other problem. Virtual Machine Monitors (VMMs) currently available do not provide perfect machine and data isolation[4]. In order to establish a privileging for input and output activities, A modified Linux kernel is used in the open source x86 VMM Xen. KVM, a virtual machine based on the kernel, another source project, also converts embedding a Linux kernel in a VMM [46] ,[47] , [48] , [49]. In a virtual machine, managing multiple tenants is challenging. Resources and information are shared between multiple users, allowing for attacker access. It is challenging for the Network management for AWS EC2 several user profiles with different domain names, service types, and assigned IP addresses such that each one can be uniquely identified [11].

Virtual Instruction Detection System and Virtual Protection System, or vIDS/vIPS system guards against malware and spyware by gathering, analysing, and processing data from hosts to networks in order to secure virtual environments. vIDS/vIPS monitor and assess virtual network setup and network flaws to protect information and provide assurance of an unbreakable security policy with secure transactions [29].

TCCIs (Trusted Cloud Computing Infrastructures) was proposed by Hamid Banirostam and Alireza Hedayati to guarantee the accuracy and secrecy of computing that is responsible for utilising software services in a secure virtual environment [31]. Researchers are constantly working to improve performance and security in their study on virtualization management and virtualized environment security.

ENCRYPTION

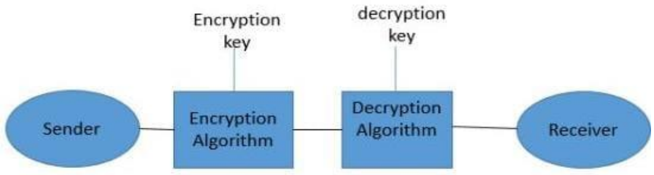
Cloud service companies utilise cryptography to process data securely. Cloud providers should utilise cryptographic methods and products for secure data transmission whenever data is being transported across a network. In a cloud computing setting, cryptographic key management is complicated, and there are currently no suitable tools for key management [5]. SaaS service providers employ SSL technology to encrypt the connection between the application and the user data base instance. When a database instance is provisioned for MySQL and SQL Server, RDS prepares an SSL certificate and installs it [11]. To safeguard resources and data

when exchanging data in a multi-tenant context, a highly scalable encryption technique is required [15]. Encryption techniques have a crucial component. A important component of encryption methodology is its ability to solve problems. (A) A secure comparison mechanism that is effective.(b) An effective delegation mechanism for encryption.(c) A productive delegation mechanism for decryption.(d) Computation over authenticated/encrypted data [17, 18].

Three algorithms were suggested for data security algorithms by .

Cryptography Encryption and decryption algorithm

Although one of the most popular methods for securing data transmission is cryptography, it still lacks some security measures. Although much work has previously been done on key management and cryptography theory, much more has to be done on cryptography methods [30]. In order to maintain their reputation in the cloud market, cloud storage companies do Data security issues include data leakage, forgery attacks, and replacement attacks. A cloud storage system ought to have TCCP and SSL support [55].



Fig; 1

The message can now be encrypted using one of the most fundamental methods of encryption, "Caesar's Cypher" (sometimes referred to as a shift cypher).

With this cypher, we simply move each letter a specific number of spaces up or down the alphabet.

A = D, B = E, C = F, D = G, E = H, F = I, and so on.

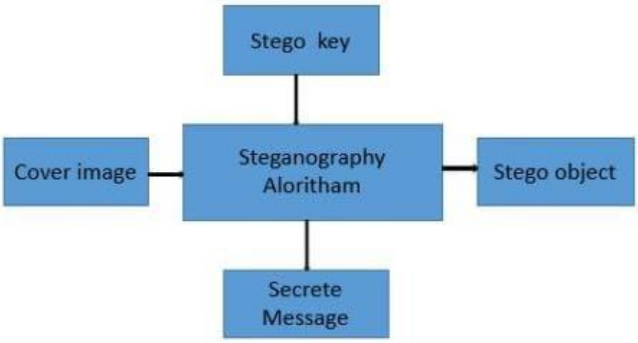
When we apply this cypher, our plaintext "Hello" becomes the ciphertext "Khoor."

To the untrained eye, "Hello" and "Khoor" are not similar. The message's contents could be easily deciphered by a beginner cryptographer, though, if they were familiar with Caesar's encryption.

Kan Yang, Xiaohua Jia, Kui Ren, and Bo Zhang's concept for data access with security measures This proposed method is referred to as DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), which is an effective and secure data access control strategy for multi-authority cloud storage systems. It was also advised to use a brand-new multi-authority CP-ABE (Ciphertex Policy Attribute-based Encryption) system with efficient decryption [32].

2): Steganography Encryption and decryption algorithm

Steganography is typically understood as a technique for concealing hidden communications or their presence such that they go unnoticed or undetected. Steganography has a number of benefits over cryptography, including the ability to hide the existence of a secret message and the prospective secret message's inability to draw attention to itself as a security measure. Today's steganography, however, is far more advanced and enables users to conceal substantial amounts of data within image, audio, and video files. These types of steganography are frequently employed with cryptography so that the information is double secured; first, the secret message is encrypted and then buried so that an adversary must first uncover the information(a process that is frequently challenging) and then decrypt.



Fig; 2

AES (Advanced Encryption Standard) Encryption algorithm and decryption

The Advanced Encryption Standard (AES), a block cypher with a block length of 128 bits, is a cryptographic algorithm. It supports keys with three distinct key lengths: 128, 192, or 256 bits. The main difference between using a key length other than 128 bits and using a key length of 128 bits in this research is that the key generation from the key is scheduled differently in AES.

For 128-bit keys, the encryption procedure takes 10 rounds; for 192-bit keys, 12 rounds; and for 256-bit keys, 14 rounds. Except until the last round, every round is the same.

Each processing round consists of a single-byte based replacement step, a column-wise mixing step, a row-wise permutation step, and the round addition.

The four phases of the Advance Encryption Standard (AES) are as follows:

Byte Replacement , Switch Rows , Blend Column , Insert Round Key Before any of them, the input block is first organised into a 4x4 byte array and then XORed with the 128-bit.

You encrypt a 128-bit block using the AES procedures below:

Step1: From the cypher key, create the set of round keys.

Step2: Provide the block data (plaintext) as the state array's first value.

Step3: The starting state array should now include the initial round key.

Step4: Carry out nine iterations of state modification.

Step5: Execute the eleventh and last state manipulation.

Step6: Make a copy of the final state array using the ciphertext for the encrypted data.

Although the Advanced Encryption Standard (AES) is one of the best methods for securing data transmission, it still lacks some security mechanisms. Cryptographic algorithms include block cyphers, which have blocks of 128 bits. It accepts keys with one of three different key lengths, either 192 or 256 bits. Analysis and simulation findings provided by Kan Yang, Xiaohua Jia, Sahai and Waters, who first developed the Attribute-based Encryption (ABE) method, show that our proposed data access control technique is secure in the random oracle model. Using our attribute revocation strategy, both forward security and backward security may be efficiently obtained [34].

CURRENTLYSOLUTION SCHEME PROVIDERS, ACTANDCERTIFICATE

The Cloud Cube Model also draws attention to the difficulties associated with comprehending and relating cloud models to control frameworks and standards like ISO/IEC 27002, which offers "a series of guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization [14]." CSA is a group headed by a collaboration of business owners, associations, and other interested parties.

Verilog is used to implement the AES algorithm.It has been done to simulate the encryption and decryption of the 128-bit AES method. In this simulation, the 128-bit data SATHYABAMA is taken to be the plain text. The simulation has been given a 128 bit key. The key and the plain text are inputs into the encryption process. Both the plain text and the key will be encrypted using the AES method at every stage. Figures 4 and 5 display the simulation graph for the AES algorithm's encryption and decryption. MTBAOHYBAA is the result of the encryption method. The decryption process receives this text and a 128-bit key as input.

The AES algorithm will go through all the decryption stages with the cypher text and the key. We can get the original plain text after decoding. The AES algorithm operates more quickly when pipelining registers are used.

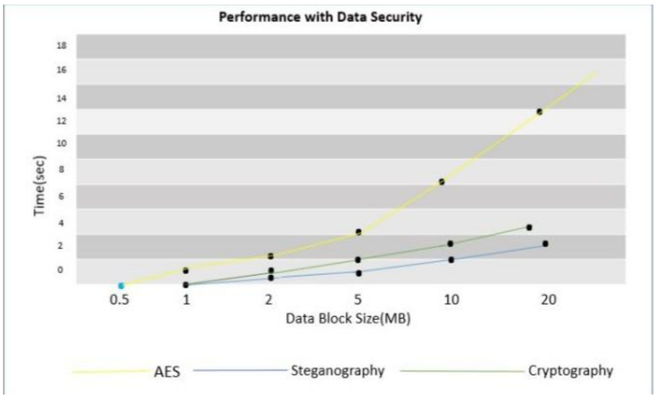


Fig.3 Data Security

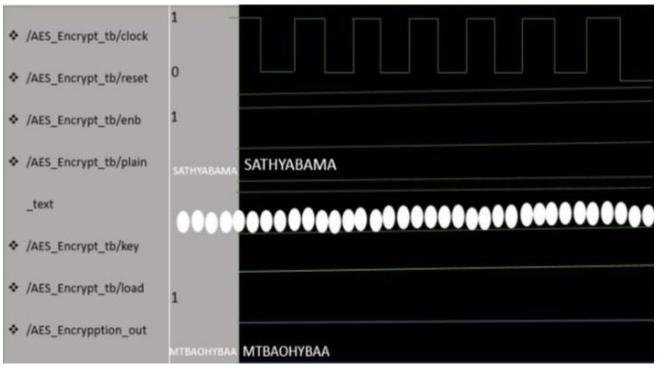


Fig.4 AESEncryptionresult.

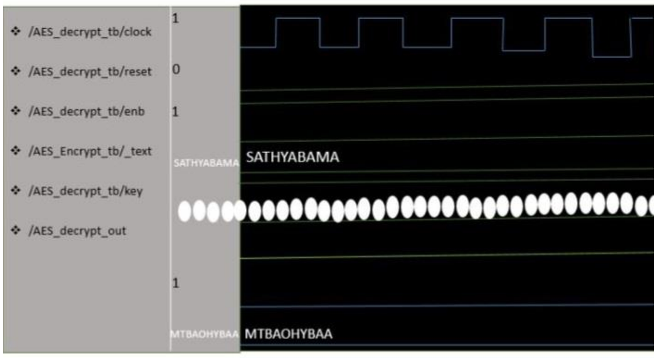


Fig.5 AESDecryptionresult

REFERCES

[1] DavidS.Linthicum,"ApproachingSaaSIntegrationwithDataIntegrationBestPracticesandTechnology,",WhitePaper2009.

[2] PaulMeinl,"SoftwareasaService–CorrectConclusionofContracts2ndenhancededition,ITClusterVienna |CloudComputingGroup,".

[3] Subashini, Subashini, and V. Kavitha. "A survey on security issues inservice delivery models of cloud computing." *Journal of Network and*ComputerApplication34.1(2011):1-11.,www.elsevier.com/locate/jnca.

[4] "SecuringSaaSApplications:ACloudSecurityPerspectiveforApplicationProviders,"LeoTechnoSoftPvtLtd.

[5] "Smart QuestionsForYour SaasVendor," ASAManageeBook,

[6] Kumar,Prashant,andLokeshKumar."SecurityThreatstoCloudComputing."InternationalJournalofIT,EngineeringandAppliedSciencesResearch(IJIEASR) Volume2,No.1,December2013,

[7] Subashini, Subashini, and V. Kavitha. "A survey on security issues inservice delivery models of cloud computing." Journal of Network andComputer ApplicationsVol34,pp.1-11,2011.

[8] GonzalezNelson,MiersCharles,RedıgoloFernando,SimplıcioMarcos, Carvalho Tereza , Naslund Mats , and Pourzandi Makan ,2012.A quantitative analysis of current security concerns and solutions forcloud computing ,AJournal of Cloud Computing: Advances, SystemsandApplications2012,1:11

[9] Zetta, "Zetta: Enterprise cloud storage ondemand,"http://www.zetta.net/,2008.

[10] Ma D.,"Cryptographic Approach for Delegation and Authorization inCloudComputing,"PresentationatNSF WorkshoponSecurityforCloudComputing,March14-16,2012.

[11] Sahai,Amit,andBrentWaters."Fuzzyidentity-basedencryption."In *Advances in Cryptology–EUROCRYPT 2005*, pp. 457-473. SpringerBerlinHeidelberg,pp.457–473,Springer2005.

[12] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computingsecurity issues." Future Generation Computer Systems, Vol 3, pp 583-592,2012.

[13] Kandukuri,BalachandraReddy,V.RamakrishnaPaturi,andAtanuRakshit. "Cloud security issues." In Services Computing SCC'09. IEEEInternationalConferenceon,pp.517-520.IEEE,2009.

[14] Chen, Deyan, and Hong Zhao. "Data security and privacy protectionissuesincloudcomputing."In ComputerScienceandElectronicsEngineering (ICCSEE),International Conference on, vol. 1, pp. 647-651.IEEE,2012.

[15] Cloud Security Alliance. Security Guidance for critical areas of focus incloudcomputingVersion2.1.2009.

[16] A.Karger,"I/O for Virtual Machine Monitors: Security and performanceissue,"IEEESecurityandprivacy,September/October2008.

[17] Kandukuri,BalachandraReddy,V.RamakrishnaPaturi,andAtanuRakshit. "Cloud security issues." In Services Computing, SCC'09. IEEEInternationalConferenceon,pp.517-520.IEEE,2009.

[18] Badger,Lee,TimGrance,RobertPatt-Corner,andJeffVoas. CloudComputing Synopsis and Recommendations: Recommendations of theNationalInstituteofStandardsandTechnology.CreateSpaceIndependentPublishingPlatform,2012.

[19] Brunette, Glenn, and Rich Mogull. "Security guidance for critical areasoffocusincloudcomputingv2.1." CloudSecurityAlliance pp1-76,2009

[20] García-Valls,Marisol,TommasoCucinotta,andChenyangLu."Challengesinreal-timevirtualizationandpredictablecloudcomputing." Journal of Systems Architecture Vol 60, no. 9, pp 726-740,2014.

[21] “Security Recommendations for Cloud Computing Providers,” WhitePaper,Federalofficeofinformationsecurity.

[22] Jansen, Wayne A. "Cloud hooks: Security and privacy issues in cloudcomputing."In SystemSciences(HICSS),44thHawaiiInternationalConference on,pp.1-10.IEEE,2011.

[23] Hashizume, Keiko, David G. Rosado, Eduardo Fernández-Medina, andEduardoB.Fernandez."Ananalysisofsecurityissuesforcloudcomputing."Journal of Internet Services and Applications 4, Vol 1, pp1-13.2013