Investigational Analysis of Security Measures Effectiveness in Cloud Computing: A Study

Vijay.G.R
PhD Scholar, Dept. of CSE J.N.T.U.A, Anantapuramu A.P, India ,Email:-vijay.gcr@gmail.com

Dr.A.Rama Mohan Reddy
Professor, Dept. of CSE S.V.U College of Engineering, Tirupati, A.P, India Email:-ambatiramamohanreddy@gmail.com

Abstract

In the modern era of business operation, the technical adoption of cloud services are high on rise by the large scale to small scale business establishment on various products and services. Needless to say that with the rise of adoption also gives birth to security concerns as cloud runs on common internet which are also used by trillions of internet-users. There are various means by which introducing a malicious program inside the cloud is not that complicated task for attacker. The various services providers as well as past researcher have introduced some of the potential security features which is claimed to be highly effective. However, accomplishing fail-proof security systems in cloud is never witnessed nor reported by any user or researcher, which clearly specifies that security problems do persist and are on exponential rise. Therefore, this paper discusses about the security issues in cloud supported by brief description of standard security models currently available in cloud. With extensive literatures on the existing security solutions, a significant research gap is explored in robust authentication system in cloud services.

Keywords-component; Security, Cloud Computing,attacks, security models

INTRODUCTION

Cloud computing is a state of the art computing model in which the computing resources for example; software, hardware, databases and data are accessed as a service usually through a web browser or light-weight desktop machine over the internet [1]. A typical cloud is a pool of commuting resources such as servers, application development platforms, storage devices, load balancers and virtual machines that are shared among cloud users. Cloud computing also suffers from a lot of security issues and threats that can outlaw the entire cloud to function; hence posing a serious question mark on the cloud handiness and security [2]. On the other hand, these issues are truly opportunities to further enhance the cloud to make it more alive, productive and secure by implementing the state of the art and refined security measures. A distinctive cloud is affected by different issues like Denial of Service (DOS) attacks, session hijacking threats, flashing attacks, failing to obey governmental regulations and data confidentiality issues [3]. The issues such as DOS attacks, malware injection, hijacking of a server or a specific service and user identity theft are very common [4]. Network sniffing is yet another severe threat in which a packet sniffer can steal protected data which may include session cookies, users' passwords, UDDI (Universal Description Discovery Integrity) files and WSDL (Web Service Description Language) [4]. SQL injections to execute an always true statement in a query to get all the tables back can harm a cloud by unauthorized access to users´ data [4]. These issues can seriously distress the use of a cloud as cloud users do not want to share their secret information with anyone especially with their business contenders [5]. By comparing the uses of cloud computing with traditional networking model one can effortlessly decipher the supremacy and technical superiority of cloud computing over the outmoded networking techniques, on the other hand the threats attached to cloud computing are, however, of an extreme nature [4]. These threats are essentially compelling numerous users not to use cloud services in present time because the consequences of such security issues can be tremendously severe to any business entity and can even result in a total cessation of a pretentious entity [5]. Due to these actualities, several measures have been being taken to safeguard cloud security, few of them are Virtual Private Cloud (VPC) by Amazon, Firewalls, unscrambling the host administrator and cloud administrator in defining security, the use of HTTPS protocols, competent encryption algorithms, monitoring the information stream and conformance to the multi-layered security shields [3]. Several security management standards and measures have been intended to safeguard the cloud but nevertheless cloud security is at a high risk due to the innovative hacking techniques. These security standards comprise of Information Technology Infrastructure Library (ITIL) guidelines, ISO/IEC 27001/27002 standard and Open Virtualization Format (OVF) standards [6]. The dark side of this picture is that; despite having such measures we cannot promise cloud security. This hard reality has two explanations; one is the weaknesses in these security routines currently adopted all over the globe and secondly the innovative hacking techniques that are quickly becoming extraordinarily intelligent, sophisticated and hard to detect. A lot of other measures are also being undertaken by different cloud venders but are themselves, not flawless [5]. Section 2 discusses about the security issues in cloud followed by in-depth investigation on existing security model in cloud services from past literatures in Section 3. Section 4 discusses about the related work followed by research gap in Section 5. Section 6 concludes the paper.

SECURITY ISSUES IN CLOUD

At the present system, it is seen that majority of the operations of small businesses are migrated to cloud computing by joining up with private providers that make sophisticated applications more affordable as well as setting up their own accounts with public social networking applications. The ways of functioning of private and public clouds are almost equivalent i.e. applications are hosted on a server and accessed by client over the Internet. Majority of the corporate are dependent on the trust of third party vendor only for storage of their data, applications or sensitive intellectual property on cloud. In the present market, although the service offered by the cloud service provider ranges from highly paid services for premium client to cost effective services for small clients. However, as majority of the small clients have started adopting clouds for their business, it is not free from risk or potential threats to data security. In a nutshell, the cloud service provider cannot actually ensure data security and authentication system to clients always, as their services are hosted over internet. Therefore, the significant issues that raises up due to adoption of cloud services by clients are briefed as follows:

- **Highly Insecure Data Transfer:** The services of the cloud service provider is usually done using internet which is infected by innumerous malicious program in various shape and size. Hence, providing sufficient protection for a single cloud user is almost equivalent to a single non-cloud user. All the security problems that can possibly victimize a non-cloud user are equally applicable for a paid cloud user too. If the data used by the user are not properly encrypted and robustly authenticated using efficient protocols like IPSec, the degree of susceptibility is on rise.
- **Vulnerable Interfaces:** It is well known that due to adoption of weak and sufficiently not strong interface, the cloud user encounters sufficient vulnerability. Depending on less insecure interfaces and APIs exposes organizations to a numbers of security issues pertaining to integrity, non-repudiation, accountability, availability, confidentiality etc.
- **Insecure data:** Although the cloud computing infrastructure is usually very secure, it is also a very tempting target for the criminal underground. All public clouds have been engineered with cloud computing security as one of the top concerns. Any such vulnerability reported or not, in your chosen cloud, might put the entire data at risk. In the "old world", infrastructural vulnerabilities sometimes actually pose a critical risk, but often are hidden behind multiple layers of security devices, both physical security and network/OS security.
- **Breach notification and data residency**: Not all data requires equal protection, so businesses should categorize data intended for cloud storage and identify any compliance requirements in relation to data breach notification or if data may not be stored in other jurisdictions. Data management at rest Businesses should ask specific questions to determine the cloud service provider's data storage life cycle and security policy. Businesses should find out if: Multitenant storage is being used, and if it is, find out what separation mechanism is being used between tenants. Mechanisms such as tagging are used to prevent data being replicated to specific countries or regions. Storage used for archive and backup is encrypted and if the key management strategy includes a strong identity and access management policy to restrict access within certain jurisdictions.
- **Data Protection in Motion**: It is seen that businesses always encrypt sensitive data in motion to the cloud, but if data is unencrypted while in use or storage, it will be incumbent on the enterprise to mitigate against data breaches. However, the existing clients still encounters security issues of data protection while in motion.
- **Robust Authentication:** Interestingly, the authentication mechanisms of the existing cloud users are similar to that of non-cloud users in majority. This raises a question that why the cloud services didn't provided a different security access schemes different from conventional access schemes. It is suggested that they must ensure access management controls are in place that will satisfy breach notification requirements and data residency. If keys are managed by the CSP, then businesses should require hardware-based key management systems within a tightly defined and managed set of key management processes. When keys are managed or available in the cloud, Gartner says it is imperative that the vendor provides tight control and monitoring of potential snapshots of live workloads to prevent the risk of analyzing the memory contents to obtain the key.
- **User access control.** Data stored on a cloud provider's server can potentially be accessed by an employee of that company and the user have none of the usual personnel controls over those people.
- **Data separation.** Every cloud-based service shares resources, namely space on the provider's servers and other parts of the provider's infrastructure. However, efficiencies of the compartmentalization approaches, such as data encryption, the provider uses to prevent access into the virtual container by other customers are very rare.

With the advancement of cloud services and their delivery models, the potential risks of security are also on constant rise. Although conventional cryptographic techniques are used in majority of the networking application, but the cloud environment will requires significant data to be remotely processed in plaintext. For effective mechanism of the security implementation in cloud, it calls for some of the effective authentication mechanism to manage securely the data accessed over time. One of the biggest impediments of developing an effective security system on authentication is that conventional approaches of security are not directly applicable as the cloud storage contains large number of aggregated data for the purpose of processing. It may be impractical to hash entire datasets or else one would have to bear great computational and communication overheads [7]. Moreover on cloud environments, trust issues arise because a customer infrastructure resides at an off-site foundation and is controlled by a second- or third-party entity. These two attributes imply a human factor not known to customers to interact with the infrastructure.

SECURITY MODELS IN CLOUD

The brief illustration of available cloud security models are:

- **Cloud Multiple-Tenancy Model of NIST**: Multiple-tenancy [8] is an important function characteristic of cloud computing that allows multiple applications of cloud service providers currently running in a physical server to offer cloud service for customers. Multiple-tenancy model of cloud computing implemented by virtualization offers a method to satisfy different customer demands on security, segmentation, isolation, governance, SLA and billing/chargeback etc [9].

- **Cloud Risk Accumulation Model of CSA**: Understanding the layer dependency of cloud service models is very critical to analyze the security risks of cloud computing. IaaS is the foundation layer of all cloud services, PaaS is built upon IaaS and SaaS is built upon PaaS, so there is an inherited relation between the service capability of different layers in cloud computing. Similar to the inheritance of cloud service capability, the security risks of cloud computing is also inherited between different service layers [8]. i) IaaS provides no distinctive function similar to application service but maximum extensibility for customers, meaning that IaaS holds little security functions and capabilities except for the infrastructure’s own security functions and capabilities. IaaS demands that customers take charge of the security of operating systems, software applications and contents etc. ii) PaaS offers the capability of developing customized applications based on the PaaS platform for customers and more extensibility than SaaS, at the cost of reducing those available distinctive functions of SaaS. Similarly, the intrinsic security function and capability of PaaS are not complete, but customers possess more flexibility to implement additional security. iii) SaaS presents the least customer extensibility, but the most integrated service and the highest integrated security among three service layers. In SaaS, cloud service providers take charge of more security responsibilities, and customers pay for little security effort on the SaaS platform. One critical feature of cloud security architecture is that the lower service layer that a cloud service provider lies in, the more management duties and security capabilities that a customer is in charge of. In SaaS, cloud service providers need to satisfy the demands on SLA, security, monitor, compliance and duty expectation etc. In PaaS and IaaS, the above demands are charged by customers, and cloud service provider is only responsible for the availability and security of elementary services such as infrastructure component and underlying platform [9].

- **Jerico Formu’s Cloud Cube Model**: Jerico formu’s cloud cube model is a figuration description of security attribute information implied in the service and deployment models of cloud computing and the location, manager and owner of computing resources [9].

- **The Mapping Model of Cloud, Security and Compliance*:*** The mapping model of cloud ontology, security control and compliance check presents a good method to analyze the gaps between cloud architecture and compliance framework and the corresponding security control strategies that should be provided by cloud service providers, customers or third parties [8]. Unfortunately, the compliance framework of cloud computing is not naturally existed with the cloud model. Correspondingly, the mapping model of cloud, security and compliance contributes to determining whether accept or refuse the security risks of cloud computing [9].

- **Data Security based on Diffie Hellman and Elliptical Curve Cryptography:** The authors [10] have discussed a design for cloud architecture which ensures secured movement of data at client and server end. The non breakability of Elliptic curve cryptography is used for data encryption and Diffie Hellman Key Exchange mechanism for connection establishment. The encryption mechanism uses the combination of linear and elliptical cryptography methods. It has three security checkpoints: authentication, key generation and encryption of data.

- **User Authentication, File encryption and Distributed Server**: The authors [11] have discussed security architecture for cloud computing platform. This ensures secure communication system and hiding information from others. AES based file encryption system and asynchronous key system for exchanging information or data is included in this model. This structure can be easily applied with main cloud computing features, e.g. PaaS, SaaS and IaaS. This model also includes onetime password system for user authentication process. The work mainly deals with the security system of the whole cloud computing platform.

- **Trusted Computing Technology**: The author [12] proposed a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system. A model system is discussed in which cloud computing system is combined with trusted computing platform with trusted platform module. In this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.
- **Identity-Based Cryptography**: The authors in [13] introduced a Hierarchical Architecture for Cloud Computing (HACC). Then, Identity-Based Encryption (IBE) and Identity-Based Signature (IBS) for HACC are proposed. Finally, an Authentication Protocol for Cloud Computing (APCC) is presented. Performance analysis indicates that APCC is more efficient and lightweight than SSL Authentication Protocol (SAP), especially for the user side. This aligns well with the idea of cloud computing to allow the users with a platform of limited performance to outsource their computational tasks to more powerful servers.

Apart from the above standard cloud model, the recent years (2009-2014) has witnessed evolution of various models by prior researchers attempting to solve the security issues in cloud authentication system. Table 1 highlights the list of significant contributions of the past authors for the purpose of enhancing the security in cloud.

Table 1 Summary of Significant Security Models evolved in recent years.

Authors/Pub/Year	**Model Name**	**Issues Addressed**	**Techniques Applied**
Chow et al [14]-ACM-2010	TrustCube	To manage the authentication infrastructure	Learning Algorithm
Park et al [15]-IEEE-2012	THEMIS	Security on Billing System	PKI based authentication
Ahmad et al. [16]-IJAST-2012	Trust Model	Trust between cloud provider & user	Trust and SLA based technique
Tang & Sandhu-[17]-IEEE-2013	CTTM (*cross-tenant trust model*)	Authentication & authorization	Graph theory
Wang et al.-[18]-Elsevier-2012	Cloud-DLS	problems of evaluating direct and recommendation trust degree based on Bayesian method	Trusted Dynamic Scheduling Framework
Asghar et al. [19]-Elsevier-2013	$\text{ESPOON}_{\text{ERBAC}}$	Data confidentiality	Policy based management
Hamlen et al [20]-IEEE-2013	Policy Enforcement Framework	Security and privacy issues	Semantic aware policies
Waizenegger et al. [21]-Springer-2013	Policy4TOSCA	Cost and security for automated provisioning	Policy based management
Habib et al. [22]-IEEE-2013	Trust Aware Framework	Trust for security controls	Hard & Soft Trust Mechanism
Bykov et al. [23]-ACM-2011	Orleans	Scalability & Security	Grain Model and Activation
Noor & Sheng-[24]-Springer-2011	Trust as a service	Trust issues in cloud	Adaptive credibility model
Kamongi et al. [25]-IEEE-2013	VULCAN	Analysis of vulnerabilities & mobile environments	Ontological approach
Tetali et al. [26]-ACM-2013	MrCrypt	Data Confidentiality	Homomorphic encryption scheme
Gadaleta et al. [27]-IFIP-2012	HyperForce	Protection of virtualized OS	Security critical code
Wei et al. [28]-IEEE-2009	SecureMR	Integrity of data	scalable decentralized replication-based verification scheme
Lu et al. [29]-ACM-2010	BLADE	Mitigating drive by download malwares	Hardware based approach
Gao et al. [30]-IEEE-2013	TrPF	Privacy preservation	Graph theory

		issues	
Hyuk [31]- UCS, 2012	HUC-HISF	Security issues	Security protocols & users privacy.
Balajee [32]-IJCST-2011	IPVDD	Intrusion issues in virtual data centers (service hijacking)	Color chart approach
Accorsi [33]-Elsevier-2013	BBox	Remote auditing in distributed system	Public key cryptography

RELATED WORK

After reviewing the standard models of the security applicable in cloud in the previous section, it has been seen that authentication and authorization techniques are not emphasized much as majority of the techniques are equipped with cryptography or policy based approach. Hence, literatures pertaining to the standard authentication system are referred to understand their potential features and its applicability on cloud. This section discusses about significant prominent individual research work performed by the prior researcher and their respective interpretation of results and techniques applied.

The author [34] has presented a unique technique that uses public key infrastructure for mitigating authentication issues. According to the author, even authentication based scheme is not completely secure and robust with potential proneness to vulnerability towards confidentiality and integrity. The author has used session identifier and random value using the potential of cryptographic hash function thereby ensuring better integrity in this modified authentication based scheme approach. The prime advantage of this technique is that it offers better resiliency against birthday attacks and hash Collision Problem. However, one of the major issue in this approach is the system performs complicated stages of encryption due to its target mitigation factor that forces the system to consider public key infrastructure. Hence, the system cannot be termed as totally cost effective and reliable when it comes to algorithm time and space complexity.

The author [35] has introduced a technique called as 'Noisy Password' technique after visualizing the potential capability of authentication based scheme and demerits of static password. The technique applied by the author endeavor to render the password as of no operational use for the purpose of addressing shoulder surfing and eavesdropping issues over the network. According to the scheme, the user is furnished with unique password at the time of accessing their resources. The outcome of this technique shows better mitigation approach against any types of illegitimate intrusion over the insecure public network. However, the technique is shrouded by some specific flaws as the system gives more stress on authentication scheme where the authorization scheme is not addressed to that extent. The existence of error rates in the scheme is also additional issues over the reliability of the technique.

According to this scheme, the author [36] mechanizes the technique based on Diffie-Hellman problem that deploys dynamic password for enhancing the security of authentication token using authentication based scheme. The authors adopts a technique where smart card is used on the basis of bilinear pairing for provide extended security over existing password scheme and mitigation against identity attack and forgery attack. In-depth analysis of the scheme also exhibits that it has time complexity which makes the system vulnerable for other types of potential attacks (Denial of Service) which are not considered in the study. Moreover, the authentication and authorization scheme is very robust only at the time of user-enrollment on their system, which reduces when the number of the access is increased on multiple insecure public network.

The author [37] has presented a unique authentication system that uses volatile password like static authentication based scheme. The interesting approach of this work is that the author also considers usage of time and location data of the user having a possession of the trusted handheld device using the in-built GPS features on the mobile devices. One of the prime advantage of the scheme is that authentication is based on new features (time/location) which is GSM based data and authorization approach is both time and space compliant in algorithm implementation. According to the technique, the validation of the volatile password is done with respect to the time and location of the user requesting for accessing new data through their handheld devices. The authentication fails if the users (even if they are legitimate) are not in specified territory. However, the systems also have some potential threats when accessing such services via GPS. It is quite known that GPS services on mobile devices are usually assisted by free services, where the positioning is not that accurate. Hence, two different users on the same territory may share the same location information and thereby posing potential threat to the authentication scheme by itself.

The approach discussed by author [37] in this work is more on operational management of authentication based scheme and less on enhancement of security schemes. The author uses a technique where the legitimate user is furnished with one static password which can be used for accessing multiple internet services using the principles of authentication based scheme for the purpose of authentication. The work is no doubt good in terms of usability as users don't need to memorize multiple passwords for multiple applications which use authentication based scheme principles. However, there are some serious security threats to this approach due to usage of one common static password for multiple applications. If the user is in public network, then tracking down users accessing behaviour and URLs, it is possible to design an algorithm which can perform cryptanalysis of the intermediate key between static and authentication based scheme.

The author [38] has presented a work towards secure authentication in mobile banking system by introducing multi-model parameters to perform the authentication of a user. According to the adopted technique, author discussed that if the authentication of a legitimate user of mobile banking is done considering a biometric attribute of user and authentication based scheme, the system can be rendered more secure and highly difficult to bypass the security algorithms. The technique allows user to receive a password with session validity limitation, which after feeding to the primary authentication server, ask for biometric traits of user. Once the biometric trait of the user is furnished, the authentication is performed. After the authentication is successfully accomplished from authentication server, the legitimate user can perform secure transaction. Although the process discussed and tested by the author is claimed secured enough, but in reality it suffers from various loopholes. The first issue is every user end device will require having specific hardware to read the biometric traits which are expensive in nature and usually bulky. The second issue is that the author has not discussed much security of biometric template itself, which if compromised can lead to exposure of security protocol to the intruders. Third, the algorithm discussed is quite computationally time consuming in nature, which leads to the system much exposed to some potential threats like routing attacks and replay attack.

The author [39] has introduced a new authentication based scheme using PingPong128 Stream Cipher for the purpose of enhancing the security of authentication system for the legitimate users. The author uses a technique where LM-generators are considered for the purpose of mitigating attacks against summation generators and other types of clock controlled keystream generators. However, the technique is pretty outdated as many sophisticated cryptographic technique of authenticating the user based on timestamp already existed. Moreover, the stream cipher is already shrouded by multiple security problems which poses threat to the reliability of the work discussed here.

The author [40] in this work has specified one of the interesting security protocol designs that don't use cryptography for the purpose of authentication and hence this work has attracted for being reviewed. The author has applied a technique of enhancing one prior scheme called as 'ColorPallete' which was explored with possible security loopholes. The outcome of the experiment was found to be satisfactory only on the ground of enhancing the new scheme against possible threats of unintentional access by user. However, we strongly feel that although the system is cost-effective due to absence of cryptographic technique, but the system doesn't exhibit privacy, confidentiality, and integrity in authentication scheme.

RESEARCH GAP

The proposed investigational study have selected papers from well-ranked scientific journals and conferences or symposiums, all of them indexed by digital scientific databases such as the Association for Computing Machinery (ACM) Digital Library, Elsevier, the Institute of Electrical and Electronics Engineers (IEEE) Xplore and Springer. Additionally, the discernment resulting from the revision work is filtered out a few works that were less interesting. The studies that are not pertaining to cloud security were excluded. The literatures presented in this manuscript have an indirect impact on the cloud computing paradigm and its security. After reviewing the above literatures, following are the research gap explored:

- In the process of exploring various techniques adopted in past and even existing system, it was found that usage of authentication based scheme are highly adopted and seems to guarantee better security in access management in public as well as private network. Authentication based scheme are also found to be valid for only one attempt of access while trying to make a unit of transactions. One of the obvious advantages of using authentication based scheme is its fail-proof security towards replay attack which means that unique password once generated will never be repeated for second time and hence if the password is in possession of attacker, it will be of no use. Thereby usage of authentication based scheme has been investigated to explore a better possibility of make further more secure system in user authentication. Various authentication based scheme technologies are also seen patented however standardization of the authentication based scheme technique is challenging step due to its diverse format of usage and architecture proposed by many previous researchers and protocol makers.
- Although there are multiple sets of research publication done in past, as evident from previous section, for the purpose of enabling security in two factor authentication systems in past, but effectiveness of all these

techniques are yet to be proved. A malicious event occurrence results in the cost of user system account. Even if the security of the individual user may be highest but the system may already be in risk. All of the research work carried out in past as discussed in the previous section has only focused on initial level of verification using two factor authentication system which eventually is not used after the user is successfully verified and accesses for the second time. Especially the studies carried out in [41][38] have stressed on the illegitimate attempt of intrusion. We strongly believe that stressing on primary access level to create a potential security system cannot be reliable in long run as multiple malicious programs can eventually corrupt the security policy in future and successfully steals the user identity. None of the above mentioned studies has stressed on security priviledge escalation where the probabilities of malicious activities are always maximum and it initiates from normal access of any user. And if such malicious event successfully incorporates within the system, the user will never able to explore the root location of malicious program to perform quarantine.

- Eventually, it can be seen that after the 1st phase of the two factor authentication is performed, it becomes usual authentication approach just like conventional user-ID and password based authentication system. However, various prior studies have already proved the weakness of password based authentication system. The most potential attacks are explored as discovery attack, brute force attack, and social engineering attack. However, two factor based authentication system are also shrouded by security loopholes. It is very clear that two factor authentication systems cannot furnish a complete security to its user. Although two-factor based authentication system furnishes a layered protection but it is 100% not capable of circumventing all the potential threats on the network. In order to have clear visualization of the open issues in two-factor authentication system, we will attempt to understand the usual techniques adopted by illegitimate users to access the resources even where two-factor authentication is used. Two-factor authentication uses multiple devices to process or store or generates some of the password i.e. mobile phone. Hence, it can be said that availability of the two-factor devices cannot be ensured in the case of stealing events.
- Man-in-Middle attack is another possible scenario which was not considered in the previous studies. Such types of attack scenario uses an illegitimate proxy server positioned within the communication channel and authentication server. At the event of service request, when the authentication token is generated, the token passes via the insecure routes directing the sensitive information to the intruder. Once the data is stolen, the intruder can easily configure the entire authentication system, and from hence onward, the intruder can have permanent access on the resources. Such types of attack scenarios are not found to consider in the past studies posing as open issues.

Hence, it can be seen that the cloud security model described so far is schematized, where it is possible to discriminate possible attack vectors. Although usage of services under cloud domain is on rise, but still the literatures were found to use conventional security techniques in hybrid manner to superimpose security profiles in cloud. Hence, there is a potential research gap found for effective authentication based mechanism that ensures better data security with fail-proof privacy, confidentiality, non-anonymity, and non-repudiation.

CONCLUSION

The chapter has presented the explicit discussion of the prior research work that has been introduced in the past for the purpose of incorporating secure authentication and authorization for any legitimate members attempting to perform secure transactions on the cloud environment. The standard security issues as well as standard model of security mitigation existing presently are also discussed. Various studies discussed in the paper have shown significant approach which has their own pros and cons along with brief highlights of research gap. Our future work direction will be to introduce a novel authentication based scheme to ensure effective security in cloud computing.

REFERENCES

B. Furht, Armando Escalante, Handbook of Cloud Computing, Springer, 2010

K. Hamlen, Murat Kantarcioglu, Latifur Khan, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), vol. 39, pp. 39-51, 2010

D. Jamil, & H. Zaki., Cloud Computing Security. International Journal of Engineering Science and Technology, vol.3, Iss.4, pp.3478-3483, 2011

B.C. Brown, B.C. Brown, How to Stop E-mail Spam, Spyware, Malware, Computer Viruses, and Hackers from Ruining Your Computer Or Network: The Complete Guide for Your Home and Work, Atlantic Publishing Company, 2010

D. Zissis, & D. Lekkas, Addressing cloud computing security issues. Future Generation Computer Systems, Elsevier ,vol. 28, Iss. 3, 2012

K.D. Kadam, S.K. Gajre, & R.L. Paikrao, Security issues in cloud computing. International Journal of Computer Applications, 2012

K.Hashizume, D.G Rosado, E.F.-Medina, and E.B.Fernandez, “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications, 2013

Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing(v2.1). Decemeber, 2009.

J.Chea, Y.Duanb, T.Zhanga, J.Fana, “Study on the security models and strategies of cloud computing”, International Conference on Power Electronics and Engineering Application, Elsevier, 2011

N. Tirthani, R. Ganesan, Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography, IACR Cryptology, 2014

K.W.Nafi, T.S.Kar, S.A.Hoque, “A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture”, *International Journal of Advanced Computer Science and Applications*, Vol. 3, No. 10, 2012

Z. Shen, Q. Tong, “The Security of Cloud Computing System enabled by Trusted Computing Technology”, 2nd IEEE International Conference on Signal Processing Systems,2010

H. Li, Y. Dai, B. Yang, Identity-Based Cryptography for Cloud Security, Springer, 2009

R. Chow, Markus Jakobsson, Ryusuke Masuoka, Authentication in the Clouds: A Framework and its Application to Mobile Users, ACM, 2010

K-W Park, J. Han, J.W Chung, “THEMIS: A Mutually Verifiable Billing System for the Cloud Computing Environment”, IEEE Transactions on service computing, 2012

S. Ahmad, B. Ahmad, S. M. Saqib, and R. M. Khattak, “Trust Model: Cloud’s Provider and Cloud’s User”, *International Journal of Advanced Science and Technology*, Vol. 44, July, 2012

B. Tang and R. Sandhu, “Cross-Tenant Trust Models in Cloud Computing”, IEEE, 2013

W. Wang, G. Zeng, D. Tang, J.Yao, Cloud-DLS: Dynamic trusted scheduling for Cloud computing, Experts systems with Applications, Elsevier, vol.39, pp.2321-2329, 2012

M. R. Asghar, M. Ion, G. Russello, B. Crispo, “ESPOON$_{ERBAC}$: Enforcing Security Policies In Outsourced Environments”, Elsevier Computers & Security 2013.

K.W. Hamlen, L. Kagaly, M. Kantarcioglu, “Policy Enforcement Framework for Cloud Data Management”, IEEE Computer Society, 2013

T. Waizenegger, M. Wieland, T. Binz, U. Breitenbucher, “Policy4TOSCA: A Policy-Aware Cloud Service Provisioning Approach to Enable Secure Cloud,” Computing, Springer Berlin Heidelberg, 2013

S. M. Habib, V. Varadharajan, M.Muhlhauser, “A Trust-aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces”, IEEE 2013

S.Bykov, A.Geller, G.Kliot, J.R. Larus, R.Pandya, J.Thelin, “Orleans: A Framework for Cloud Computing”, *ACM Symposium on Cloud Computing*, Portugal, October 2011

T.H. Noor and Q.Z. Sheng, “Trust as a Service: A Framework for Trust Management in Cloud Environments”, Springer-Verlag Berlin Heidelberg, pp. 314–321, 2011.

P. Kamongi, S. Kotikela, K. Kavi, “VULCAN: Vulnerability Assessment Framework for Cloud Computing”, IEEE 7th International Conference on, 2013.

S. D. Tetali, M. Lesani, R. Majumdar, T. Millstein, “MrCrypt: Static Analysis for Secure Cloud Computations”, ACM, 2013

F.Gadaleta, N. Nikiforakis, J.Tobias Muhlberg, and W.oosen, “HyperForce: Hypervisor-enForced Execution of Security-Critical Code”, *International Federation for Information Processing*, pp. 126–137, 2012.

W. Wei, J. Du, T. Yu, X. Gu, “SecureMR: A Service Integrity Assurance Framework for MapReduce”, *IEEE*, 2009

L.Luy, V.Yegneswaranz, P. Porrasz, W. Lee, “BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections”, ACM, 2010

S.Gao, Jianfeng Ma, Weisong Shi, “TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing”, IEEE transactions on information forensics and security, Vol. 8, no. 6, June 2013

J.H. Park, “HUC-HISF: A Hybrid Intelligent Security Framework for Human-centric Ubiquitous Computing”, Doctorial Thesis, Ubiquitous Computing and Security (UCS) Lab, 2012

M.Balajee, C.Narasimham, “IPVDD: Intrusion prevention for virtual Data Centers (A Framework for Encryption and Decryption)”, *International Journal of Computer Science & Technology*, Vol. 2, Iss ue 4, Oct . - Dec. 2011

R. Accorsi, “A secure log architecture to support remote auditing, Mathematical and Computer Modelling”, Elsevier, 57 (2013) 1578–1591

H.C. Kim, H.W. Lee, K.S. Lee, M.S. Jun, M.S. “A Design of One-Time Password Mechanism using Public Key Infrastructure”, Fourth IEEE International Networked Computing and Advanced Information Management, vol-1, pp. 18 – 24, 2008

K. Alghathbar, H.A. Mahmoud, H.A., “Noisy Password Scheme: A New One Time Password System”, IEEE Canadian Conference on Electrical and Computer Engineering, pp. 841 – 846, 2010

S. Luo, J. Hu, Z. Chen, Z., “An Identity-Based One-Time Password Scheme with Anonymous Authentication”, International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009

M. Long and U. Blumenthal, “Manageable One-Time Password for Consumer Applications”, IEEE International Conference on Consumer Electronics, pp. 1 – 2, 2007

C.L. Tsai, C.J. Chen, D.J. Zhuang, “Secure OTP and Biometric Verification Scheme for Mobile Banking”, Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, 2012

B. Davaanaym, Y.S. Lee, H.J. Lee, H.J., “A Ping Pong based One-Time-Passwords authentication system”, Fifth International Joint Conference on INC, IMS and IDC, 2009

Y.C Yeh, W.C Ku, W.P. Chen, W.P., and Y.L. Chen, “An Enhanced Simple Secure Remote Password Authentication Scheme Without Using Cryptography”, First IEEE International Conference on Communications in China: Communications Theory and Security (CTS), 2011

W.B. Hsieh, J.S. Leu, “Design of a Time and Location Based One-Time Password Authentication Scheme”, 7th IEEE International Wireless Communications and Mobile Computing Conference, pp. 201 - 206, 2011