Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 167 (2020) 163–173

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Computational Intelligence and Data Science (ICCIDS 2019)

Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation

Gayatri S Pandi (Jain)[a], Saurabh Shah[b], K.H.Wandra[c]*

[a]*L.J.Insitute of Engineering and Technology and C.U.Shah University, Ahmedabad, Gujarat,India*
[b]*Director C. U.Shah University, Surendranagar,Gujarat, India ,*
[c]*Director Gujarat Marine Board, Gujarat,India*

Abstract

Cloud computing environment offers many services which have attracted the criminals or oppugners to commit cyber-crimes in a more sophisticated manner. Most of the crimes conducted by the criminals are data tampering, spam assaults, distributed denial of service attack and many others. There is a deficiency of reports which relates crime and the usage of cloud computing services. This paper discusses about the threat model STRIDE and the ill-use of the cloud services for many mischievous purpose by the oppugners around the world. This paper employs STRIDE threat modelling approach as a reference to relate the attacks to threats. Some of the malicious activities committed using cloud are distribution of considerable amount of spams, using the cloud service provider's reputation to cheat the firewalls, distributed denial of service, virus dissemination, credit card fraud and arraying the botnet command and control servers. This paper also discusses on a few real websites which have been affected by threats in the recent years. Most of the criminals get away because of lack of evidence. Evidence collection and analysis in the digital world and especially in cloud environment is a great challenge. This paper also touches on a few issues of forensics in cloud computing environment.

* Corresponding author. Tel.: +09825829356.
E-mail address: gayatri.jain@ljinstitutes.edu.in

1877-0509 © 2020 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the scientific committee of the International Conference on Computational Intelligence and Data Science (ICCIDS 2019).
10.1016/j.procs.2020.03.194

Keywords: Cloud Computing; Cyber crime; Oppugners; Threats ; Vulerabilities; Stride

1. Introduction

Many countries all over the world are facing major issues with criminal activities pursued through mobiles and services provided by the Cloud Service Provider (CSP). India is ranked fourth among the top ten targeted countries. In India the major targets of cyber-crimes are the banks for the financial loot which affects the society [38]. The CSP fails to provide security and privacy for the assets. The claims made by them are very great and they also guarantee for protection. The cloud computing environment faces many threats which leads to unintended behaviour and thus can lead to the loss of assets. Before assessing a security risk to assets, it is very important to categorize and recognize the threats. A risk can be assessed based on the probability and the effect of the threat. The probability is also referred as likelihood, that banks on the number of assaults that can be successful. The impact can be referred to as the amount of damage an asset can face and thus lead to successful attack. A weakness or security loop-hole which exists in the cloud deployed, can be employed to launch assaults. Security analyst's face a lot of challenges after the vulnerabilities are traced. They need to analyse which vulnerability poses which threat, the list of assaults that may abuse it and the list of system parts that may be affected. The security administrators have no appropriate methods to identify and mitigate these threats in cloud. Thus it is extremely important to categorize and recognize the threats in the cloud. To categorize and recognize the threats the steps to be followed are (1) perceive the threats (2) recognize assaults that emerge into threats (3) perceive the vulnerabilities in the cloud computing resources and components and (4) connect the vulnerabilities in the cloud environment misused by assaults and the modelled threats. The motivation for writing this paper is to provide insights and solutions for the real world problems and threats faced in the distributed environment of cloud. The author's contributions include conceiving, researching the literature, collecting the real world problems and the suggesting the related solutions and finally writing the researched contents. The authors of this paper have provided an innovative dimension to handle the major threats and mapping it to a matured threat model STRIDE and discussed the recent threats as case studies that need major attention.

This paper is organized as follows : section 2 discusses about the related work which discusses about the current literature survey of different researchers, section 3 discusses about the threat model STRIDE , section 4 discusses about the top threats in the cloud , mapping of the threats to the STRIDE threat model and its mitigating steps , section 5 relates about how crime is provided as a service on the dark web , section 6 lists about the case studies and the major threats faced in the recent years, section 7 lists the security requirements for the clouds , section 8 discusses about the importance of forensic procedures in the cloud and finally section 9 concludes the paper.

2. Related Work

This section discusses about the literature survey of different researchers in the field of crime through cloud. The researcher Daan has explored about the usage of cloud for malicious activities [1]. The author has listed the different types of crimes that are committed using cloud. The author has also provided an algorithm for finding the lifetime of an IP address in the Passive Spam Block List (PBSL). The author has not discussed the issues as discussed here with appropriate deftness in all the researched topics. An identity protection system for reporting of a crime on cloud is developed by Tzay et al. [2]. The authors have developed an online illegal reporting system based on cloud system. The authors have blended all types of keys, digital certificate and signatures to ensure informers safety and anonymity of the reported users. The system also ensures the non-repudiation and integrity. Guodong et al. have worked on detecting and categorizing the vulnerabilities into different groups [41]. The authors have analysed the vulnerabilities revealed in the recent years in the different virtualization platforms. The authors have designed a framework for bug detection and have applied symbolic execution techniques. John et al. focused on the particular issue of data breaches and weak authentication on a private cloud infrastructure implemented on cloudstack [42]. The authors have used open source tools like Scalpel and PhotoRec. Scalpel is a very efficient tool for recovering deleted files. It has been included in Sleuthkit which is used for forensic analysis [43].Its employed in both the Linux and the Windows environment and runs with a modest set of resources and performs carving operations very promptly. PhotoRec is used to recover all types of files from the different types of memory. The tool focuses on data recovery ignoring the file system. This feature makes it work even if the media's file system is damaged very rigorously or even reformatted.

There are very few research papers which focus on the different types of threats and their mitigating steps. Syed et al. worked on identifying attacks and risk levels and have built a multilevel classification model [4]. The authors have classified the risk as low, medium and high. The authors have classified the security and privacy risk at the different levels of the cloud. The authors have implemented dynamic security provision across the different layers of the cloud as per the need of providers and the users of the cloud. The system provides a new dimension to handle the major security concerns. C Modi et al. surveyed about already known vulnerability and attacks and delivered solutions to fortify security and privacy issues in cloud environment [17]. Nabeel et al. identified around 18 security issues affecting several attributes of cloud computing [18]. In this paper the focus is on the detailed study of the threats and their mapping on the STRIDE model and the mitigating steps provided by the different researchers for every threat. The authors of this paper have provided an innovative dimension to handle the major threats and mapping it to a matured threat model STRIDE.

3. STRIDE Model

There is a lot of conceptual difference between cyber space and the cloud as focused by David [3]. STRIDE Model which is a threat model from Microsoft for identifying the cloud computing security threats. STRIDE is an acronym for threats defined as follows : Spoofing of user identity, Tampering , Repudiation, Information disclosure (privacy breach or data leak), Denial of service (DoS), Elevation of privileges[7]. The threats on IaaS (Infrastructure as a Service) discussed in this paper are those threats listed by CSA Top threats 2018 [6]. The STRIDE model has been applied on to the cloud by some researchers like Den et al. and Saripalli et al. [9][10]. The researchers have discussed a high level view of the different types of threats.

Spoofing of user identity: Oppugners can imitate to be a legal entity and perform some malicious activity and thus cheat the system. The system can be compromised thus allowing access to sensitive data and misuse it, spreading of malware can also be possible. Some examples of such assaults are discussed by Duman et al. [11]. This researcher focused on spoofing of metadata by mimicking a trusted email sender. Wu et al. discussed about ARP spoofing [12]. Xu et al. developed a secure web referral service for a mobile cloud-based virtual computing. Each user is provided a VM as a proxy for security. The system uses web crawling technology with services to check for validation of IP addresses and certificate chains [13]. Aviv et al. discussed about how the oppugner can conduct cross site request forgery bypassing the perimeter defences such as firewalls [33]. Juraj Somorovsky et al. stated that the Cross Site Scripting assaults against Web-based cloud control interfaces have severe repercussions for the overall cloud security [34].

Tampering: Oppugners can make changes to the underlying data, functionalities and communications and thus hamper with the operations. When compared to spoofing this threat can affect the system directly due to modification whereas in the later the illicit information is provided to transform the behaviours. For e.g. by XML poisoning, the system can stop functioning or can malfunction due to change of codes and command. The authors Saripalli et al. discussed about the tampering and such related issues [10].

Repudiation: can deny their own actions due to lack of evidence. There is no trace of evidence of which oppugner did what in the system. Oppugners who plan, attack and clean all the evidences fall under this kind of group. For example when implementing DoS assaults, the oppugners can mask the computers source IP addresses so that they are not traced through the network traces. The authors Chapade et al. discussed about the IP spoofing during the DoS attack so that the IP addresses are not added to the Network logs. The authors Opeyemi et al. also discussed about the DoS attack and the taxonomy and a conceptual cloud DDoS mitigation framework based on change point detection [15].

Information disclosure: The significant information can be leaked or disclosed to the unauthorized persons due to some malicious activities performed by the oppugner. The oppugner can acquire admin privileges and can manipulate the VM or configurations by deactivating ports for the inbound connections even by altering the firewall procedures [7]. Yu et al. have explored more about the revealing validation data by URL forgery [19]. Cheng et al. discussed about security hardness and evaluation and provided some suggestions [16].The authors have used symbolic model checking algorithm and have generated attack graphs for modelling and visualization. They have also blended the features of markov chain with attack graph for proposing the security evaluation metrics.

Denial of Service: This kind of threat affects the availability of service by attacking the resources and exhausting them. This kind of threat can also exploit the flaws in the communication system. For example the attack can be planned and implemented on computing capabilities, network bandwidth, memory etc [14]. Through the malicious activities of this threat by the oppugners, the valid users are denied a service.

Elevation of privilege: Vulnerabilities that are a part of the system, are more easily abused by the oppugners to evade the verification process, thus allowing the unauthorized oppugners to access the system. With this kind of threat the unprotected authenticated data can be whipped [10]. Also due to forgery the authenticated data can be uncovered [19].

4. Top threats in cloud , mapping them to STRIDE threat model and its mitigation

Following Table 1 discusses about the top threats of the cloud [5, 6, 8, 40]. The table includes the threats, the analysis of the threats and which threat in STRIDE they are mapped and the mitigating steps.

Table 1. Top threats and a few migrating steps

Threats	Threat Analysis Mapping to STRIDE	Solutions provided	Solutions by different authors
Data Breach: is an incident which may occur intentionally or unintentionally and the secured sensitive or trusted data is observed, taken or misused by an unlawful individual. It could be an unintentional human fault or a weak security exercise. It's not unique to cloud computing but is the top most concern of the cloud users.	***Information disclosure***	***'Concealment of the Information Storage'***	Nesrine et al. suggested cryptographic techniques for data privacy and security [20], Enhanced Attribute Based Encryption algorithm with hash functions, digital signature and asymmetric encryption method by Saravana et al. [21]
Insufficient Identity, Credential and Access Management: Users should be distinctively identifiable with a federated authentication (e.g. SAML) that works across the CSP.	***STRIDE***	***Validation of users and access control - Virtualization level.'***	Use robust multi-tier code words and authentication mechanisms First tier uses simple username and password. Second tier is pre-determined series of steps. The advantage of this scheme is that it does not require any additional hardware and software as discussed by Manider et al. [29].
Insecure Interfaces and APIs: as the cloud services are of open nature, interfaces and APIs often practice an unknown access, clear text authentication of content transmission and cloud software exposures	***Tampering with data ,Repudiation ,Information disclosure, Elevation of privilege's***	***Validation at Network and API Level***	Data transmission is in encrypted form, strong access control and authentication mechanism. Subashini et al. surveyed about the issues due to the nature of the service delivery prototypes of a cloud computing system [22]. Gracia et al. handled vulnerability called the storage leeching problem [23]. The authors show how easy it is to implement a file-sharing application able to

			distribute digital content by abusing Personal Clouds.
System Vulnerabilities: are exploitable wiretaps in programs that oppugners practice to penetrate a computer system for the purpose of data theft, trying to govern the system or distracting service procedures.	***STRIDE***	***Concealment***	Manageable services under control and strong checking. Gayatri et al. discussed about the adoption of strong authentication mechanisms so as to maintain confidentiality [28].
Account or Service Hijacking: Infrastructure Security, Using social engineering, phishing, deceit or weakness exploits.	***STRIDE***	***Concealment, integrity and availability***	Gayatri et al. focused on adoption of strong authentication mechanisms using ECC and also provided solutions on integrity of data [28].
Malicious Insiders: A mischievous insider risk to an organization is a existing or previous employee having authorized access to an organization's data and the network and has misused his access rights intentionally leading to the damage of the CSPs reputation.	***Repudiation and Denial of Service Elevation of privilege's***	***Concealment, integrity, or availability of data.***	employ agreement reporting and breach notices, security and management process are made transparent Gayatri et al. provided solutions for privacy integrity and availability. They provided methods of identifying the change in evidences if the evidences are maligned by the malicious insiders [28].
Advanced Persistent Threats: (APTs) are a parasitical form of cyber-attack that penetrates systems to establish a foothold in the computing infrastructure of a few selected companies from which they rob data and intellectual property	***Information disclosure and Elevation of privilege's***	***Intrusion detection***	emphasis should be on outbound stream of traffic, Recognize the varying threat, proper co-ordination of the endpoints Yasin et al. developed a innovative framework entitled as Cloud-based Intrusion Detection Service (CBIDS). The system allows the identification of mischievous activities from diverse points of network and overcome the deficiency of classical intrusion detection. CBIDS is employed to detect variety of assaults in diverse types of clouds [31].
Data loss: Data ownership, encryption, transmission, operational failure, data disposal/data erasure and readiness are all major defies in a cloud environment.	***Repudiation***	***Data Privacy & Availability***	Deliver data storage and standby mechanisms Oppermann et al. applied extension of Homomorphic encryption library to meet the real world [30].
Insufficient Due Diligence: building a good roadmap and specification list when assessing technologies and CSPs is vital for the extreme gamble of attainment. (more of Organizational)	**STRIDE**	This threat is diverse from those stated here.	This risk has to be dealt by cloud administrator and the government.
Abuse and Nefarious Use of Cloud Services: the distributed and anonymous nature of the cloud can be more appealing to the criminals	**Denial of Service**	***Authentication***	Witness the network status, deliver firm registration and authentication procedures.

			Maxwell Farnga related in his report about such threats and mitigated it by the idea of principal of least privilege for all authorized users, by malicious code protection and by monitoring [32].
Denial of Service: compelling the selected cloud service providers for employing excessive amounts of limited system resources such as processor power, memory, and disk space or network bandwidth. Such assaults leads to slowing down of services of the system and also leads to frustration of legal users of the system.	**Denial of Service**	***Availability*** Service availability is affected,	Strong authentication and authorization methods can be employed Lindemann et al. [25] suggested that DoS assaults can be detected at the network level using sensors at the boundary as VLANs and has also identified the existence of different approaches for inbound detection from other researchers. The authors have suggested VMI-based IDS technique as it can directly inspect any machine state and can detect malicious software running on the host. Aljahdali et al. suggested that during unexpected increase of traffic, a port scanning can be performed to detect any DDoS assaults [24].
Shared Technology: allotment of resources and services among different users. It escalates the reliance on logical seclusion and other controls to safeguard the tenant against the interference against one another and the security procedures.	***Information disclosure and Elevation of privilege's***	***Virtualization availability***	Separation of data and replica needs to be safeguarded. Robust verification and access control are some mechanisms to preclude such problems. Tan et al. has proposed TinyChecker, a system to protect VMs against hypervisors by using nested virtualization methods. The system uses context based and on-demand checking to identify and rectify any failure. However, it does generate small performances overhead [26]. Kazim et al. has suggested in implementing proper isolation among VMs in order to prevent leakage. The authors have suggested of having proper access controls and risks assessments so to avoid unauthorized access to sensitive business data [27].
Meltdown: breaks the seclusion concerning the user applications and the operating system. **Spectre:** breaks seclusion concerning the applications. These attacks cannot be traced as they do not leave any traces. These attacks	***STRIDE***	*Employ patches provided to secure.*	Paul Kocher and Moritz Lipp specify that the fix for such attacks are at the processor level and the Instruction set needs to be updated [44][45].

can expose all the secrets in the memory. Cloud providers who use Intel CPU or Xen PV as virtualization without having patches are prone to such attacks. Side channel is employed to obtain the information from the memory.

5. Crimes provided as Services

The cloud computing environment has elevated the crime ratio and has the potential for the encouraging the cyber-crimes through the cloud. This section discusses about the special kind of services which are on the cloud especially for the criminals. There are many services that are sold as a special type of service by the Dark web. The Dark web is an anonymous and untraceable World Wide Web to the users employing this web. It is accessible by means of special software's like Tor browser. This Tor browser routes the page requests through a series of proxy servers activated by millions of volunteers around the globe [36-39]. The IP addresses used on this web and through the Tor browser are unidentifiable and untraceable. The figure 1 depicts the different services provided as a crime. Following is a list of such services:

5.1 *Crime as a Service (CaaS)* is a new threat on the Dark Web. A professional group of criminals are offering their services to the criminal group by developing advance tools, kits and packaged services. These tools are rented or are put on sale for the less experienced oppugners. On Demand DDoS attacks are also offered at a cost.

5.2 *Ransomeware as a Service (RaaS)* is a special type of Software as a Service offered for the criminals. Cybercriminals provide a compact malicious kit which is capable of launching a ransom ware attack. These products are advertised on the Dark web. Such tools save time of development or are helpful to the novice oppugners. Some of the products sold on the Dark web are Satan, Cerber, Atom, Hostman etc.

5.3 *Botnet as a Service (BaaS)* offers DDoS attacks for IoT devices. These services are offered at a cost by the criminals who don't want to execute the attack themselves. They develop such tools for making business. These services are offered to others who lack such skills. The low skilled criminals can assemble a BaaS and cause a huge volume of destruction.

5.4 *Hacking as a Service (HaaS)* is used to outsource a complete cyber-enabled attack. It also provides technical support for cybercrime activities. They provide a robust and dynamic integration of stolen data. These services are offered to the low skilled professional who want to employ such services for financial gain.

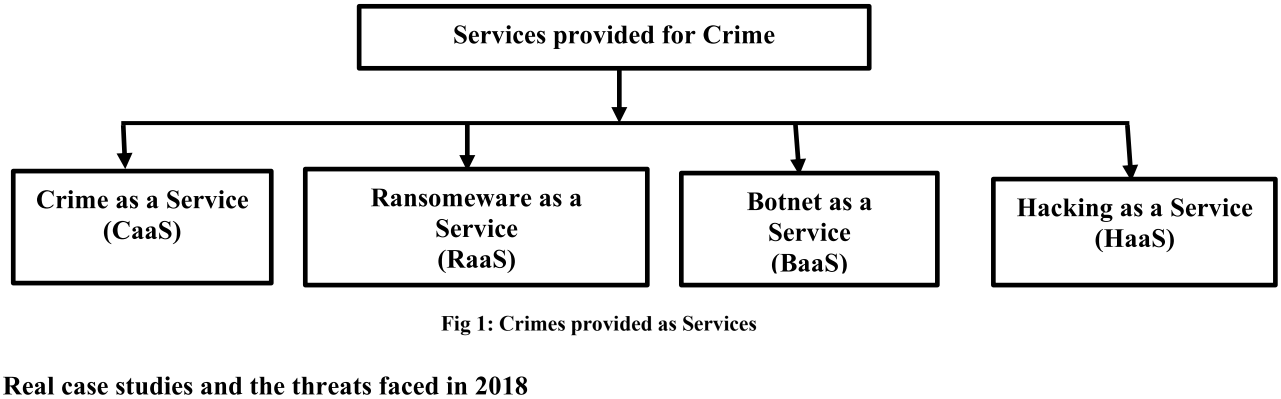
Services provided for Crime
Crime as a Service (CaaS)
Ransomeware as a Service (RaaS)
Botnet as a Service (BaaS)
Hacking as a Service (HaaS)

Fig 1: Crimes provided as Services

6. Real case studies and the threats faced in 2018

Table 2 lists a few websites or companies which faced the major threats discussed in this paper [6]. The threats recently faced by these companies have caused a major loss in terms of finance and credibility.

Table 2. Real case studies and the threats faced in 2018

Web Site	Threats faced
LinkedIn	Data Breaches; Insufficient Identity, Credential and Access Management; Account Hijacking; Denial of Service; Shared Technology Vulnerabilities
MongoDB	Data Breaches; Insufficient Identity, Credential and Access Management; Insecure Interfaces and APIs; Malicious Insiders; Data Loss
Dirty Cow	Insufficient Identity, Credential and Access Management; System Vulnerabilities
Zynga	Data Breaches; Insufficient Identity, Credential and Access Management; Malicious Insiders
Net Traveler	Data Breaches; Advanced Persistent Threats; Data Loss
Yahoo	Data Breaches; Data Loss; Insufficient Due Diligence
Zepto	Data Loss; Abuse and Nefarious Use of Cloud Services
DynDNS	Insufficient Identity, Credential and Access Management; Denial of Service
Tmobile	customer information theft - Malicious Insiders
Cloudbleed	Data Breaches; Shared Technology Vulnerabilities

7. Security Requirements for the Cloud

The Security properties needed in IaaS model are specified in Table 2. The properties specified also discuss about who needs to have control on which property [40, 47]. The CSP is represented as C and User is represented as U.

Table 3.Security properties needed in Infrastructure as a Service model

Security requirements	Authentication	Encryption	Integrity	Availability	Access Control
Computing Hardware	C	--	--	C	--
Virtualization	C/U		C/U	C	C/U
Data Storage	--	C/U	U	C	C/U
Networking	--	--	--	C	C/U
Cloud Software	--	--	--	C	--
Utility Computing	C	--	C	--	C
SLA	--	--		C	C
Security requirements	Authentication	Encryption	Integrity	Availability	Access Control

8. Significance of forensic procedures in cloud

The main concern in the domain of cloud forensics is the lack of specific tools and limited professional expertise. The forensic procedures when applied to investigation become more challenging when encryption, multi-jurisdiction and loss of data control is involved. The cloud organizations have to provide cloud forensic capability or else may face difficulties during the cloud forensic investigations. John Michael has highlighted the top threats faced by a few companies in 2018. The author discusses the threats faced and also discussed the corrective, preventive and detective controls for the issues faced [6]. The author focuses on proper forensics procedures needed which have to be followed to track the oppugners. Gayatri et al. surveyed about the forensic procedures and laws in India [35]. The authors have highlighted the issues in cloud forensic and the importance of evidences in cloud environment to track the oppugners. The authors also have developed a framework which assist in managing the integrity and confidentiality of the logs using cuckoo and bloom filters [46] and obtained good results with cuckoo filter. Major issues faced in cloud forensics are multi-tenancy, integrity and privacy. Issues regarding the service level agreements and volatile data are also major issues. Encryption issues and lack of tools for the current environment also highlight the problems. The tools available do not fulfil the current requirements.

9. Conclusion and future scope

Since the last decade cloud computing technology is a widely adopted paradigm. Though it is widely adopted security of critical data has been a major concern and a great barrier to adopt the cloud for many organizations. The standards adopted for procedures of investigation during a security breach are still very immature. There are many issues in the cloud like issues of volatile logs, insecure interfaces, malicious insiders and many others which still need proper mechanisms for shielding the loose ends and open issues to be resolved in future [46]. Cloud environment has also encouraged the cyber–criminals to host the crime services on the dark web and market the same. The security management in a distributed environment becomes a difficult task and as the cyber-criminals use anti-forensic tools to wipe off the forensic evidences, tracking such cyber-criminals becomes a tough task. The authors have focused on IaaS threats specifically and discussed about Microsoft STRIDE model and have mapped it to the threats. The authors have also discussed about the issues of vulnerabilities leading to threats and the mitigation steps and the related forensic issues. The issues discussed by the authors are the major research gaps and there is a lot of scope in future in security and forensic management domain.

Acknowledgements

The authors are thankful to the anonymous reviewers and the editors for their suggestions. The authors are also thankful to the managers for quick and timely responses. The authors are also thankful to the staff members of LJK trust, Dr. H.B.Bhadka of C.U.Shah University, Dr. Sameer Patel of PDP University, Dr. Maniklal Das from DAIICT for their best co-operation, support and guidance.

References

[1] Daan Kolthof (2015) “Crime in the Cloud: An Analysis of the Use of Cloud Services for Cybercrime” , in 23rd Twente Student Conference on IT June 22nd, Enschede at the Netherlands.

[2] Tzay-Farn Shih, Chin-Ling Chen, Bo-Yan Syu and Yong-Yuan Deng: (2019) “A Cloud-Based Crime Reporting System with Identity Protection”, in Symmetry 11, 255; doi: 10.3390/sym11020255 : 1-29

[3] David S. Wal (2017) “TOWARDS A CONCEPTUALISATION OF CLOUD (CYBER) CRIME”, in Human Dimensions of Cyber security panel of the 5th International Conference on Human Aspects of Information Security, Privacy and Trust, Vancouver Convention Centre, Vancouver, Canada 9-14 July 2017, in T. Tryfonas (Ed.) Hu-man Aspects of Information Security, Privacy and Trust, New York: Springer International, DOI: 10.1007/978-3-319-58460-7_37 : 529–538.

[4] Syed Asad Hussain, Raja Khurram Shahza (2017) “Multilevel classification of security concerns in cloud computing” in Applied Computing And Informatics 13(1), Jan : 57-65

[5] CLOUD SECURITY ALLIANCE (2018) “The Treacherous 12 - Cloud Computing Top Threats in 2018”. https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf {accessed on 11-Mar-2019}

[6]TOP THREATS TO CLOUD COMPUTING: DEEP DIVE (2014) Jon-Michael C. Brook, ISSP, CCSK,

https://ghllc.co/wpcontent/uploads/2019/03/2018.12.13.Millennium_Alliance.03.pdf {accessed on 11-Mar-2019}

[7] Adam Shostack, Threat modelling Designing for security Published by John Wiley & Sons, Inc.

[8] Jin B. Hong, Armstrong Nhlabatsi , Dong Seong Kim , Alaa Hussein , Noora Fetais Khaled M. Khan, (2019) "Systematic identification of threats in the cloud: A Survey", 150 : 46 - 69

[9]M. Deng, M. Petkovic, M. Nalin, I. Baroni. (2011) "A home healthcare system in the cloud–addressing security and privacy challenges", in: Proc. of the 4th IEEE International Conference on Cloud Computing (CLOUD 2011), doi: 10.1109/CLOUD.2011.108 : 549–556.

[10]P. Saripalli, B. Walters, (2010) "QUIRC: a quantitative impact and risk assessment framework for cloud security", in Proc. of the 3rd IEEE International Conference on Cloud Computing (CLOUD 2010), doi: 10.1109/CLOUD.2010.22 : 280–288

[11]S. Duman, K. Kalkan-Cakmakci, M. Egele, W. Robertson, E. Kirda, (2016), "Email Profiler: spear phishing filtering with header and stylometric features of emails" , in: Proc. of the 40th IEEE Annual Computer Software and Applications Conference (COMPSAC) , doi: 10.1109/COMPSAC.2016.105 : 408–416.

[12]H. Wu, Y. Ding, C. Winer, L. Yao (2010) "Network security for virtual machine in cloud computing" in: Proc. of the 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT 2010), doi: 10.1109/ICCIT.2010.5711022 : 18–21.

[13] L. Xu, L. Li, V. Nagarajan, D. Huang, W. Tsai (2013) "Secure web referral services for mobile cloud computing" in Proc. of the 7th IEEE International Symposium on Service-Oriented System Engineering (SOSE 2013), doi: 10.1109/SOSE.2013.94 : 584–593.

[14] S. Chapade, K. Pandey, D. Bhade (2013) "Securing cloud servers against flooding based DDOS attacks", (2013) in: Proc. of the International Conference on Communication Systems and Network Technologies (CSNT 2013), doi: 10.1109/CSNT.2013.114 : 524–528.

[15] Opeyemi. Osanaiye, K. Choo, N. Dlodlo, (2016) "Distributed denial of service (DDos) resilience in cloud: review and conceptual cloud DDos mitigation framework" , Journal of Network and Computer Applications. Appl. 67, doi: 10.1016/j.jnca.2016.01.001 : 147–165

[16] Y. Cheng, Y. Du, J. Xu, C. Yuan, Z. Xue, (2012) "Research on security evaluation of cloud computing based on attack graph"(2012), in: Proc of IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 01, doi: 10.1109/CCIS.2012.6664 448 : 459–465 .

[17] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, (2013) "A survey of intrusion detection techniques in cloud", Journal of Network and Computations. Appl. 36 (1) , doi: 10.1016/j.jnca.2012.05.003, 42–57 .

[18] Nabeel Khan , Adil Al-Yasiri (2016) "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework" in Proc of 2nd International Workshop on Internet of Thing: Networking Applications and Technologies (IoTNAT'(2016) , Procedia Computer Science 94, 485– 490

[19] Y. Yu, Y. Yang, J. Gu, L. Shen (2011) "Analysis and suggestions for the security of web applications" in: Proc. of the International Conference on Computer Science and Network Technology (ICCSNT 2011), 1 , doi: 10.1109/ICCSNT.2011.6181948 : 236–240 .

[20] Nesrine Kaaniche, Maryline Laurent (2017) "Data Security and Privacy preservation in Cloud Storage Environments based on Cryptographic Mechanisms" in Computer Communications, doi: 10.1016/j.comcom.2017.07.006

[21] Saravana Kumar Na,Rajya Lakshmi G.Vb,Balamurugan Ba (2014) "Enhanced Attribute Based Encryption for Cloud Computing" in International Conference on Information and Communication Technologies (ICICT 2014).

[22] S. Subashini, V. Kavitha (2011) "A survey on security issues in service delivery models of cloud computing". Journal of Network and Computer Applications 34(1), January

[23] R. Gracia-Tinedo, M. Artigas, P. Lopez (2013) "Cloud-as-a-gift: effectively exploiting personal cloud free accounts via REST APIs" in: Proc. of the 6th IEEE International Conference on Cloud Computing (CLOUD 2013), 621–628, doi: 10.1109/CLOUD.2013.47

[24] H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, (2014) "Multi-Tenancy in Cloud Computing," in IEEE 8th International Symposium on Service Oriented System Engineering (SOSE) : 344–351.

[25] J. Lindemann, (2015) "Towards abuse detection and prevention in IaaS cloud computing" in Proc. - 10th International Conference. Availability, Reliability. Security ARES : 211–217

[26] C. Tan, Y. Xia, H. Chen H and B. Zang B (2012), "Tiny Checker: Transparent Protection of VMs against Hypervisor Failures with Nested Virtualization.": in Proc of : Dependable Systems and Networks Workshops (DSN-W), IEEE/IFIP 42nd International Conference.

[27] M. Kazim and S. Y. Zhu (2015) "A survey on top security threats in cloud computing," Int. J. Adv. Comput. Sci. Appl., 6(3) : 109-113

[28] Gayatri S Pandi, Dr K H Wandra. (2018) "Secured Forensic Framework for Various Users in the Virtualized Environment of Cloud" in Proc of International Conference on Information and Communication Technology for Sustainable Development. ISBN 978-981-13-7166-0, AISC Vol 933, Springer Singapore : 712 - 727

[29] Maninder Singh, Sarbjeet Singh (2012) "Design and Implementation of Multi-tier Authentication Scheme in Cloud" in International Journal of Computer Science Issues, 9(5) September

[30] Oppermann A., Yurchenko A., Esche M., Seifert JP (2017) "Secure Cloud Computing: Multithreaded Fully Homomorphic Encryption for Legal Metrology" in: Traore I., Woungang I., Awad A. (eds) Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments. (ISDDC 2017) Lecture Notes in Computer Science, 10618. Springer, Cham

[31] W. Yassin , N.I. Udzir ,Z. Muda , A. Abdullah , M.T. Abdullah (2012) "A Cloud-based Intrusion Detection Service framework" in Proceedings of International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec-2012)

[32] Maxwell Farnga. "Case studies: Information Security and Assurance" https://arxiv.org/ftp/arxiv/papers/1808/1808.03892.pdf { accessed on 30-March-2019}

[33] A . Ron, A . Shulman-Peleg, A . Puzanov, (2016) "Analysis and mitigation of nosql injections" IEEE Security. Privacy 14 (2), doi: 10.1109/MSP.2016.36 : 30–39.

[34] J Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, L. Lo Iacono (2011) "All your clouds are belong to us: security analysis of cloud management Interfaces" in: Proc. of the 3rd ACM Workshop on Cloud Computing Security Workshop (CCSW 2011), in: CCSW '11, ACM, New York, NY, USA, doi: 10.1145/2046660.2046664 : 3 – 14.

[35] Gayatri S Pandi, Dr K H Wandra. (2018) "CLOUD FORENSIC FRAMEWORKS, CHALLENGES, STATE OF ART AND FUTURE DIRECTIONS." in: Journal of Emerging Technologies and Innovative Research 5(5), May : 712 – 721.

[36] Symantec Report Webpage (2019) https://www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware{accessed on 11-Mar-2019}

[37] Trendmicro Report (2019) Webpage https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-

lazarus-groups-operations {accessed on 11-Mar-2019}

[38] Vakilno1 Report Webpage (2019) https://www.vakilno1.com/legal-news/cybercrime-in-india.html{accessed on 11-Mar-2019}

[39] Csoonline Report Webpage (2019) https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html {accessed on 20-Mar-2019}

[40] El Balmany Chawki, Asimi Ahmed, Tbatou Zakariae (2018) " IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors" in Procedia Computer Science 134 : 328–333

[41] Guodong Zhu ; Yue Yin ; Ruoyan Cai (2017) "Detecting Virtualization Specific Vulnerabilities in Cloud Computing Environment" in proceedings of 10th International Conference on Cloud Computing (CLOUD), IEEE, Electronic ISSN: 2159-6190.

[42] John Patrick Barrowclough and Rameez Asif (2018) "Securing Cloud Hypervisors: "A Survey of the Threats, Vulnerabilities, and Counter measures" in Security and Communication Networks, Article ID 1681908, https://doi.org/10.1155/2018/1681908

[43] Richard and Vassil Roussev (2005) "Scalpel: A Frugal, High Performance File Carver" in the proceedings of DIGITAL FORENSIC RESEARCH CONFERENCE, USA.

[44] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin,Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, Yuval Yarom "Spectre Attacks:Exploiting Speculative Execution".

[45] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher,Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin; Yuval Yarom, Mike Hamburg, "Meltdown: Reading Kernel Memory from User Space"

[46] Gayatri S Pandi, Dr. Saurabh Shah and Dr K H Wandra (2019) "Augmenting the Operations on Cloud Virtual Forensic Data by employing Probabilistic Data Structures" in International Journal of Sensors, Wireless Communications and Control.

[47] Ravi Kumar, P., Herbert Raj, P., Jelciana, P., (2018) "Exploring Data Security Issues and Solutions in Cloud Computing." 6th International Conference on Smart Computing and Communications 125: 691-697. https://doi.org/10.1016/j.procs.2017.12.089