Grenze International Journal of Engineering and Technology, Jan Issue

Encryption-Decryption Approach to Cryptographic Security Concerns of Cloud Computing

Mr. Hirdesh Sharma[1], Dr. Gaurav Aggarwal[2] and Dr. Sachin Kumar[3]
[1]Research Scholar, Jagannath University, Bahadurgarh (Jhajjar), Haryana, India
ORCID iD: 0000-0002-1278-4135, EmailID:- hirdesharma@gmail.com
[2]Professor & Dean, Dept. of CSE, Jagannath University, Bahadurgarh (Jhajjar), Haryana, India
ORCID iD: 0000-0002-6836-9352, EmailId:- gauravaggarw@gmail.com
[3]Associate Professor, Dept. of MCA, Noida Institute of Engg. & Tech., Greater Noida, India
ORCID iD: 0000-0002-1136-8009, EmailId:- sachinks.78@gmail.com
Contact Number- +91-9410017983

***Abstract*—In this paper security concerns of cloud computing with cryptographic security, which is investigate here by recognizing the most widely recognized shortcomings in these frameworks and among the most regularly referred to risks in the Cloud Computing writing and its environmental factors, just as to identify and associate shortcomings and dangers to possible cures. Here, SPI's Model is proposed and a few surveys have investigated cloud security without recognizing dangers and weaknesses. It is focused on this qualification since we accept it's essential to get a handle on these worries.**

***Index Terms*— Security, Cloud Computing, Analysis, Security Issues, Review, Encryption, PaaS, SaaS, IaaS.**

I. INTRODUCTION

Distributed computing is turning out to be additional significant and it is drawing in additional consideration from the logical and modern gatherings. As per a Gartner research, Cloud Computing is the 1st among the best ten several critical advances, with a more brilliant standpoint for endeavours and associations before long.

The principal objective of distributed computing, which is both a computational worldview and an appropriation engineering, to give protected and net registering administrations, with all PC assets portrayed as administrations and provided by means of the Internet. Coordinated effort, dexterity, adaptability, accessibility, the ability to respond to request varieties, the capacity to assist advancement work, and the opportunities for cost decrease through upgraded and productive figuring are generally advantages of the cloud.

Regardless of the way that there are a couple of advantages to using Cloud Computing, there are furthermore a few liberal obstacles to make due. Security is one of the primary deterrents to gathering, followed by difficulties with consistence, insurance, and legitimate issues. Since Cloud Computing is an especially unique enrolling model, there is a lot of obscurity with respect to how security can be achieved. Because of the weakness, information bosses have constantly said that security is top worry with respect to Cloud Computing.

External data storing, reliance on "general society" web, nonattendance, multi-inhabitancy, and compromise with security are to a great extent districts where security issues exist. The cloud has a couple of specific characteristics when stood out from traditional developments, for instance, massive size and how cloud provider

Grenze ID: 01.GIJET.9.1.68

resources are by and large dispersed, different, and virtualized. Customary security techniques like unmistakable evidence, confirmation, and approval are right now lacking for appropriated registering in its status. Appropriated processing wellbeing endeavors are, something similar than security in some other Information Technology environment. Appropriated processing, on the other hand, may give different threats to a relationship than ordinary IT plans.

Moving huge applications and delicate data to public cloud settings is a critical wellspring of stress for associations that are reaching out external the association the chiefs of their server ranches. To placate these sensations of fear, a cloud game plan provider ought to ensure that clients hold a comparable security and insurance controls over their applications and organizations, give check to clients that their affiliation is secure and fit for meeting organization level game plans, and have the choice to show consistence to evaluators.

A couple of assessments centre around a singular help type or perceive cloud security stresses by and large without perceiving shortcomings and risks. We have collected a once-over of shortcomings and risks, similarly as a summary of cloud organization models that might be impacted.

Coming up next is the means by which the rest of the paper is facilitated: The delayed consequences of our exact review are presented in Section 2. Then, in Section 3, we go through the most key security features for each level of the Cloud model thoroughly. Following that, we'll look at the security stresses in conveyed figuring, perceiving the most notable shortcomings, the most notable risks, and all possible answers for these risks and weaknesses. Finally, we give a couple of proposition.

A. Survey of Safety Issues for Distributed Environment

We led an exhaustive report of the accessible writing on Cloud Computing security, not exclusively to depict the known weaknesses and dangers, yet in addition to distinguish and evaluate the current state and the most pertinent security concerns.

B. Formalization of Questions

The goal of the solicitation was to recognize the primary concerns in Cloud Computing, including shortcomings, risks, risks, necessities, and security courses of action. This request should be associated with the goal of this endeavour, which was to perceive and communicate shortcomings and threats to likely fixes. Thusly, the assessment question watched out for by our survey was: What are the most fundamental security shortcomings and risks in Cloud Computing that ought to be dissected through and through to be made do?

C. Determination of sources

The models by which we reviewed focus on sources relied upon the makers' investigation expertise, and we expected to consider a couple of constraints to pick these sources: reads up associated with the picked sources should be circulated in English, and these sources should be web-accessible. IEEE electronic library, ACM progressed library, ScienceDirect, DBLP and Scholar Google are among sources that have been evaluated. A while later, the experts will deal with the revelations and add key works that were not tracked down in these sources, similarly as update these endeavors to address various restrictions, for instance, influence factor, got references, prominent journals, and eminent makers, etc.

This current review's incorporation and rejection measures were controlled by the exploration subject. Not set in stone that the examination should incorporate topics and subjects connected with Cloud Computing security, just as dangers, weaknesses, countermeasures, and concerns.

D. Survey execution

During this progression, you should do a hunt in the characterized sources and survey the exploration you track down utilizing the set-up standards We got a bunch of around 120 outcomes in the wake of running the hunt chain on the picked sources, which were then sifted utilizing the incorporation standards to give a bunch of about 40 significant explores. This gathering of examination was sifted again utilizing the prohibition models, yielding an assortment of papers that compared to 15 significant ideas.

II. RESULTS AND DISCUSSIONS

Most of the methods portrayed distinguish, group, assess, and list various Cloud Computing-related weaknesses and dangers. The examinations analyse the dangers and perils and, by and large, make suggestions on how they might be stayed away from or alleviated, bringing about an unmistakable connection among weakness and likely arrangements and systems for managing them. Besides, we can see from our hunt that a large number of the methodologies, as well as discussing dangers and weaknesses, additionally talk about different parts of cloud

security, like data security, trust, or security ideas and parts for any of the issues that arise in these circumstances.

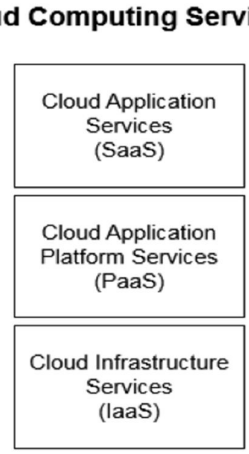

Figure 1: Cloud Computing Services and Cloud Security Management Services

A. SPI model's Security

Three types of services are available in the cloud model:
Programming as-a-Service (SaaS). The customer is offered the opportunity to utilize the provider's applications, which are worked with on a cloud establishment. A humble client interface, similar to a web program, is used to get to the applications from a combination of client devices (e.g., electronic email).
Stage as-a-Service (PaaS). The client has the chance to send his own applications to the cloud framework without introducing any stage or apparatuses on their neighbourhood gadgets. PaaS represents stage as an assistance, and it incorporates things like working framework backing and programming improvement structures that might be utilized to make more significant level administrations.
Framework as-a-Service (IaaS). The client is enabled to supply handling, stockpiling, organizations, and other essential PC assets, permitting them to send and execute discretionary programming, like working frameworks and applications.
With SaaS, the cloud provider has the commitment in regards to security. This is most of the way in view of the degree of consultation; the SaaS model depends on a huge level of consolidated helpfulness with little client control or improvement. The PaaS approach, on the other hand, engages more noticeable flexibility and client control. IaaS gives better occupant or client control over security than PaaS or SaaS, inferable from the lower level of reflection.
A PaaS provider might lease an improvement climate to a SaaS organization, while an IaaS supplier might lease framework to a SaaS supplier. Each specialist organization is answerable for ensuring his own administrations, which may prompt an irregularity in the security approaches utilized. It likewise makes it hard to figure out which specialist co-op is at fault in case of an assault.

B. Security Issues with SaaS

Conferencing programming, email and business applications like SCM, CRM and ERP are occasions of SaaS applications. Among the three principal cloud transport types, SaaS buyers have insignificant control over security. Security issues could arise due to the usage of SaaS applications.

C. Application security

Normally, these applications are conveyed through the Internet utilizing a Web program. Web application flaws, then again, may open SaaS applications to weaknesses. Aggressors have been using the web to gain admittance to clients' PCs and complete destructive activities, for example, information burglary. SaaS applications have a similar security issue as some other web-based application innovation, yet standard security arrangements are ineffectual in shielding them from attacks, requiring new strategies. The 10 most genuine internet-based application security dangers have been perceived by the OWASP. There are greater security issues, yet it's a magnificent spot to begin with regards to web application security.

D. Multi-tenancy

Adaptability, configurability by means of multi-tenure and metadata are largely includes that might be utilized to order SaaS frameworks into development models. Every customer gets their own redone occasion of the program in the principal development model. This model contains imperfections, despite the fact that security concerns aren't however not kidding as they may be with different models. The seller offers unmistakable examples of the applications for every customer in the subsequent model, however all cases use a similar application code. Clients can modify different design decisions in this model to accommodate their own necessities. Multi-tenure is presented in the third development model, permitting a solitary example to support all customers. This technique utilizes assets; but it has limits as far as adaptability. Applications can be increased in the last model by migrating them to an all the more remarkable server if important.

E. Data security

Information security is a not kidding issue for any innovation; however, it turns out to be much more troublesome when SaaS clients should depend on their providers for insurance. Information reinforcement is additionally significant to empower recuperation in case of a catastrophe, albeit likewise raises security issues. Besides, cloud organizations may rethink extra administrations, like reinforcement, to outsider specialist co-ops, raising issues. Besides, most consistence guidelines do not expect administrative consistence in the Cloud Computing period. Since information is put away in the supplier's datacenters, the course of consistence is convoluted in the SaaS climate. This can bring about administrative consistence concerns including information protection, isolation, and security, which the supplier should uphold.

F. Accessibility

Utilizing an internet browser to get to programs over the web improves on access from any organization gadget. It additionally builds the security concerns related with the help. The Cloud Security Alliance has circulated a document that depicts the current status of flexible handling and the top risks around here, including data taking compact malware, temperamental associations (Wi-Fi), and shortcomings tracked down in device OS.

G. Security Issues with SaaS

PaaS grants cloud-based applications to be sent without the expense of purchasing and staying aware of the essential hardware and programming layers. PaaS, as SaaS and IaaS, requires a protected and stable association similarly as a strong web program, presents data security stresses similarly as various issues, which are recorded under:

Third-party relationships

PaaS additionally incorporates outsider web administrations parts, for example, mashups, notwithstanding standard programming dialects. Mashups are a kind of mashup that joins many sources into a solitary substance. Thus, security issues related with mashups, like information and organization security, are likewise acquired by PaaS models. Clients of PaaS ought to rely upon the security of both web-worked with progression instruments and third-social event organizations.

Development Life Cycle

Fashioners go facing the trial of creating safe applications to work with cloud. SDLC and security will be affected by the speed at which cloud applications advance. Engineers should know, in any case, that any adjustments to PaaS parts might endanger the security of their applications. Engineers should be prepared on information lawful issues notwithstanding safe improvement draws near, to guarantee that information isn't put away in uncertain regions. Information might be kept in an assortment of areas, each with its own arrangement of lawful guidelines, putting its protection and security in danger.

Hidden foundation security

In Paas, in spite of the fact that engineers only here and there approach the fundamental layers, providers should get both the basic foundation and the applications administrations. Despite the fact that designers have unlimited authority over their applications' security.

At last, there is a shortage of data in the writing on PaaS security issues. PaaS gives advancement instruments to develop SaaS applications, while SaaS conveys programming circulated over the web. PaaS applications and client information are likewise kept on cloud servers, which, as referenced in the former segment, may be a security issue. Information is connected to a cloud-based application in both SaaS and PaaS situations. The provider is liable for the security of this information as it is handled, communicated.

H. Security Issues with SaaS IaaS

Clients save the choice to execute any program they single out the resources that have been distributed to them. However lengthy there is no security flaw in the virtual machine screen, cloud clients have well control over security with IaaS. They are answerable for the item dealing with their virtual machines and of fittingly planning security courses of action. Cloud providers, of course, control the key figuring, association, and limit establishment. To reduce the hazards introduced by creation, correspondence, checking, change, and compactness, IaaS providers ought to advance a basic endeavor to get their structures. Part of security stresses with IaaS.

I. Demineralisation

Clients could utilize demineralisation to build, duplicate, proposition to execute a wide extent of uses. Regardless, due of the additional layer that ought to be guaranteed, it opens up new open doors for aggressors. For standard systems, demineralized structures are powerless against a large number of assaults; in any case. Virtual machines, rather than certifiable servers, have two indisputable cutoff points: physical and virtual.

J. Virtual machine screen

VMM is answerable for virtual machine separation, since, assuming that the VMM is hacked. It, similar to some other piece of programming, has security weaknesses. Keeping the VMM as fundamental and insignificant as achievable limits the danger of safety weaknesses since any imperfection will be not difficult to distinguish and address.

Besides, virtualization empowers virtual PCs to be moved between genuine servers. This accommodating component, in any case, can cause security issues. An assailant can exploit the VMM's relocation module. Moreover, clearly VM movement uncovered the VM's data to the organization, subsequently risking its information trustworthiness and classification.

Shared resource

Virtual machines on a similar server can share assets like CPU, memory, and I/O. Dividing assets among VMs might think twice about one's security. For instance, without compromising the hypervisor, a malignant VM may induce data about other VMs by means of shared memory or other shared assets. Two VMs can convey through secret channels, evading all of the VMM's security limitations.

Public VM image repository

PVM contains the arrangement documents that are needed to construct VMs in an IaaS climate. Subsequently, these photos are basic for the cloud's general security. One can either assemble her own virtual machine picture without any preparation or use one from the supplier's storehouse. Amazon, for instance, has a public picture archive where approved clients might acquire or submit virtual machine pictures. Hurtful people may transfer noxious code-contaminated pictures to public storehouses, compromising different clients and possibly the cloud framework. An aggressor with a real record, for instance, may make a malignant picture containing a Trojan pony. Assuming another customer utilizes this picture to develop a virtual machine, that virtual machine will be contaminated with the hid infection. Moreover, VM replication may coincidentally cause information spillage. This delicate information may be open to different clients assuming the picture isn't "cleaned." Virtual machine pictures are latent antiques that are hard to fix when disconnected.

K. Virtual machine rollback

Moreover, assuming that a slip-up happens, virtual machines can be moved back to an earlier state. Moving back virtual machines, then again, may open them to recently fixed security weaknesses or permit recently impaired records or passwords to be re-empowered. We really want to deliver a "duplicate" (preview) of the virtual machine.

L. Life Cycle of virtual machine

It's similarly critical to get a handle on the VMs' lifetime and the way that their states vary as they cross the environment. Malware location is confounded by the way that virtual machines can be turned on, off, or stopped. Moreover, virtual machines can be vulnerable in any event, when they are switched off. By embedding noxious code into other virtual machines during the development cycle, these malevolent pictures can fill in as a springboard for malware proliferation.

M. Virtual networks

Because of asset pooling, network parts are shared across a few occupants. As recently expressed, aggressors can complete cross-occupant attacks through sharing assets. Virtual Networks improve the interconnection of virtual machines, which represents a huge security hazard in Cloud Computing. Committed actual channels are the most reliable way to deal with associate each VM to its host. Virtual organizations, then again, are ordinarily utilized by hypervisors to associate VMs and permit them to connect all the more straightforwardly and viably. Most virtualization innovations, like Xen, permit two methods for making virtual organizations: crossed over and directed, but these procedures make it simpler to do assaults.

N. Examination of safety issues in distributed computing

We inspect the current security shortcomings and perils related with distributed computing in a deliberate way. We figure out which cloud administration models are impacted by these security issues for each shortcoming and risk.

Table 2 shows a weakness examination in Cloud Computing. This exploration gives a short outline of the weaknesses just as a rundown of cloud administration models (SPI) that might be affected. We principally center around innovation-based weaknesses in our review; nonetheless, there are extra weaknesses that are normal to each business and should be considered since they may think twice about security of the cloud and its hidden stage. Coming up next are a couple of instances of these imperfections:

- Absence of representative screening and poor selecting strategies - certain cloud suppliers may not attempt record verifications on their laborers or suppliers. Cloud overseers and other favored clients regularly have unhindered admittance to cloud information.
- Nonattendance of client individual examinations - most cloud providers don't lead individual confirmations on their clients, and basically anyone with a substantial charge card and email address might build up a record. Assailants can utilize imaginary records to complete any destructive exercises without being distinguished.
- Absence of safety training – people is still weakness in data security. This is valid in any association; however, it has a more prominent impact in the cloud.
- Various current progressions, for instance, web organizations, internet browsers, and virtualization, are utilized in distributed computing, adding to the development of cloud conditions. Therefore, every weakness connected with these advancements affects the cloud, and it could be extreme.
- We could find that data accumulating and virtualization are the hugest, and that an assault on them would actually hurt. Lower-layer attacks influence higher-layer attacks. We put a more noteworthy accentuation on weaknesses connected with information stockpiling and handling in the cloud, asset sharing, and virtualization.

The goal of this examination is to discover some current protections that can counter these dangers. Abuse designs can be utilized to address this data in a more careful manner.

According to the aggressor's point of view, misuse designs clarify how an abuse is completed. During live movement, an aggressor can access or mess with the substance of the VM state documents, for instance, in danger T10. This is possible on the grounds that VM movement sends information through unstable organization channels like the Internet. The accompanying methodologies can be utilized to decrease unreliable VM relocation: TCCP considers the private execution of virtual machines just as protected movement techniques. PALM [64] presents a solid movement strategy that takes into account live VM relocation when a VMM-secured framework is available and functional. Another cloud danger is Threat 11, which includes an assailant making a malignant., extra VMs made with this pernicious VM picture will be tainted also. Illusion, a picture the executive’s framework, was intended to balance this risk. Access control structure, picture channels, provenance global positioning framework, and storehouse upkeep administrations are among the security the executives highlight it offers.

O. Countermeasures

Except for dangers T02 and T07, we offer a concise rundown of every countermeasure portrayed before in this segment. The CSA is a non-benefit affiliation focused on progressing acknowledged systems. Brought together catalog, access the executives, personality the board, job-based admittance control, client access testaments, favored client and access the board, division of assignments, and character and access revealing are completely shrouded in this review. Tells the best way to build up unique qualifications for portable distributed computing stages utilizing a calculation. At the point when a client changes their area or trades a particular measure of

information bundles, the unique qualification's worth changes. This methodology plans to give interruption resistance just as protected stockpiling, therefore. This strategy involves separating touchy material into insignificant parts, with each section containing no significant data all alone. The pieces are then scattered all through the circulated framework's various destinations in an excess way.

While information is being sent over the Internet, suggests using computerized marks and the RSA technique to ensure information. They said that RSA is most remarkable method and used to get data in cloud settings. Move, store, and cycle are the three primary elements of cloud information. To deal with scrambled information, cloud organizations should decipher it, raising stresses over security. They suggest in a solution for cloud security reliant upon the usage of totally homomorphic encryption. Completely homomorphic encryption permits ciphertexts to be registered without being decoded. A couple homomorphic activities like expansion and augmentation are upheld by current homomorphic encryption frameworks. The creators of introduced a few instances of genuine cloud applications that need specific central homomorphic processes. Notwithstanding, it requires a lot of registering power which could tone down client reaction.

For quite a while, encryption strategies have been utilized to ensure touchy information. Information will be secured in the event that it is sent or put away scrambled on the cloud. It is valid, notwithstanding, in the event that the encryption strategies are powerful. Some encryption calculations are notable, like AES (Advanced Encryption Standard). SSL innovation may likewise be utilized to get information on the way.

Web applications are available to people in general, including planned aggressors; they may be an obvious objective. It's a procedure for ensuring hypervisor control-stream consistency. They showed up at the goal that HyperSafe was productive in thwarting these assaults and that the display above was immaterial. Suppliers can offer shut box execution conditions utilizing TCCP, and buyers can check in the event that the climate is protected prior to beginning their virtual machines. A believed virtual machine screen (TVMM) and a believed facilitator are two fundamental parts of the TCCP (TC). The TC is a confided in outsider that controls a gathering of reliable hubs that run TVMMs. The TC participates in the send-off or relocation of a virtual machine, guaranteeing that it runs on a protected stage. As per the creators in, TCCP has a considerable detriment since all exchanges should check with the TC, causing an over-burden. To resolve the issue, they suggested utilizing Direct Anonymous Attestation (DAA) and the Privacy CA strategy.

In cloud conditions, TVDc guarantees seclusion and respectability. Believed Virtual Domains are jobs that bunch virtual machines with comparative objectives (TVDs). TVDc upholds required admittance control, hypervisor-based detachment, and secured correspondence courses like as VLANs to empower responsibility isolation. Uprightness is given through TVDc, which utilizes a heap time confirmation strategy to approve the framework's honesty. The creators of propose a distributed computing based virtual machine picture the board framework. Access control structure, picture channels, provenance following, and store support administrations are a portion of the security components remembered for this strategy. Notwithstanding, channels will most likely be unable to distinguish all infections or erase all touchy information from the photos, which is a disadvantage of this method. Moreover, in light of the fact that these channels approach the substance of the photographs, which might contain private data about clients, they might make protection concerns. Presents a strong live migration designing that guarantees data decency and security during and later development.

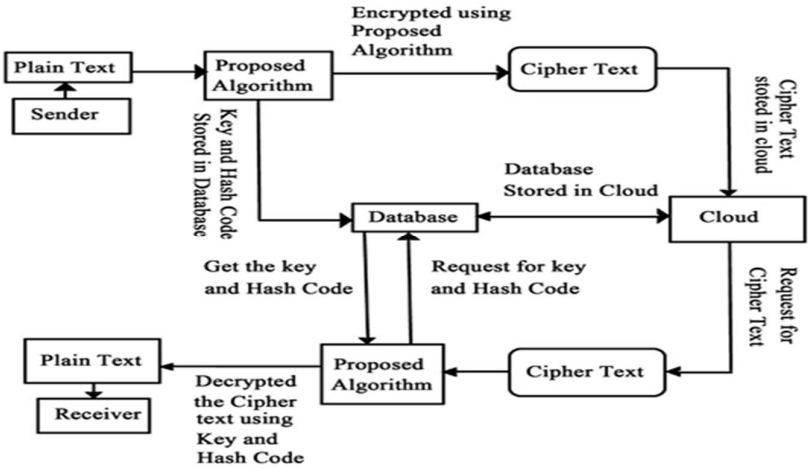

Figure 2: Encryption-Description Model in Cloud Computing

They utilized stateful firewall innovations and user space apparatuses including iptables, xm orders, and contract-instruments to fabricate a model framework dependent on Xen hypervisors. The creators ran a few tests to perceive how well their structure functioned, and the outcomes showed that security controls are set up all through live movement. A virtual organization system is introduced by Wu and et al., which ensures correspondence between virtual PCs. At the point when this paper was delivered, no assessment of this procedure had been finished. Moreover, in cloud settings, web administrations are the most frequently utilized execution procedure.

III. CONCLUSIONS

Distributed computing is a generally novel thought that offers an assortment of benefits to its clients; all things considered, it likewise raises specific security worries that might restrict its utilization. Understanding the shortcomings in Cloud Computing will help associations in rolling out the improvement to the Cloud. Another issue is that there are a few kinds of virtualization advances, every one of which approaches security systems in an unexpected way. A few assaults target virtual organizations, particularly while interfacing with far off virtual PCs.

To decrease these risks, a few contemporary cures were likewise introduced. New security draws near, just as adjusted regular arrangements that are viable with cloud foundations, are required. Since cloud engineering is a muddled design comprised of an assortment of advancements, conventional safety efforts may not perform successfully in these circumstances.

REFERENCES

[1] Gartner Inc: Gartner identifies the Top 10 strategic technologies. (2011). Online Available: Accessed:15-Jul 2011 http://www.gartner.com/it/page.jsp?id=1454221.

[2] N. Sharma, Prabhjot, & H. Kaur. (2017). A Review of Information Security using Cryptography Technique. International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, pp. 323-326.

[3] B. Preneel. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. London: Springer.

[4] Marshall Ball, Dana Dachman-Soled, & Mukul Kulkarni. (2020). New techniques for zero-knowledge: Leveraging inefficient provers to reduce assumptions, interaction, and trust. Daniele Micciancio and Thomas Ristenpart, editors, CRYPTO2020, PartIII, volume 12172 of LNCS, pages 674–703. Springer, Heidelberg.

[5] Shohei Egashira, Yuyu Wang, & Keisuke Tanaka. (2019). Fine-grained cryptography revisited. StevenD. Galbraith and Shiho Moriai, editors, ASIACRYPT2019, PartIII, volume 11923 of LNCS, pages 637–666. Springer, Heidelberg.

[6] Paulo S. L. M. Barreto. (2017). The WHIRLPOOL Hash Function.

[7] Saarinen, M-J; Aumasson, & J-P. (2015). The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). IETF. doi:10.17487/RFC7693. RFC 7693. Retrieved 4.

[8] J. Dittman, P. Wohlmacher and K. Nahrstedt, 2001 “Using Cryptographic and Watermarking Algorithms” IEEE Multimedia, vol. 8, no. 3, PP. 54-65.

[9] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X & Tang N. (2009). Cloud Computing: A Statistics Aspect of Users. International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 347–358.

[10] Zhang S, Zhang S, Chen X & Huo X. (2010). Cloud Computing Research and Development Trend. International Conference on Future Networks (ICFN’10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 93–97.

[11] Cloud Security Alliance. (2011). Security guidance for critical areas of focus in Cloud Computing. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[12] Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin; 2009.

[13] Centre for the Protection of National Infrastructure: Information Security Briefing 01/2010 CloudComputing..2010. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

[14] Khalid A: Cloud Computing: applying issues in Small Business. International Conference on Signal Acquisition and Processing (ICSAP’10) 2010, 278–281.

[15] KPMG: From hype to future: KPMG’s 2010 Cloud Computing survey. 2010. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291

[16] Rosado DG, Gómez R, Mellado D, Fernández-Medina E: Security analysis in the migration to cloud environments. Future Internet 2012, 4(2):469–487.

[17] Mather T, Kumaraswamy S, Latif S: Cloud Security and Privacy. Sebastopol, CA: O’Reilly Media, Inc.; 2009.

[18] Li W, Ping L: Trust model to enhance Security and interoperability of Cloud environment. In Proceedings of the 1st International conference on Cloud Computing. Beijing, China: Springer Berlin Heidelberg; 2009:69–79.

[19] Rittinghouse JW, Ransome JF: Security in the Cloud. In Cloud Computing. Implementation, Management, and Security, CRC Press; 2009.
[20] Kitchenham B: Procedures for performing systematic review, software engineering group. Australia: Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd; 2004. TR/SE-0401 TR/SE-0401
[21] Kitchenham B, Charters S: Guidelines for performing systematic literature reviews in software engineering. Version 2.3 University of keele (software engineering group, school of computer science and mathematics) and Durham. UK: Department of Computer Science; 2007.
[22] Brereton P, Kitchenham BA, Bugden D, Turner M, Khalil M: Lessons from applying the systematic literature review process within the software engineering domain. J Syst Softw 2007, 80(4):571–583. 10.1016/j.jss.2006.07.009
[23] Cloud Security Alliance: Top Threats to Cloud Computing V1.0. 2010. Available: https://cloudsecurityalliance.org/research/top-threats
[24] ENISA: Cloud Computing: benefits, risks and recommendations for information Security. 2009. Available: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
[25] Dahbur K, Mohammad B, Tarakji AB: A survey of risks, threats and vulnerabilities in Cloud Computing. In Proceedings of the 2011 International conference on intelligent semantic Webservices and applications.
[26] Ertaul L, Singhal S & Gokay S. (2010). Security challenges in Cloud Computing. International conference on Security and Management SAM'10. Las Vegas.
[27] Grobauer B, Walloschek T & Stocker E. (2011). Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 2011, 9(2):50–57.