LITERATURE REVIEW: AGENT BASED DATA SECURITY APPROACH FOR HYBRID CLOUD COMPUTING

SHRAVYA SUDHA O

PG Scholar, Dept of CSE

Cambridge Institute of Technology

Bengaluru, India

Shravya.19scs10@cambridge.edu.in

PANKAJA K

Associate professor, Dept of CSE

Cambridge Institute of Technology

Bengaluru, India

Abstract:

As the cloud computing is spreading around the world, need of inter cloud communication is becoming a growing in the organizations. It is causing the researchers to focus on first, for making it possible to communicate between two or more clouds and second security of communication is to considered up to utmost level. Hybrid Cloud computing mainly deals with working of data centers where different software are installed with huge of growing data to provide information to the users of the system. The techniques which can be used in hybrid cloud securities can be built around the encryption and decryption of data, key based security algorithms which are mainly oriented on authentication and authorization techniques as in wired and wireless networks. One such mechanism is to share the challenge text between the clouds before actual communication should start for authentication. The various works done in this area till date are oriented on other techniques ofsecurity between the two or more clouds in a hybrid cloud.

Keywords:

Cloud computing; Hybrid cloud; Challenge text; Security.

1. Introduction:

Cloud computing is becoming a buzz word in computer industry and everyone is looking to associate in one way or other with this brand new concept. Cloud computing is a very current topic and the term has gained a lot of traction being sported on advertisements all over the Internet from web space hosting providers, through data centers to virtualization software providers search complex technology. Such complex technology and business models setting entails an extensive research and provides the motivation towards writing this paper. With emergence of cloud computing, the term "Hybrid Topology" or "Hybrid Deployment" is becoming more and more common. Definition of "Hybrid Topology" is when you join different cloud deployments into one connected cluster. Another area of research is to focus on communication between a cloud and non cloud computing system. The main goal is to “clear the air on hybrid cloud computing security” and provide an unbiased and independent, albeit critical outlook of the technology. Special emphasis is put on the critical examination of each strategy as now more than ever inthe face of the global economic crisis, companies face higher refinancing and investment costs and as any company thinking about adopting or moving to cloud computing technology would do in practice. Short-to medium term disadvantages of the technology have to be pragmatically and carefully weighted out against any hyped long-term potential efficiency achievements be it strategic, technical or cost related [1]. In order to understand the vision, goals and strategy behind cloud computing, two key concepts that form its foundations need to be explained first.

Autonomic computing, the term initially being introduced by IBM's Senior Vice President Paul Horn to the National Academy Engineers at Harvard University in 2001, represents a research aim towards achieving, self-managing, computing- systems, whose components integrate effortlessly. Utility computing is the second key concept that one computing power will be offered as a standardized service billed on actual usage with very limited or no upfront set-up charges.

2. Cloud Computing Definitions:

A scientific definition is proposed by the GRIDSLab at the University of Melbourne:"A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreement established through negotiation between the service provider and consumers." Berkeley's defines it as:"Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services (Software as a Service -SaaS). The data centres hardware and software is what we will call a Cloud. When a Cloud is made available in a pay- as-you-go manner to the public, we call it a Public Cloud; the service being sold is Utility Computing." [1] Building blocks of cloud computing:

- **i.** Storage-as-a-Service
- **ii.** Database-as-a-Service
- **iii.** Information-as-a-Service
- **iv.** Process-as-a-Service
- **v.** Application-as-a-Service
- **vi.** Integration-as-a-Service
- **vii.** Security-as-a-Service
- **viii.** Management/Governance-as-a-Service
- **ix.** Testing-as-a-Service

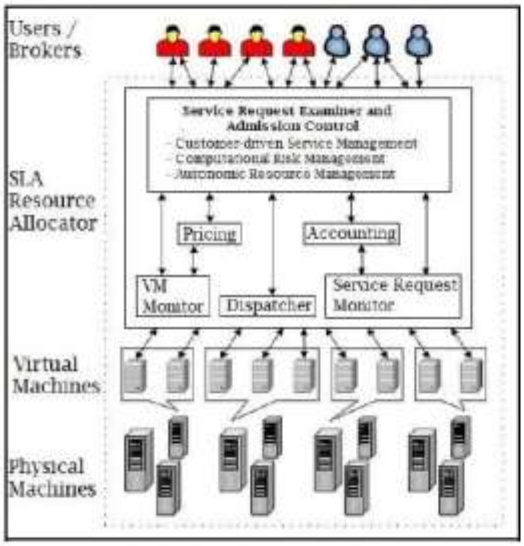
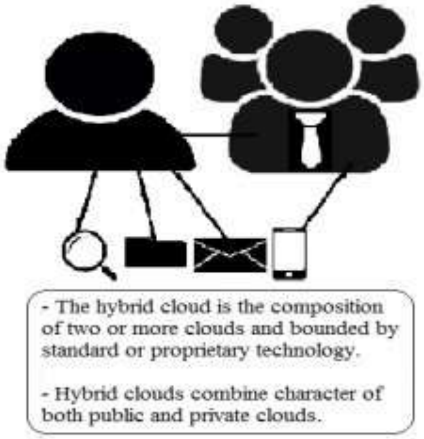

Users / Brokers
Service Request Examiner and Admission Control
- Customer-driven Service Management
- Computational Risk Management
- Autonomic Resource Management
SLA Resource Allocator
Pricing
Accounting
VM Monitor
Dispatcher
Service Request Monitor
Virtual Machines
Physical Machines

Fig1. Cloud Computing

3. Hybrid Cloud Computing

A hybrid cloud is a composition of at least One private cloud and at least one public cloud. A hybrid cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms. A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in- house storage for operational customer data. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities. This type of hybrid c loud is also referred to as hybrid IT.



- The hybrid cloud is the composition of two or more clouds and bounded by standard or proprietary technology.

- Hybrid clouds combine character of both public and private clouds.

Fig2. Hybrid Cloud Computing

4. Challenges in hybrid Cloud

Here are some challenges to consider when setting up hybrid clouds:

i. On Demand Start-up and Shutdown:

Your infrastructure must be able to start up and shut down cloud nodes on demand. Usually you should have some policy implemented which listens to some ofyour application characteristics and reacts to them by starting or stopping cloud nodes. In simplest case, you can react to CPU utilization and start up new nodes if main cloud gets overloaded and stop nodes if it gets under loaded.

ii. Cloud-based Node Discovery:

The main challenge in setting up regular discovery protocols on clouds is that IP Multicast is not enabled on most of the cloud vendors (including Amazon and Go Grid). Your node discovery protocol would have to work over TCP. However, you do not know the IP addresses of the new nodes started on the cloud either. To mitigate that, you should utilize some of the cloud storage infrastructure, like S3 or Simple DB on Amazon, to store IP addresses of new nodes for automatic node detection.

iii. One-Directional Communication:

One of the challenges in big enterprises is Opening up new ports in Firewalls for connectivity with clouds. Quite often you will only be allowed to make only out going connections to a cloud. Your middleware should support such cases. On top of that, sometimes you may run into scenario of disconnected clouds where cloud A can talk to cloud B, and cloud B can talk to cloud C, however cloud A cannot talk to cloud C directly. Ideally in such case cloud A should be allowed to talk to cloud C through cloud B.

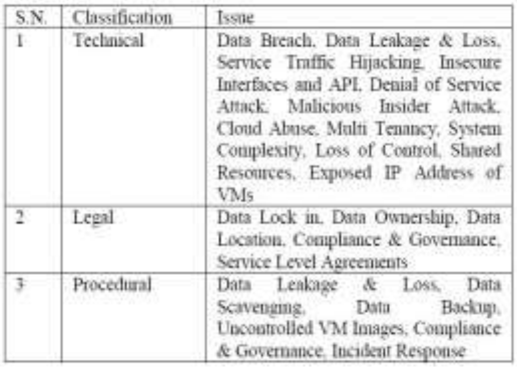
iv. Latency

Communication between clouds may take Longer than communication between nodes within the same cloud. Often, communication within the same cloud is significantly slower than communication within local data centre. Your middleware layer should properly react to and handle such delays without breaking up the cluster into pieces.

v. Reliability and Atomicity:

Many operations on the cloud are unreliable and non-transactional. For example, if you store something on Amazon S3 storage, there is no guarantee that another application can read the stored data right away. There is also no way to ensure that data is not over written or implement some sort of file locking. The only way to provide such functionality is at application or middleware layers.

Table1: Classification of Information Security Issues in cloudcomputing.



S.N.	Classification	Issue
1	Technical	Data Breach, Data Leakage & Loss, Service Traffic Hijacking, Insecure Interfaces and API, Denial of Service Attack, Malicious Insider Attack, Cloud Abuse, Multi Tenancy, System Complexity, Loss of Control, Shared Resources, Exposed IP Address of VMs
2	Legal	Data Lock in, Data Ownership, Data Location, Compliance & Governance, Service Level Agreements
3	Procedural	Data Leakage & Loss, Data Scavenging, Data Backup, Uncontrolled VM Images, Compliance & Governance, Incident Response

5. Study of Related Frameworks:

i. Data Security and Authentication in Hybrid Cloud Computing Model:

This paper describes several methods to protect user data, which includes single encryption, multi-level virtualization, and authentication-interface. Authentication intercloud is the other main theme of this paper. This paper also discussed a model of authentication inter cloud which based on CA and PKI model which be extended to the scenario without CA system or it crashed.

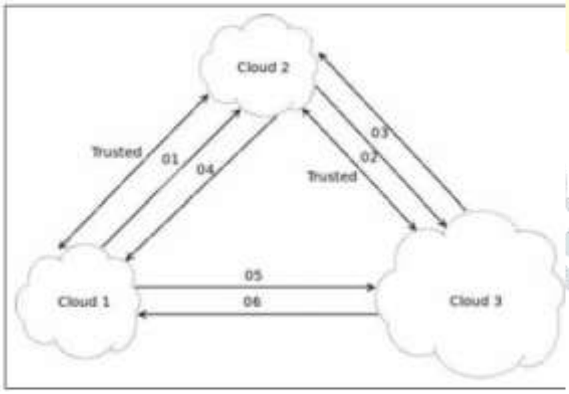


Fig.3. Generalization of the Authentication Model

Here is a generalization of the authentication model. In figure 8, there is a scenario that cloud 1 is already trust cloud 2, and cloud 2 is already trust cloud 3. Now cloud 1 wishes to extend its computing capacity via connect another cloud. Here cloud 2 has some reason that cannot connect to cloud1, so the cloud 1 has to find another cloud to connect.

The cloud 1 first send a request to cloud 2 for another trustable cloud, the cloud 2 will check its trust list to find a cloud it trusts. Like the situation in the figure, the cloud 2 finds that cloud 3 could be trusted, so it will send a request to cloud 3 to find whether it could provide connection to other cloud. The cloud 3 has the extra capacity so it will send the answer to cloud 2. Then the cloud 2 will send the information about cloud 3 to cloud 1, meanwhile the cloud 3 will send the information about itself to cloud 1.Cloud 1 will check the information from cloud 2 and cloud 3, if they are same, the cloud 3 could be trust by cloud 1. And the process of the authentication will finish, and if the information is not same, the cloud 3 would not be trusted bycloud 1.

ii. Hybrid two-tier framework for improved security in cloud environment:

Cloud computing has already grabbed its roots in IT industry. It has become an appealing choice for small budget organizations since on demand resources are available on pay as you use basis. However, security of data being stored at cloud servers is still a big question for organizations in today’s digital era where information is money. Large organizations are reluctant to switch to cloud services since they have threat of their data being maltreated. Cloud service provider’s claim of providing robust security mechanism being maintained by third party, but still there are many reported incidents of security breach in cloud environment in past few years. Thus there is need of robust security mechanism to be adopted by cloud service providers in order for excelling cloud computing.

This work proposes a hybrid two-tier agent based framework which deploys symmetric and asymmetric key algorithms in combination to provide robust security to user data. Further, this mechanism provides data decryption control to user only, thereby eliminating threat of data being misused by cloud service provider. Both cryptography algorithms being used in this work, have proved excellence for small key size, small encryption time and high speed, thus this framework would increase security without affecting processing speed of virtual machine

Main motive of this security mechanism is to provide strong security of data placed in cloud and to ensure that even CSP can't breach this security. However, it is well known fact that as complexity of encryption mechanism is increased, security increase but efficiency of the system decreases. To remove this problem, this work proposes combined use of two encryption algorithms having smaller key sizes to provide stronger security than existing. As far as threat of security breach from CSP is concerned, security mechanism must provide data decryption control to user only, even CSP should not be able to decrypt data in any way; it is possible with use of symmetric key cryptography; however in case of symmetric key algorithm complexity is less but security is also low. Whereas in case of asymmetric key algorithms complexity is more and security of data while travelling in network is also more. However, if asymmetric key mechanism is opted in CC, then one part of key would be saved with CSP, which is a constant threat for the users.

Proposed mechanism presents hybrid two tier security engine henceforth termed as HT2SE, it is an agent based framework which uses both types of encryption i.e. symmetric and asymmetric in combination before sending data to CSP. This mechanism has two layers, first layer makes use of symmetric key algorithm i.e. Blowfish to encrypt data, this key would only be known to the user. Output of the first layer would be processed by second layer, which would again encrypt it with asymmetric key ECC, for this layer ECC private key will be with user and corresponding public key will be with CSP. Figure 1. given below provides high level view of HT2SE architecture where first layer makes use of symmetric key algorithm BF and second layer makes use of asymmetric key algorithm ECC.

iii. Security Solution for Hybrid Cloud Information Management Using Fuzzy Deductive Systems:

The computing technology growing in an effective way by utilizing the cloud services as a backbone, tremendous amount of information is generated everyday from multiple sources. This Information stored under distinct data centre as a collaborated service nature of computing technology. Hybrid cloud model will hold the business critical content securely over on-premises cloud data centres to process consumer grade level alternative solutions. However, there will be a process specific security controls in the content-specific environments need to be established. It is important to manage all generic type of information and its sources in hybrid cloud access platform. Hybrid cloud platform deals with the various business insights, which increases the volume cloud systems. Any private and public cloud service users can request the service from the cloud and use it as a model of on demand services. It is necessary to monitor and regulate the data security systems for controlling unauthorized access from malicious intruder of the data. So, the proposed system will brings the solution of secured information management in hybrid cloud service model. The proposed work can be implemented and tested over the cloud analyst simulator. The results show that better outcomes based on the fuzzy inferences.

The hybrid cloud management model will provide the infrastructure for private and public cloud services will run their client applications, and analyzing the security patterns along with data management solutions across the cloud servers. Any enterprise that will leverage all the services, generic service products and managing clients level information on the hybrid cloud system. It is must to know how the applications, legacy systems, software and storage components are processed under the defined security boundaries. Hybrid cloud system will determine how the services are widely used by the customers and type of security access patterns are followed by the service provider at the client location. There will be an API's, and interface can navigate the user applications and evaluate the performance level of secured information access management. There are many management level processes which are listed below:

i. API management
ii. Resource management
iii. Cloud management platforms
iv. Performance management
v. DevOps management
vi. Security management
vii. Network management
viii. Native platform management

iv. Enhancing Cloud Data Security using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms:

Cloud computing is an IT model that offers a large number of storage space, unbelievable computing power and inconceivable speed of calculations. There are a number of costumers like corporate components, social media programs and individual customers are all moving towards to the vast area of cloud computing. The importance of cloud computing comes outwith the security of data accessibility, reliability and reliability of information. The verification and permission is more necessary to access information as "cloud" is only assortment of actual supercomputer speed through the world. There are many research has been done on security of file encryption with AES algorithm.

There is no any successful attack yet against AES but because of a higher increasing of cybercrime it could be possible attack on it like brute force attack and algebraic attack. Hence, in this research has been proposed a hybrid structure of Dynamic AES (DAES) and Blowfish algorithms. This procedure specifies the security of uploaded file on the cloud with a strong encryption method and also the privacy and reliability of submitted information of a user with considering performance of speed. We endorse a configuration in this unit that hold a securing of Information file which is existing on the information file will be secured based on hybrid of DAES and Blowfish algorithms To make the AES more secure will enhance slightly in s-boxstructure. At first will do the transformation and then will process the inverse of multiplication. It could be more secure to AES to break the key by a third party. Thus the client cans attainany of the submitted encrypted files and study on it. The benefits of hybrid of DAES and Blowfish are many again stun believable power attack. The security key dimension used by AES criteria is of the order of the 128,198 or 256 bits which out comes in massive amount of permutation and mixtures because of this, it is not an easy job the incredible power attack even for an extremely computer.

Where Blow fish has 64-bit block size and the key lengthv aries from 32 bits until 448 bits. It uses large key dependent S-boxes as well as experience a 16 round Fiestel cipher process. In this work blowfish will be useful to extend the keysize. Thus, its make an excellent choice for security of information on the cloud.

V. Enhanced Model for Cloud Data Security based on Searchable Encryption and Hybrid Fragmentation:

The main idea of encryption algorithms for cloud data is to permit cloud clients queries to be handled using encrypted data without decryption. This paper presents a new security mechanism using hybrid method of encryption algorithms and a distribution system to enhance cloud database confidentiality. A vertical fragmentation technique is adopted from alsirhani's model for distributing data over clouds. However, to overcome a weakness in alsirhani's model where compromises to a fragment can still make data meaningful. Instead, the proposed model uses a hybrid fragmentation technique to make data on fragments meaningless if compromised. The proposed model distributes the cloud database among the clouds using the provider views and level of confidentiality that is delivered by the employed encryption algorithms. To evaluate the proposed searchable encryptionand hybrid fragmentation model, the study developed a Java application for simulating the hybrid cloud. The simulation combines public and private clouds; as essential processes is conducted inside the private cloud. The evaluation of the work was conducted by comparing the proposed model with existing solutions in query response and security characteristics. Preliminary results showed that the proposed searchable encryption and hybrid fragmentation model provides a secure mechanism that enhances data confidentiality in terms of faster response and additional security.

The research followed mixed design methodology. Firstby applying qualitative strategies to design the proposed model in Java programming language. This wasachieved through literature review on searchable encryption algorithms and fragmentation techniques that can enhance data isolation in cloud to provide the hybrid fragmentation technique for data distribution instead of vertical fragmentation (as in Alsirhani’s model). The simulation of Alsirhani’s was also developed in Java and quantitative strategies were used to test the model (that is, calculate and compare query responses in milliseconds).

The evaluation of the proposed model involved a qualitative component wherea desk-based comparison of security characteristics was performed to compare with Alsirhani's and Popa's models.

6. Proposed Methodology

Agent Based Information Security Framework for Hybrid Cloud Computing:

This paper proposes Agent Based Information Security Framework for Hybrid Cloud Computing as an all- inclusive method including cloud related methods to review and compare existing different renowned methods for cloud computing risk issues and by adding new tasks from surveyed methods. The concepts of software agent and intelligent agent have been introduced that fetch/collect accurate information used in framework and to develop a decision system that facilitates the organization to take decision against threat agent on the basis of information provided by the security agents. The scope of this research primarily considers risk assessment methods that focus on assets, potential threats, vulnerabilities and their associated measures to calculate consequences. After in-depth comparison of renowned ISRA methods with ABISF, we have found that ISO/IEC 27005:2011 is the most appropriate approach among existing ISRA methods. The proposed framework was implemented using fuzzy inference system based upon fuzzy set theory, and MATLAB® fuzzy logic rules were used to test the framework. The fuzzy results confirm that proposed framework could be used for information security in cloud computing environment.

i.Agents Based Information Security Framework

The most critical roadblock in the development of Cloud Computing is its security and privacy constraints. Although every vender claims that it is providing adequate security to its customers and various research efforts have been made to cater the needs of security in Cloud computing, but still it is a great challenge for the Cloud organizations. Security risks and threats always directly decrease the operational processes of the organization. During literature review, it is extracted that various Information Security frameworks exist but none of the Information Security framework use Software Agents and Intelligent Agents technology to meet the challenges of Information Security.

In this paper, we introduced Software Agents to formulate Information Security framework and used Information Security Metrics that is a valuable tool to measure the performance of the Information Security System. Furthermore, risk management techniques are also used to define the severity level of the risk. In order to provide Information Security to the Cloud customers and venders, a four stages approach is proposed.

7. Conclusion and Future Work

Since cloud connects to thousand and thousand of people over internet or intranet on pay perbasis, therefore security of the cloud is a focused are for researchers and with the growth of the cloud computing and hybrid computing, requirements for security are increasing heavily. The proposed work is expected toprovide a good security infrastructure over cloud. One mechanism is to share the challenge text between the clouds before actual communication should start for authentication. The various works done in this area till date are oriented on other techniques of security between the two or more clouds in a hybrid cloud. Cloud Computing is facilitating users around the world for the best of the services available across the world on their machines through web. It is beneficial for both the service providers (they get huge clientele) and clients (they get all available services). For data security and privacy protection issues, the fundamental challenges are separation of sensitive data and access control. Our objective is to designa set of unified identity management and privacy protection frameworks across applications or cloud computing services. As mobility of employees in organizations is relatively large, identity management system should achieve more automatic and fast user account provisioning and de-provisioning in order to ensure noun-authorized access to organizations' cloud resourcesby some employees who has left the organizations.

8.References

[1] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," IEEE Access, vol. 4, pp. 1375–1384, 2016.

[2] R. Sharma and R. K. Trivedi, "Literature review: Cloud Computing – Security Issues, Solution and Technologies," International Journal of Engineering Research, vol. 3, no. 4, pp. 221–225, Jan. 2014

[3]P. Samarati and S. D. C. D. Vimercati, "Cloud Security," Encyclopedia of Cloud Computing, pp. 205–219, 2016.

[4]V. Chang, Y.-H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," Future Generation Computer Systems, vol. 57, pp. 24–41, 2016.

[5]V.Arora and S. Tyagi, "Analysis of Symmetric Searchable Encryption and Data Retrieval in Cloud Computing," International Journal of Computer Applications, vol. 127, no. 12, pp. 46–51,
2015.

[6]A. Mehmood, H. Song, and J. Lloret, "Multi-Agent based Framework for Secure and Reliable Communication among Open Clouds," Network Protocols and Algorithms, vol. 6, no. 4, p. 60, 2014

[7]M. I. Tariq and V. Santarcangelo, "Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing," in Proc. of the 2nd International Conference on Information Systems Security and Privacy, pp. 201–208, 2016

[8]A. M. Talib and N. E. M. Elshaiekh, "Multi Agent System-Based on Case Based Reasoning for Cloud Computing System," Academic Platform Journal of Engineering and Science, vol. 2, no. 2, pp. 34–38, 2014.

[9]V.Rybakov, "Multi-agent Non-linear Temporal Logic with Embodied Agent Describing Uncertainty," Advances in Intelligent Systems and Computing Agent and Multi-Agent Systems: Technologies and Applications, pp. 87–96, 2014.

[10]J. Yang, J. Wang, H. Wang, and D. Yang, "Agent-based provable data possession scheme for mobile cloud computing," Journal of Computer Applications, vol. 33, no. 3, pp. 743–747,
2013.

[11]T. K. Damenu and C. Balakrishna, "Cloud Security Risk Management: A Critical Review," in Proc. of 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015.

[12]X. Yang, "Framework development in plant disease risk assessment and its application," Plant disease epidemiology: facing challenges of the 21st Century, pp. 25–34.

[13]K. Sadgrove, The complete guide to business risk management. Abingdon, Oxon: Routledge, 2016.

[14]S. Fenz, J. Heurix, T. Neubauer, and

F. Pechstein, "Current challenges in information security risk management," Information Management & Computer Security, vol. 22, no. 5, pp. 410–430, Oct. 2014.

[15]A. Rot and B. Olszewski, “Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection,” in Proc. of Position Papers of the 2017 Federated Conference on Computer Science and Information Systems, 2017.

[16]M. W. Harkins, “Emerging Threats and Vulnerabilities: Reality and Rhetoric,” Managing Risk and Information Security, pp. 81–98, 2016. Article (CrossRef Link) [38]M. Harkins, “Emerging Threats and Vulnerabilities,” Managing Risk and Information Security, pp. 71–85, 2013.

[17]P. Shamala, R. Ahmad, and M. Yusoff, “A conceptual framework of info structure for information security risk assessment (ISRA),” Journal of Information Security and Applications, vol. 18, no. 1, pp. 45–52, 2013.

[18]G. Wangen, “Conflicting Incentives Risk Analysis: A Case Study of the Normative Peer Review Process,” Administrative Sciences, vol. 5, no. 4, pp. 125–147, Sep. 2015.

[19]E. Snekkenes, “Position Paper: Privacy Risk Analysis Is about Understanding Conflicting Incentives,” Policies and Research in Identity Management IFIP Advances in Information and Communication Technology, pp. 100–103, 2013.

[20]C. Yang, “Projects Bidding Decision Risk Analysis Based on Multi-factor Clustering Analysis,” Information Technology Journal, vol. 12, no. 21, pp. 6164–6168, Jan. 2013.

[21]P. Shamala and R. Ahmad, “A proposed taxonomy of assets for information security risk assessment (ISRA),” in Proc. of 2014 4th World Congress on Information and Communication Technologies (WICT 2014), 2014

[22] A. Alsirhani, P. Bodorik, and S. Sampalli, "Improving databasesecurity in cloud computing by fragmentation of data," in 2017International Conference on Computer and Applications (ICCA), 2017, pp. 43-49.

[23] M. Elsayed and M. Zulkernine,Offering security diagnosis as a service for cloud SaaS applications," Journal of information securityand applications, vol. 44, pp. 32-48, 2019.

[24]I. Anikin and L. Y. Emaletdinova, “Information security risk management in computer networks based on fuzzy logic and cost/benefit ratio estimation,” Proceedings of the 8th International Conference on Security of Information and Networks - SIN 15, 2015.

.

[25]H. Karlzén, J. Bengtsson, and J. Hallberg, “Assessing Information Security Risks using Pairwise Weighting,” Proceedings of the 3rd International Conference on Information Systems Security and Privacy, 2017