International Journal of Pure and Applied Mathematics
Volume 117 No. 20 2017, 1021-1035
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

EFFICIENT APPROACHES FOR STORING RETRIVAL AND REPLICATION OF DATA USING CLOUD SYSTEM

Sonya A[1] Kavitha G[2]

[1]Assistant professor, [2]Associate Professor

[1,2]Department of Information Technology,

[1,2]B S Abdur Rahman Crescent University,Chennai,India.

email:sonya@bsauniv.ac.in, gkavitha.78@bsauniv.ac.in

Abstract- The security and performance are critical for the next generation large-scale systems, such as clouds. Therefore, in this paper, we collectively approach the issue of security and performance as a secure data replication problem. We present Detach and Reproduce of Data in the Cloud for Efficient Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not adjacent and are at a certain distance from each other. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time. To further improve the retrieval time, we judicially replicate fragments over the nodes that generate the highest read/write requests. The selection of the nodes is performed in two phases. In the first phase, the nodes are selected for the initial placement of the fragments based on the centrality measures. In the second phase, the nodes are selected for replication. After duplication, it will shuffle the fragments. When user requested, it will retrieve the whole information in a sequential order.

Keywords: security, fragments, computing, storage, cloud nodes.

I.INTRODUCTION

Cloud computing is innovation that uses advanced computational power and improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. The advantage of cloud is cost savings. The prime disadvantage is security. To ensure security, cryptographic techniques cannot be directly adopted. Sometimes the cloud service provider may hide the data corruptions to maintain the reputation. To avoid this problem, we introduce an effective third party auditor to audit the user's outsourced data when needed. The cloud computing paradigm has reformed the usage and management of the information technology infrastructure. Cloud computing is characterized by on-demand self-services, ubiquitous network accesses, resource pooling, elasticity, and measure services. The aforementioned characteristics of cloud computing make it a striking candidate for businesses, organizations, and individual users for adoption. However, the benefits of low-cost, negligible management and greater flexibility come with increased security concerns. Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud Computing. For a cloud to be secure, all of the participating entities must be secure. In any given system with multiple units, the highest level of the system. Security is equal to the security level of the weakest entity. Therefore, in a cloud, the security of the assets does not solely depend on an individual's security measure. The neighboring entities may provide an opportunity to an attacker to bypass the users' defenses. The off-site data storage cloud utility requires users to move data in cloud's virtualized and shared environment that may result in various security concerns. Pooling and elasticity of a cloud, allows the physical resources to be shared among many users. Moreover, the shared resources may be reassigned to other users at some instance of time that may result in data compromise through data recovery methodologies. The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes (whether accidental or deliberate) must be prevented. As

discussed above, any weak entity can put the whole cloud at risk. In such a scenario, the security mechanism must substantially increase an attacker's effort to retrieve a reasonable amount of data even after a successful intrusion in the cloud. Moreover, the probable amount of loss (as a result of data leakage) must also be minimized. A cloud must ensure throughput, reliability, and security. A key factor determining the throughput of a cloud that stores data is the data retrieval time. We present Detach and Reproduce of Data in the Cloud for Efficient Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (we use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not adjacent and are at a certain distance from each other. The node separation is ensured by the means of the FS-Algorithm. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time. To further improve the retrieval time, we judicially replicate fragments over the nodes that generate the highest read/write requests. The selection of the nodes is performed in two phases. In the first phase, the nodes are selected for the initial placement of the fragments based on the centrality measures. In the second phase, the nodes are selected for replication. After duplication, it will shuffle the fragments. When user requested, it will retrieve the whole information in a sequential order.

II.PROPOSED SYSTEM

In the proposed system the issue of security and performance as a secure data replication problem. To present Detaching and Reproduction of Data in the Cloud for Excellent Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a

file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (we use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. In addition we added two algorithms are used first one is FS-Drops (Fragment and Snuffle -Drops) Which will fragment a file into 4 pieces and shuffled (like 1-2, 2-3, 3-4, 4-1) And store in different server So in future some Server is not available are Hacked we can get back our original data from remaining Server. The second algorithm is Third Party Audit Cloud Server(TP-ACS), Time to time will audit our Storage Sever for Data Integrity, Also for Every Data Modification it will do audit So that the Storage Server Performance will not be affected and Data will be very Safe, data's sequential order will find easily.

Algorithm

1. FS-Drops (Fragment and Snuffle -Drops)
2. Third Party Audit Cloud Server(TP-ACS)

Fs-drops

This FS-Algorithm for file allocation that guarantees high assurance, availability, and scalability in a large distributed file system. The algorithm can use replication and fragmentation schemes to allocate the files over multiple servers. The file confidentiality and integrity are preserved, even in the presence of a successful attack that compromises a subset of the file servers. The algorithm is adaptive in the sense that it changes the file allocation as the read-write patterns and the location of the clients in the network change. In this FS-DROPS (Fragment and shuffle) algorithm will fragment a file into 4 pieces and shuffled (like 1-4, 2-3, 3-2, 4-1) And stored in different server. In future when the server is low or hacked by attackers, we can retrieve our original data by the rest of the server.

A.FS-DROPS ALGORITHM SPECIFICATIONS

i.Inputs and initializations

I = {I1;I2; :::;In} (I refers input)

S = {sizeof(I1); sizeof(I2); ::::; sizeof(In)}

Compute

Step1: start

Step2: select I

Step3: Check the S of I (Size of Input)

Step4: Split D = S (I)/4;

Step5: After split, I 1, I2, I3, I4 generated.

Step6: Replicate R (I1… I4)

Step7: Shuffle R& I

Step8: retrieve I1, I2, I3, I4

Step9: end

B. Third Party Audit Cloud Server (TP-ACS)

This algorithm will audit our Storage Sever for Data Integrity, and also audit if any modification will be done in data with the regular intervals of time. , So that the Storage Server Performance will not be affected and Data stored in the server also be much secured. Here, a third party can be used as an auditor. In cloud environment the computing resources are under control of service provider and the third-party-auditor ensures the data integrity over out sourced data. TPA used to protect the privacy and integrity of outsourced data. To ensure the correctness of data, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud., the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. It supports scalable and efficient

public auditing in the Cloud Computing. In particular, the TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data.

C. Third Party Audit Cloud Server Algorithm

Step1: Start the process

Step2: Client request to access a file from CSP.

Step3: CSP ask client for authentication like login page.

Step4: Client authentication CSP by his password

Step5: Verify password if correct than send a file that he want to access. Else move to step 2.

Step6: Client decrypts the file by applying RSA decryption algorithm.

Step7: If client modify the file than he will send file to TPA and CSP with a message like Md as (C'Ψs M) and C' here C' for encrypted file Ψs for ElGamal Digital Signature and M denotes for modification.

Step8: CSP check the signature for authenticity and compute the message digest to find encrypted file which is compare with encrypted file of another message.

Step9: If correct it will change previous file with this one end.

D. REQUIREMENT

SYSTEM REQUIREMENTS

Processor : Any Processor above 500 MHz

Ram : 512Mb

Hard Disk : 40 GB

Compact Disk : 650 MB

Input device : Standard Keyboard and Mouse

Output device : VGA and High Resolution Monitor

SOFTWARE REQUIREMENTS

Operating System : Windows Family

Front End : JAVA

Database : MySQL

E.UML DIAGRAMS

i. Class Diagram

It shows the object organization as shown below. Here in collaboration diagram the method call sequence is indicated by some numbering technique as shown below. The number indicates how the methods are called one after another. We have taken the same order management system to describe the collaboration diagram. The method calls are similar to that of a sequence diagram. But the difference is that the sequence diagram does not describe the object organization where as the collaboration diagram shows the object organization.

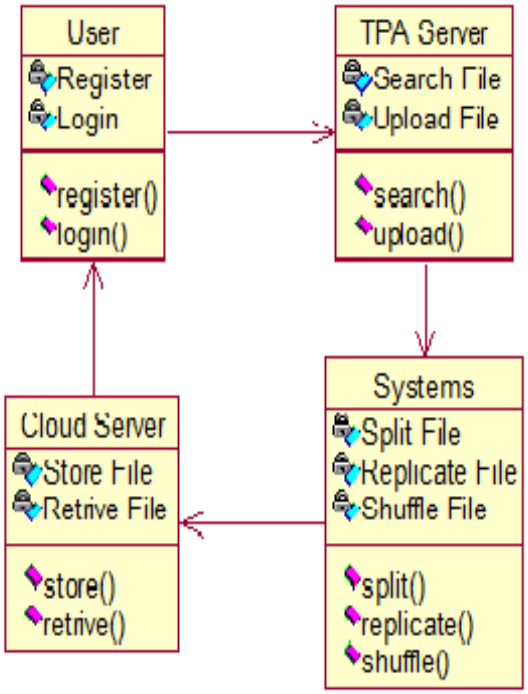

Fig 1.Class Diagram

F. Use Case Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those

use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted

i. Activity Diagram

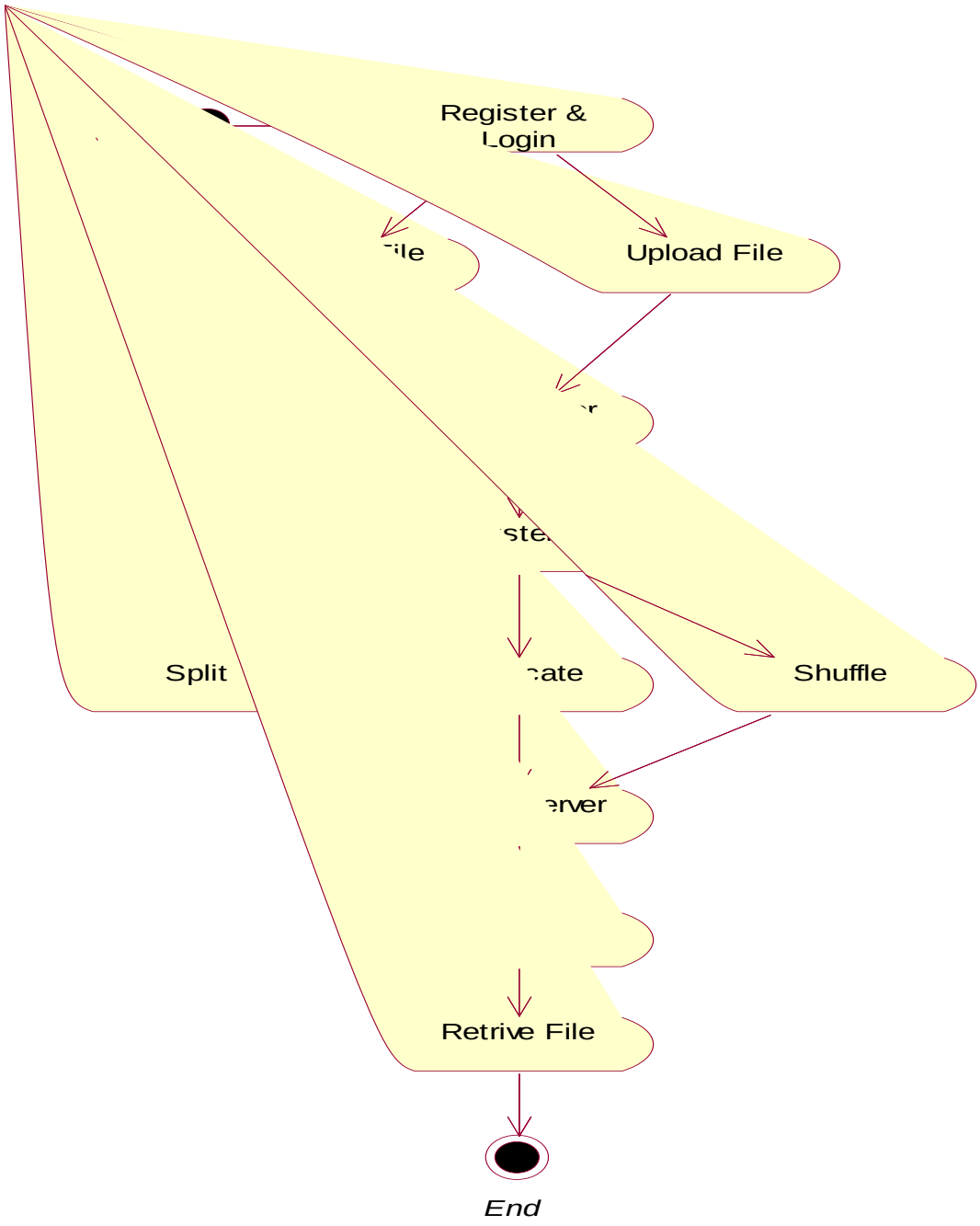

Fig 2. Activity Diagram

ii. Use Case Diagram

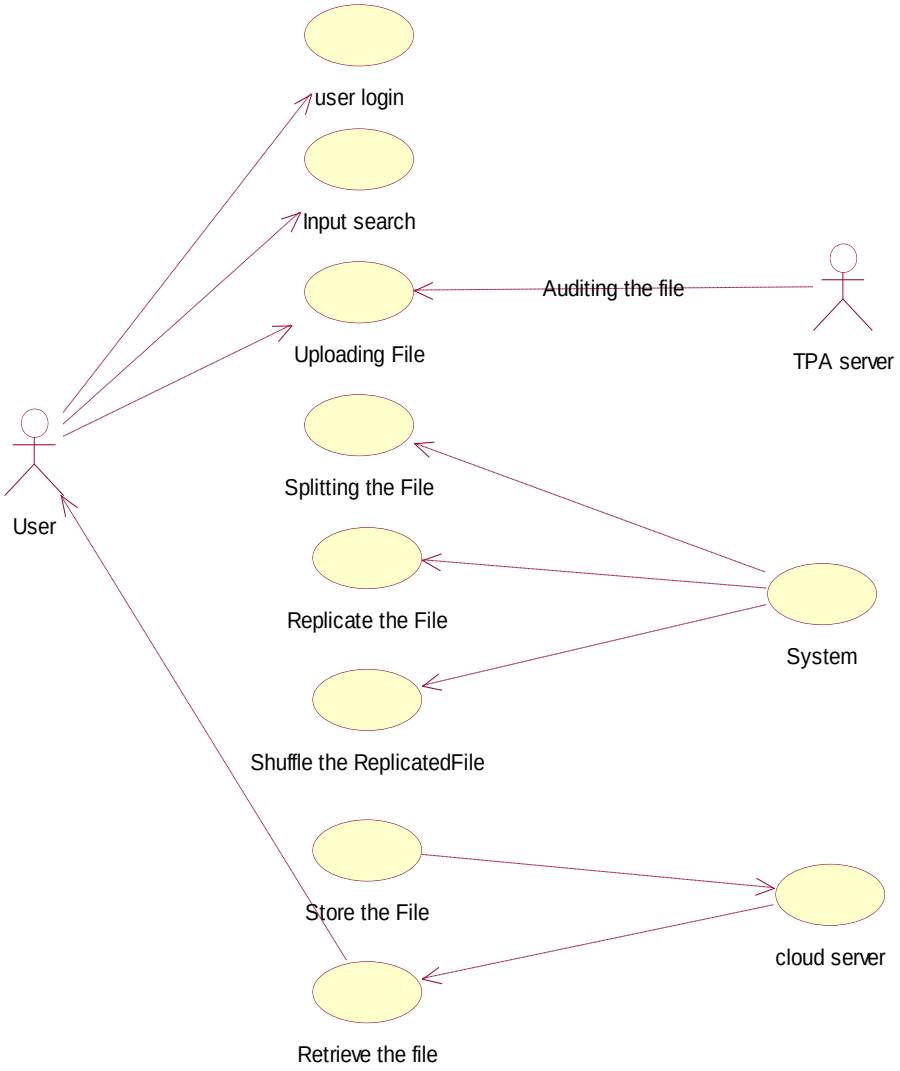

Fig 3. Activity Diagram

III. RESULT ANALYSIS

A. PERFORMANCE EVALUATION

i. Time Consumption for uploading

The below bar chart shows the analysis of existing and proposed system for time consumption to upload the files in the cloud. The X-axis denotes the number of files

uploaded and the Y-axis denotes the time taken to upload the files which is measured in seconds(s).

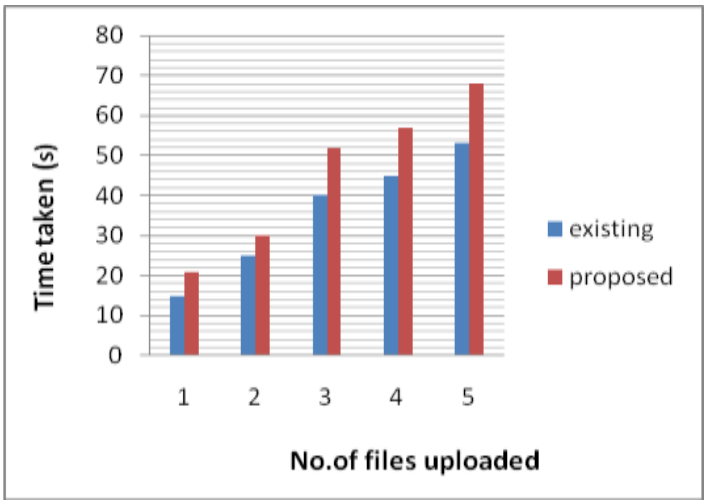

Fig3. Time Consumption for uploading

ii. Time Consumption for Auditing:

This bar chart shows the comparison between the existing and the proposed system for auditing the file by the third party auditor. The X-axis denotes the number of files denoted in MB and the Y-axis denotes the time taken which is measured in seconds(s).

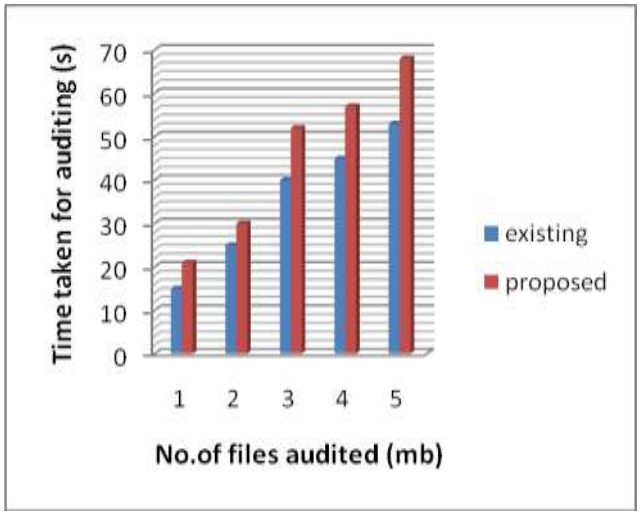

Fig4. Time Consumption for auditing

B.COMPARATIVE ANALYSIS

The below table shows the comparative analysis between the existing and the proposed system for uploading the file in the cloud table 9.1 and auditing the file in cloud table 9.2.

***Table1Comparative Analysis of time Consumption for uploading*:**

No. of files	File 1	File 2	File 3	File 4	File 5
Existing system	15	25	40	45	53
Proposed system	21	30	52	57	68

Table2Comparative Analysis for time consumption for auditing:

No. of files	File 1	File 2	File 3	File 4	File 5
Existing system	13	25	40	42	53
Proposed system	22	30	52	57	64

IV.CONCLUSION

We proposed the DROPS methodology, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by means of T coloring. The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. No node in the cloud, stored more than a single fragment of the same file. The performance of the DROPS methodology was compared with full-scale replication techniques. The results of the simulations revealed that the simultaneous focus on the security and performance resulted in increased security level of data accompanied by a slight performance drop. Currently with the DROPS methodology, a user has to download the file, update the contents, and upload it again. It is strategic to develop an automatic update mechanism that can identify and update the required fragments only. The aforesaid future work will save the time and resources utilized in downloading, updating, and uploading the file again. Moreover, the implications of TCP in cast over the DROPS methodology need to be studied that is relevant to distributed data storage and access.

V.FUTURE WORK

This project work discusses about improved secure data storage operations with integrity verification in cloud computing. In the future, to make the system work more efficiently, the system can be accessed by multiple cloud users to update and access the files more securely.

VI.APPENDIX

User manual

1. Eclipse installation
2. Java installation
3. Enter the details required in the registration form.
4. Once you are logged in you can upload the files.
5. You can also view the file fragments and the servers in which they are stored.
6. You can download the files whenever you need.
7. To view your file on the cloud you will be provided with the key.
8. The key ensures whether the user is authentic.

ACKNOWLEGMENTS

This research was supported/partially supported by BSA crescent university, vandalur, Chennai. We thank our colleagues from Information technology department of crescent university who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.

We thank Dr.kavitha, Associate professor for assistance with particular technique, methodology, and Faculty crescent university for comments that greatly improved the manuscript.

We would also like to show our gratitude to the Yasmin ansar, mother for sharing their pearls of wisdom with us during the course of this research, and we thank 3 “anonymous” reviewers for their so-called insights. We are also immensely grateful to my friend for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCE

[1] M. Krotofil, J. Larsen, D. Gollmann, The process matters: Ensuring data veracity in cyber-physical systems, in: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS'15, Singapore, April 2015, pp. 133–144.
[2] A.A. Cardenas, S. Amin, Z.S. Lin, Y.L. Huang, C.Y. Huang, S. Sastry, Attacks against process control systems: risk assessment, detection and response in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS'11, Hong Kong, March 2011, pp. 355–366.
[3] M. Krotofil, J. Larsen, Are you threatening my hazards, in: Proceeding of 9th International Workshop on Security, IWSEC'14, Hirosaki, Japan, August 2014, pp. 17–32.
[4] US Department of Homeland Security, ICS-CERT Year in Review 2012, Washington, DC, 2012.
[5] K. William, W. Knowles, D. Prince, D. Hutchison, J.F.P. Disso, K. Jones, A survey of cyber security management in industrial control systems, Int. J. Crit. Infrastructure. Prot. 9 (2015) 52–80.
[6] A. Gabus, E. Fontela, World problems, an invitation to further thought within the framework of DEMATEL, Battelle Geneva Research Center, Geneva, Switzerland, 1972.
[7] H.H. Wu, S.Y. Chang, A case study of using DEMATEL method to identify critical factors in green supply chain management, Appl. Math. Comput. 256 (2015) 394–403.
[8] G. Büyüközkan, G. Çifçi, A novel hybrid MCDM approach based on fuzzy DEMATEL, fuzzy ANP and fuzzy TOPSIS to evaluate green suppliers, Expert Syst. Appl. 39 (2012) 3000–3011.
[9] H.K. Chen, S.P. Lin, T.D. Lin, H.H. Wu, Analysis of critical evaluation factors of the EWPS scale for boundary–spanners using DEMATEL, J. Qual. 21 (2014).
[10] J.I. Shieh, H.H. Wu, K.K. Huang, A DEMATEL method in identifying key success factors of hospital service quality, Knowl.-Based Syst. 23 (2010) 277–282.
[11] H.H. Wu, Y.N. Tsai, A DEMATEL method to evaluate the causal relations among the criteria in auto spare parts industry, Appl. Math. Comput. 218 (2011) 2334–2342.
[12] M. Krotofil, A. Cárdenas, Resilience of process control systems to cyberphysical attacks, in: Proceedings of the 18th Nordic Conference on Secure IT Systems, NordSec'13, Ilulissat, Greenland, 2013, pp. 166–182.
[13] H. Kopetz, Real-Time Systems: Design Principles for Distributed Embedded Applications, second ed., in: Real-Time Systems Series, 2011.
[14] A. Hahn, R.K. Thomas, I. Lozano, A. Cardenas, A multi-layered and kill-chain based security analysis framework for cyber-physical systems, Int. J. Crit. Infrastructure. Prot. 11 (2015) 39–50.
[15] R. Hills, Common VPN security flaws, White Paper, NTA Monitor, Rochester, United Kingdom, 2005. www.nta-monitor.com/posts/2005/01/VPN-Flaws-Whitepaper.pdf.

[16] K. Stouffer, J. Falco, K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication, 2011, pp. 800–882.
[17] M. Majdalawieh, Security Framework for DNP3 and SCADA, VDM Verlag, Saarbruken, Germany, 2008.
[18] International Electrotechnical Commission, IEC 61850 Standard, Technical Specification IEC TS 61850, Geneva, Switzerland, 2003.
[19] Modbus-IDA, Modbus Application Protocol Specification V.1.1b, Hopkinton, Massachusetts, 2006. www.modbus.org/docs/Modbus_Application_Protocol_ V1_1b.pdf.
[20] H. Li, L. Lai, H.V. Poor, Multicast routing for decentralized control of cyber physical systems with an application in smart grid, IEEE J. Sel. Areas Commun. 30 (2012) 1097–1107.
[21] M. Krotofil, A.A. Cárdenas, J. Larsen, D. Gollmann, Vulnerabilities of cyberphysical systems to stale data-determining the optimal time to launch attacks, Int. J. Crit. Infrastruct. Prot. 7 (2014) 213–232.
[22] D. Gollmann, Veracity, plausibility, and reputation, in: Proceeding of 6th IFIP WG 11.2 International Workshop Security Theory and Practice, WISTP'12, Egham, UK, 2012, pp. 20–28.
[23] Y.L. Huang, A.A. Cárdenas, S. Amin, Z.S. Lin, H.Y. Tsai, S. Sastry, Understanding the physical and economic consequences of attacks on control systems, Int. J. Crit. Infrastruct. Prot. 2 (2009) 73–83.
[24] B. Genge, C. Siaterlis, M. Hohenadel, Impact of network infrastructure parameters to the effectiveness of cyber attacks against industrial control systems, Int. J. Comput. Commun. Control 7 (2014) 674–687.
[25] G. Béla, I. Kiss, P. Haller, A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures, Int. J. Crit. Infrastruct. Prot. 10 (2015) 3–17.
[26] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A.Zomaya, "On the characterization of the structural robustnessof data center networks," IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013, pp. 64-77.
[27] B. Grobauer, T.Walloschek, and E. Stocker, "Understandingcloud computing vulnerabilities," IEEE Security and Privacy, Vol.9, No. 2, 2011, pp. 50-57.
[28] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B.Fernandez, "An analysis of security issues for cloud computing,"Journal of Internet Services and Applications, Vol. 4, No. 1,2013, pp. 1-13.
[29] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, "Dike:Virtualization-aware Access Control for Multitenant Filesystems,"University of Ioannina, Greece, Technical Report No.DCS2013-1, 2013.
[30] S. U. Khan, and I. Ahmad, "Comparison and analysis often static heuristics-based Internet data replication techniques,"Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008,pp. 113-136.
[31] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani,"Towards Secure Mobile Cloud Computing: A Survey," FutureGeneration Computer Systems, Vol. 29, No. 5, 2013, pp. 1278-1299.