VIVA Institute of Technology

VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL

VIVA-TECH INTERNATIONAL JOURNAL
FOR RESEARCH AND INNOVATION

ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

National Conference on Role of Engineers in Nation Building – 2022 (NCRENB-2022)

A new perspective on cloud computing

Himanshu Dhande[1], Divya Karwande[2], Atharv Kadam[3], Akshata Raut[4]
(Computer Engineering Department, VIVA Institute of Technology, India)

Abstract: *Cloud computing has become a widely exploited research area in academia and industry. Cloud computing benefits both cloud service providers (CSPs) and consumers. The security challenges associated with Cloud computing have been widely studied in the literature. This systematic literature review (SLR) is aimed at reviewing the existing research studies on cloud computing security, threats, and challenges. This SLR examined the research studies published between 2010 and 2020 within the popular digital libraries. We selected 80 papers after a meticulous screening of published works to answer the proposed research questions The outcome of this SLR reported seven major security threats to cloud computing services. The results showed that data tampering and leakage were among the most discussed topics in the chosen literature. Other identified security risks were associated with data intrusion and data storage in the cloud computing environment. These SLR's results also indicated that consumers' data outsourcing remains This is a challenge for both CSPs and cloud users. Our survey paper identified the blockchain as a partner. technology to alleviate security concerns. The SLR findings reveal some suggestions to be carried out in future work to bring data confidentiality, data integrity, and availability.*

Keywords - *Auditing, cloud computing, cloud models, decryption, encryption, intrusion, malicious behavior, secured communication*

I. INTRODUCTION

The Cloud Computing idea has emerged from distributed software design. Cloud computed technology is aimed to provide hosted services over the net. In recent years, cloud computing in Information Technology has given rise to various new user communities and markets. Cloud computing services are provided from information centers settled in different components of the globe. Microsoft SharePoint and Google applications are general samples of cloud computing services. Security plays a very important role within the wider acceptance of cloud computing services. Existing literature is targeted on completely different security solutions, together with technology and security policy implementation. The latter study introduced new attacks on the cloud setting from a sociology perspective. The planned answer to those recent attacks relies on criminal theories for the protection of the cloud.

The constant analysis proposes to beat the known issues regarding the protection of the cloud. A security guide, developed during this analysis, enables the cloud user organizations to bear in mind security vulnerabilities and approaches to invade them. Security vulnerabilities and challenges arise from the usage of cloud computing services. Currently, cloud computing models are at the first supply of those challenges and vulnerabilities. The intruders exploit the weakness of cloud models in accessing the users' non-public information, by offensive the processing power of pc systems. The ''Autonomous Cloud Intrusion Response System'' (ACIRS) has been recently planned to beat the matter mentioned earlier. Before this work, the ''Network Intrusion Detection and measure choice system'' (NICE) worked on the choice of the simplest countermeasures to mitigate the risks to cloud virtual networks. There is the widespread use of cloud computing (CC) in information technology. However, several service homeowners are still reluctant to completely adopt the CC as relevant security technologies aren't up to now matured. Thus, the literature shows service suppliers' desire to speculate in CC-associated device security. We've now found some studies that show the proposal of evaluation of cloud computing security. one in every one of these analysis studies introduces associate degree ‘‘attack treemap'' (ATM) to investigate security vulnerabilities and threats. The analysis highlights various sides of CC combined with the trusty computing platform to produce security services like confidentiality, authentication, and integrity.

II. LITERATURE SURVEY

Mehdi Bahrami, et. al. [1] has proposed to begin an explanation of the concepts behind cloud computing systems, cloud software architecture, the need for mobile cloud computing as an aspect of the app industry to deal with new mobile app design, network apps, app designing tools, and the motivation for migrating apps to cloud computing systems. The tutorial will review facts, goals, and common architectures of mobile cloud computing systems, as well as introduce general mobile cloud services for app developers and marketers. This tutorial will highlight some of the major challenges and costs, and the role of mobile cloud computing architecture in the field of app design, as well as how the app-design industry has an opportunity to migrate to cloud computing systems with low investment. The tutorial will review privacy and security issues. It will describe major mobile cloud vendor services to illustrate how mobile cloud vendors can improve mobile app businesses. We will consider major cloud vendors, such as Microsoft Windows Azure, Amazon AWS and Google Cloud Platform.

Jian Shen, et. al. [2] has proposed cloud computing and cloud storage have become hot topics in recent decades. Both are changing the way we live and greatly improving production efficiency in some areas. At present, due to limited storage resources and the requirement for convenient access, we prefer to store all types of data in cloud servers, which is also a good option for companies and organizations to avoid the overhead of deploying and maintaining equipment when data is stored locally.

Cui Lin, et. a1.[3] has proposed that most existing workflow scheduling algorithms only consider a computing environment in which the number of compute resources is bounded. Compute resources in such an environment usually cannot be provisioned or released on demand of the size of a workflow, and these resources are not released to the environment until execution of the workflow completes. To address the problem, we firstly maize a model of a Cloud environment and a workflow graph representation for such an environment. Then, we propose the SHEFT workflow scheduling algorithm to schedule a workflow elastically on a Cloud computing environment. Our preliminary experiments show that SHEFT not only outperforms several representative workflow scheduling algorithms in optimizing workflow execution time, but also enables resources to scale elastically at runtime.

Young-ho Song, el. al.[4] has proposed privacy-preserving association rules mining algorithms have been proposed to support data privacy. However, the algorithms have an additional overhead to insert fake items (or fake transactions) and cannot hide data frequency. In this paper, we propose a privacy-preserving association rule mining algorithm for encrypted data in cloud computing. For association rule mining, we utilize the Apriori algorithm of using the Elgamal cryptosystem, without additional fake transactions. Thus the proposed algorithm can guarantee both data privacy and query privacy while concealing data frequency. We show that the proposed algorithm achieves about 3-5 times better performance than the existing algorithm, in terms of association rule mining time.

Mehdi Bahrami, el. a1.[5] has proposed Cloud Computing technology offers new opportunities for outsourcing data, and outsourcing computation to individuals, start-up businesses, and corporations in health care. Although the cloud computing paradigm provides interesting, and cost-effective opportunities to the users, it is not mature, and using the cloud introduces new obstacles to users. For instance, a vendor lock-in issue causes a healthcare system to rely on a cloud vendor infrastructure, and it does not allow the system to easily transit from one vendor to another. Cloud data privacy is another issue and data privacy could be violated due to outsourcing data to a cloud computing system, in particular for a healthcare system that archives and processes sensitive data.

Fan Yang-Turner, el. a1.[6] has proposed Pathogen genomic data analysis can be extremely bespoke and diverse. This paper presents our plan and progress towards creating a Scalable Pathogen Pipeline Platform (SP3) providing an efficient and unified process of collecting, analyzing, and comparing genomic data analysis with the benefit of elastic cloud computing. SP3 enables container-centric bioinformatic workflows to run on personal computers, High-performance computing (HPC) clusters, and cloud platforms. We have deployed and tested SP3 on local HPC, Google Cloud Platform (GCP), Microsoft Azure, and OpenStack Platforms. SP3 allows users to fetch genomic sequencing data from European Nucleotide Archive (ENA) and conduct analysis with open-source bioinformatics pipelines. We believe SP3 will promote common standards around pathogen genomic data quality, data processing, and data analysis, helping answer the challenges of tools divergence and leveraging a pool of public genomic data repository and cloud resources.

David S. Linthicum, el. al.[7] has proposed Traditional approaches to data integration, including traditional data integration technology providers are typically no longer a fit. Even data integration technologies that I've built in the past as Chief Technology Officer (CTO) would no longer be on my shortlist of data integration technologies that I would recommend. Enterprise applications and the data landscape are undergoing dramatic change.

Rajkumar Buyya, el. al.[8] has proposed Cloud computing systems promise to offer subscription-oriented, enterprise-quality computing services to users worldwide. With the increased demand for delivering services to a large number of users, the need to offer differentiated services to users and meet their quality expectations. Existing resource management systems in data centers are yet to support Service Level Agreement (SLA)-oriented resource allocation, and thus need to be enhanced to realize cloud computing and utility computing. In addition, no work has been done to collectively incorporate customer-driven service management, computational risk management, and autonomic resource management into a market-based resource management system to target the rapidly changing enterprise requirements of Cloud computing. This paper presents the vision, challenges, and architectural elements of SLA-oriented resource management.

P. Geetha, el. al.[9] has proposed the enrichment knowledge of Cloud Computing is Green Cloud Computing. The term Cloud Computing is a globally interconnected network of Computing Resources (Servers, Networks, Applications, Hardware, software). Green Computing is an Environmental Benefits of eco-friendly usage of Computing Resources. The combination of Green Computing and Cloud computing is Green Cloud Computing. GCC performs both performance and efficiency. The combination of Mobile Computing and Cloud Computing is known as Mobile Cloud Computing. Now, Computational science is changing to be data-intensive. So, Load balancing is a technique to distribute the load across a given Green Cloud Network Vs Mobile Cloud Network. In this proposed system, the in-depth analysis of Load Balancing Algorithms. The Load of Cloud Balancing is a process of reassigning the total load to the individual nodes in a given network. Then the Comparative study of load balancing algorithms with their quality metrics is summarized.

Maithilee Joshi, el. al.[10] has proposed an Electronic Health Record (EHR) is an electronic document that details all the relevant clinical reports of a person, over a period of time. In a typical scenario, an HER records the vital stats, diagnoses, medications, history of immunizations, laboratory and radiology reports, doctor notes, etc. Maintaining electronic copies introduces the possibility of attacks on patient data and information privacy. The Health Information Technology for Economic and Clinical Health (HITECH) Act [3] promotes a meaningful use of electronic versions of patient health records. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the management and distribution of medical records by establishing standards for preserving the security and privacy of medical health data. Developing an EHR management solution that complies with all the legal and ethical standards becomes a huge research and development challenge.

Jihua Yang, el. al.[11] has proposed that cloud computing has been an important platform for various resources and sharing. But at present, many cloud computing platforms have not used the service-oriented system architecture, which could bring about more flexibility, higher extendibility, and reusability. Cloud computing has always been an important computing platform for sharing various resources including infrastructures, software, operation procedures, and application programs. The cloud computing middleware is just the key to the service-oriented step in computing. If PaaS is the core of the cloud computing system, then the middleware is the core of PaaS. The cloud computing platform is closely related to middleware technology. Therefore, the middleware is the backbone of the cloud computing platform.

Rajni Jindal, el. al.[12] has proposed that Cloud computing is an important computing paradigm for handling all types of computations, even the smaller ones in the past. But sometimes, it becomes ineffective when the task is to be done in real-time, with very low latency. Therefore, fog computing was introduced as a supplement computing paradigm for cloud computing. Internet of Things-based applications performs better with the amalgamation of it and fog computing. Due to low capacity, when fog can't compute the task on its own, heavy computations are offloaded from fog to cloud. But when to offload the task from fog to cloud is a major decision. The decision to offload the tasks from fog to cloud is very crucial, so this paper presents an idea to solve this problem.

Shahryar Shafique Qureshi, el. al.[13] has proposed cloud computing has gained momentum and is transforming the internet computing infrastructure. Also, mobile applications and mobile devices are developing rapidly. Cloud computing is anticipated to bring innovation in mobile computing, where mobile devices can use clouds for data processing, storage, and other intensive operations. Already there are some mobile cloud applications for example Google's Map, Gmail for iPhone, and Cisco's WebEx on iPad, however, these applications are using the Software as a Service model. In this paper we introduce state-of-the-art Mobile Cloud Computing and its implementation methods. We also investigate some critical issues to be solved and point out further future research directions.

Rajesh Doriya, el. al.[14] has proposed Cloud computing and service-oriented architecture (SOA) are the dominant computing paradigm. For the past few Year's Robotics applications have also started to build around these paradigms. This paper presents the entrance of robotic services in SOA and cloud computing. Where a client/user can opt for the robotic services present at the cloud-like navigation, map building, object recognition, etc. Map-reduce computing cluster is also facilitated at the cloud to process a large amount of data for the cloud robotic services. The whole system follows the Web 2.0 standard. We also reported the simulation results for service-based speech-controlled robots with a visual programming language (VPL) of Microsoft Development Robotics Studio (MDRS) and implementation of map-reduce computing cluster in robotic cloud.

Kurtzer GM, el. al.[15] has proposed Pathogen genomic data analysis can be extremely bespoke and diverse. Many institutions and labs around the world have their own infrastructure and software suites to collect, process and analyze data. However, those existing solutions are difficult to use outside of the organization and the datasets for clinically validating software are also not standardized. This has hindered the research and clinical service utilizing the whole genome sequencing technology for pathogen identification and diagnosis.

III. ANALYSIS TABLE

Sr. No	Title of paper	Techniques used	Dataset used	Accuracy
1	On Cloud Computing Middleware Architecture	Virtualization.	Words̓ Cloud computing,	90%

2	MTFCT: A task offloading approach for fog computing and cloud computing	Service-Oriented Architecture (SOA) Grid Computing.	Cloud Computing;
			Fog Computing;
				91%

3	Mobile cloud computing as future for mobile applications	Utility Computing.	Cloud computing;
			mobile cloud computing;
			mobile devices
				80%

4	Attribute Based Encryption for Secure Access to Cloud Based EHR Systems	Infrastructure as a Service (IaaS)	Mobile applications; security issues.	79.4%
5	Scheduling Scientific Workflows Elastically for Cloud Computing	Platform as a Service (PaaS)	Task Offloading	86.3%
6	A Dynamic Cloud Computing Platform for eHealth Systems	Software as a Service (SaaS)	Cloud Computing Middleware	88%
7	A Comparative-Study of Load-Cloud Balancing Algorithms in Cloud Environments	Service-Oriented Architecture	Pathogen genomic analysis	78%
8	A Comparative-Study of Load-Cloud Balancing Algorithms in Cloud Environments	Hardware Virtualization	Service Level Agreements	67%
9	SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture, and Solutions	Server Virtualization	Autonomic Management	82%
10	Cloud Computing Changes Data Integration Forever: What's Needed Right Now	Storage Virtualization	Mobile app design, Cloud Architecture	48%
11	Cloud Computing for Emerging Mobile Cloud Apps	Operating System Virtualization	Mobile Security	38%
12	Towards Multi-User Private Keyword Search for Cloud Computing	Data Virtualization	Data Sharing	89%
13	Block Design-based Key Agreement for Group Data Sharing in Cloud Computing	Grid Computing	Key agreement protocol	83%

14	Privacy-preserving Association Rule Mining Algorithm for Encrypted Data in Cloud Computing	Utility Computing	Association rule mining, Apriori	78%
15	Robotic Service in Cloud Computing Paradigm	Platform as a Service (PaaS)	Robotic Services, Cloud Robotics	85%

IV. CLOUD COMPUTING

1) Information at rest: The intrusion detection system scans from cloud data storage sources, encrypts the information, and removes it when it's found non-trusted. However, fine-tuning and configuration constraints are real issues for information at rest.

2) Information in motion: Clients' real concern lies in information security in moving information from shopper to cloud or cloud to shopper. Network watching of sensitive data via emails, and instant electronic communication, a system needs the identification and bar of log email data that attempts to leak data from a client or a corporation with the help of steganography.

3) Information in use: Data transmission from the client-side pc is monitored via the output peripherals like USB ports, printers, CDs, and auxiliary storage devices. If the applications access sensitive information, it's filtered before causation it to relevant peripherals. A plain-text message transmits data between a portable device and EC3 unit, and an information run will occur when a legal cloud computing services user stores the information at remote-based storage devices. However, information run is prevented by exploitation of the algorithms developed to spot the legal cloud storage devices. Cloud info maintains the list of legal devices and needs the authentication of portable devices before information exchanges between clouds and cloud shoppers. once verification of devices, the cloud shopper retrieves and transmits the information. once a cloud shopper desires to upload information, the EC3 unit sends asking to attach a cloud manager. Cloud shopper passes an obvious text denoted by the Pm to EC3, wherever a chip of encryption/decryption encrypts the Pm to a random positive whole number k.

V. METHODOLOGY

A. CLOUD MODELS :

1) Computer code as a service (SaaS). The SaaS model facilitates users to access the computer code and other programs in an exceeding cloud. victimization the SaaS answer eliminates the need for in-house applications, information storage, and application administration support. corporations pay to use the SaaS resources on a user basis.

2) PLATFORM AS A SERVICE (PaaS)

PaaS could be a cloud computing service that supports a full computer code life cycle and permits users to develop cloud applications and services. Programmers and developers don't want to purchase their equipment; instead, they use treater equipment and deliver the developed applications to purchasers over the net. In PaaS, a private or a corporation isn't required to shop for the computer code and hardware to develop the applications. Google App Engine, Azure services platform of Google, Amazon’s electronic information service services (RDS) square measure the key samples of the PaaS model.

3) INFRASTRUCTURE AS A SERVICE (Iaas)

IaaS is the cloud computing service delivered within this kind of platform in exceedingly virtual surroundings [10]. purchasers don't seem to be required to buy servers, information centers, network instrumentation, or areas (e.g. Amazon EC2).

4) Instrumentation as a service (CaaS) Based on instrumentation virtualization, CaaS has emerged as a cloud model to resolve application development problems in the PaaS surroundings. The CaaS cloud model has aimed to free the applications by creating them freelance of PaaS environment specifications. Amazon EC2 instrumentation Service (ECS) and Google instrumentation engine square measure samples of CaaS model. Information technology has speedy changes in recent years. Cloud computing has another less dimmed role of IT with the addition of storage for users. Cloud computing has enabled vendors to hire out their services at hourly rates. They conjointly hire out the house to users on their physical systems. However, these services have many security threats for users. During a report, Cloud Security Alliance unconcealed that abuse, insecure interfaces, and wicked usage were the vulnerable threats. These threats are related to the application program interfaces and cloud computing. Information security splits into 3 main objectives, such as integrity, confidentiality, and accessibility. Security threats to these security goals embrace a semi-permanent confidentiality issue as a result of one considering that gift and past encoding schema don't seem to be secure. Data discharge vulnerability is another concern as information is outsourced. change of state with information also poses threats to information confidentiality.

VI. FIGURES AND TABLES

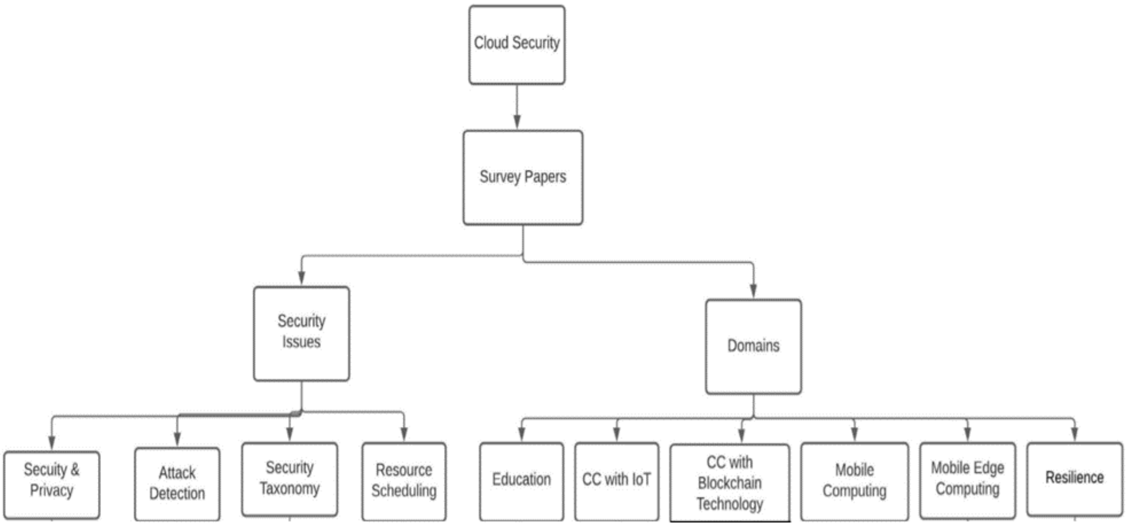

Fig 1: Taxonomy of survey literature on cloud computing topics.

Table: Studies Inclusion and exclusion criteria

Inclusion Criteria	Exclusion Criteria
Research studies that discuss cloud computing.	Studies that are published other than the English language
Research studies that discuss cloud security issues.	Papers with unidentified references
Research studies that examine the incidents of data intrusion in the larger organization.	Articles focusing on other than security topics of cloud computing
Research studies that include cloud security models.	Papers published before 2010

VII. CONCLUSION

First, during this SLR, we've reviewed the literature on cloud computing topics, together with cloud security threats and their mitigation methods. We tend to know many security risks to cloud computing. information change of state and run is one amongst the known risks. Consumers' trust, information outsourcing, and associated risks are vital challenges identified during this SLR. This SLR is known to industrial cloud services suppliers and highlights the safety problems they face throughout cloud services reading and implementation. The trustiness of cloud users is difficult for shoppers of business cloud services suppliers. information inaccessibility, light security measures, merchant lock-in, lack of ability, and standards are known additionally to the above-named problems. Moreover, we tend to know that speaker unit information generates and is used to judge the projected CC approaches. This SLR identified that researchers had seldom used Facebook and Instagram information for the analysis of projected methods. Throughout the CC readying and implementations, information security and privacy are considerations that a cloud adopting should think about before victimizing the cloud services. Blockchain technology is found as AN rising technology to alleviate the safety concerns within the CC surroundings.

VIII. ACKNOWLEDGMENTS

We would like to express a deep sense of gratitude towards our Professors of the Computer Engineering Department, their constant encouragement, and valuable suggestions. The work that we can present is possible because of her timely guidance. We would like to pay gratitude to the panel of examiners for the time, the effort they put into evaluating our work, and their valuable suggestions from time to time. We would like to thank the Head of the Computer Engineering Department. We are also grateful to the teaching and non-teaching staff of the Computer Engineering Department who lend their helping hands in providing continuous support.

REFERENCES

[1] Afgan E. et al., “The Galaxy platform for accessible, reproducible and collaborative biomedical analyses: 2016 update,” Nucleic Acids Res.,vol. 44, no. W1, pp. W3–W10, 2016.

[2] Weinstein J. N. et al. (2013) The Cancer Genome Atlas Pan-Cancer analysis project. Nat. Genet. 45, 1113–1120(2015)

[3] Merkel, D.: Docker: lightweight Linux containers for consistent development and deployment. Linux J. 2014 (239), 2 (2014)

[4] H. A. Khalid, A. Erradi, S. Abdelwahed, and F. Baiardi, ‘‘Cui Lin,’’ Computing, vol. 98, no. 11, pp. 1111–1135, Nov. 2016.

[5] C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, ‘‘NICE: Network intrusion detection and countermeasure selection in virtual network systems,’’ IEEE Trans. Dependable Secure Comput., vol. 10, no. 4, pp. 198–211, Jul. 2013.

[6] J.-Y. Park, S.-H. Na, and E.-N. Huh, ‘‘An optimal investment scheme based on ATM considering cloud security environment,’’ in Proc. 11th Int. Conf. Ubiquitous Inf. Manage. Commun., Jan. 2017, pp. 1–7.

[7] P. A. Boampong and L. A. Wahsheh, ‘‘Different facets of security in the cloud,’’ in Proc. 15th Commun. Netw. Simulation Symp., 2012, pp. 1–7.

[8] K. James, Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security, and More. Burlington, MA, USA: Jones & Bartlett, 2012.

[9] Wong, Wai Kit, et al. "Security in outsourcing of association rule mining." Proceedings of the 33rd international conference on Very large data bases. VLDB Endowment, 2007.

[10] Giannotti, Fosca, et al. "Privacy-preserving mining of association rules from outsourced transaction databases." IEEE Systems Journal 7.3 (2013): 385-395.

[11] Yi, Xun, et al. "Privacy-preserving association rule mining in cloud computing." Proceedings of the 10th ACM symposium on information, computer and communications security. ACM,2015.

[12] Agrawal, Rakesh, and Ramakrishnan Srikant. "Fast algorithms formining association rules." Proc. 20th int. conf. very large data bases,VLDB. Vol. 1215. 1994.

[13] Kim, Hyeong-Jin, Hyeong-Il Kim, and Jae-Woo Chang. "A Privacy-Preserving kN Classification Algorithm Using Yao' Garbled Circuit on Cloud Computing." Cloud Computing (CLOUD), 2017 IEEE 10th International Conference on. IEEE, 2017.

[14] Jakobson, Markus, and Ari Juels. "Mix and match: Secure function evaluation via ciphertexts." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2000.

[15] Brijs, Tom. "Retail market basket data set." Workshop on Frequent Itemset Mining Implementations (FIMI'03). 2003.