Journal of Computer Engineering & Information Technology

Research Article A SCITECHNOL JOURNAL

Leveraging Information Flow Tracking for Enhanced Security in Cloud Computing

Mohammed Almutairi* **and Frederick Sheldon**

Department of Computer Engineering and Information Technology, Loma Linda University School of Medicine, California, USA

***Corresponding author:** Mohammed Almutairi, Department of Computer Engineering and Information Technology, Loma Linda University School of Medicine, California, USA; E-mail: almu9701@vandals.uidaho.edu

Received date: 30 August, 2024, Manuscript No. JCEIT-24-146856;

Editor assigned date: 02 September, 2024, PreQC No. JCEIT-24-146856 (PQ);

Reviewed date: 17 September, 2024, QC No. JCEIT-24-146856;

Revised date: 10 June, 2025, Manuscript No. JCEIT-24-146856 (R); **Published date:** 17 June, 2025, DOI:10.4172/2324-9307.1000330.

Abstract

Cloud computing has transformed modern computing by providing unique flexibility and scalability to businesses and individuals. However, it also introduces significant security challenges. This mini review paper explores Information Flow Tracking (IFT) and its role in enhancing cloud computing security. By focusing on the flow of information within cloud environments, IFT offers a data-centric approach to security enforcement. This paper reviews various IFT approaches and their applications in cloud security, highlighting their benefits and challenges. Future research directions are also discussed, emphasizing the need for refined IFT mechanisms and seamless integration into cloud environments to address evolving security threats.

Keywords: Cloud Computing; Information Flow Tracking (IFT); Cloud security; Data privacy

Introduction

Cloud computing has transformed the landscape of modern computing, offering unparalleled flexibility and scalability to businesses and individuals. However, alongside its benefits, cloud computing introduces significant security challenges. In this mini-review paper, we delve into the Information Flow Tracking (IFT) concept and its role in strengthening the security posture of cloud computing environments. This article provides a distillation of an earlier published, and much longer version through a filter meant to highlight the outcomes, assertions as well as add on insights that have been (re-)born. More of the details from that work can be found here [1].

According to the National Institute of Standards and Technology (NIST), cloud computing is defined as a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. It encompasses key characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. Cloud computing provides a dynamic and scalable platform for delivering computing services by leveraging technologies like virtualization.

Materials and Methods

Cloud deployment models and security concerns

Various deployment models characterize cloud computing, including private, public, community, and hybrid clouds. Each deployment model brings its own set of security considerations, ranging from data privacy and access control to regulatory compliance and data residency requirements. Security concerns in cloud computing encompass trust issues between consumers and providers, data storage vulnerabilities, and access management challenges.

Information Flow Tracking (IFT) in cloud security

IFT represents a paradigm shift in security enforcement that offers a data-centric approach to tracking and controlling data propagation within cloud environments. In contrast to traditional access control models such as Mandatory Access Control (MAC) and Discretionary Access Control (DAC), which focus on resource-centric security policies, IFT focuses on the flow of information through the system. Centralized and Dynamic IFT systems enable fine-grained control over data flow. That allows administrators to define security policies that govern data propagation based on its security attributes.

IFT mechanisms and models in cloud security

Several IFT approaches enforce cloud security in the literature. However, none of them have taken into consideration the consumer's perspective and the importance of IFT as a security challenges solution of cloud computing [1]. For instance, Yuan, et al. have introduced a fine-grained IFT framework capable of identifying malware within cloud environments [2].

As seen in Figure 1, the fine-grained IFT system offers taint tracking mechanisms tailored to the security requirements of Cloud applications. This includes a configuration file based on:

- Script,
- Source triggering mechanisms, and
- A customizable security detection method [3-5].

Bacon, et al. have reviewed some IFT mechanisms and identified the challenges needed to apply IFT to a cloud environment [1]. In their work, the researchers recommended that IFT be used for different aspects that would provide better Cloud security including

- Policy specification,
- Translation and enforcement,
- Auditing, and
- For digital forensics.

In their research, Chess and West utilized dynamic taint propagation to identify vulnerabilities without attacking the target systems in the process [6].

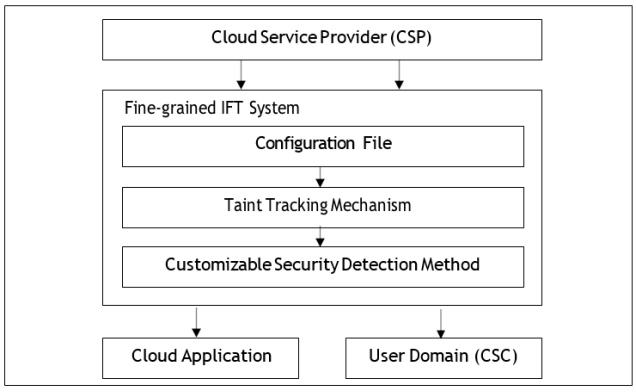

Figure 1: Cloud taint-fine-grained IFT System for cloud applications, featuring customizable taint tracking mechanisms.

Similarly, Marcel, et al. have employed IFT for privacy assessments in IoT applications [7]. This approach enables security auditors to model the flow of critical data in IoT systems and automatically verify compliance with given privacy constraints. Fu has studied the scalability of IFT for distributed systems. Fu presented "DisTtaint," a DIFT system designed to safeguard privacy and detect potential leaks of sensitive data. Similarly, other researchers have introduced, Pileus, a system aimed at preventing unauthorized or malicious attempts by users to access resources belonging to others [8]. Their approach applies a Dynamic IFT model that blocks adversaries from executing vulnerability scans, typically the initial step in attempting unauthorized access to another user's data. Papagiannis and Pietzuch introduced CloudFilter, as depicted in Figure 2, which serves as a mechanism ensuring enterprises save control over their sensitive data while enabling employee access and utilization of Enterprise Cloud Services [9].

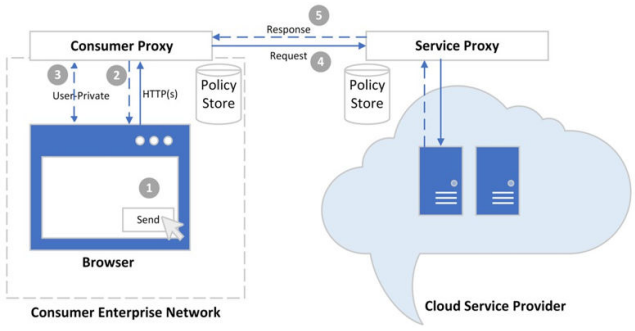

Figure 2: Cloud filter-dynamic IFT model defending against vulnerability.

Results and Discussion

Wang, et al. proposed a distributed system for IFT that can test a large number of applications that would have required a long time with "normal" similar systems CloudFence, a model proposed by Vandebogart [9], is depicted in Figure 2. The researchers have proposed Data Flow Tracking (DFT) as a service model that supports both consumers and providers in auditing security parameters pertaining to data residing in the Cloud [10].

In addition, CloudFence is maintained by the Cloud provider and the consumer would access this just as any other service. This concept overcomes the possible distrust that may exist and requires that the consumer be responsible and thus cognizant to protect their own data in the Cloud, from an auditing standpoint (*i.e.,* non-preventive). There are other instances where IFT systems are implemented in cutting-edge technologies for security purposes including SDN [11], and IoT networks (Figure 3) [12-14].

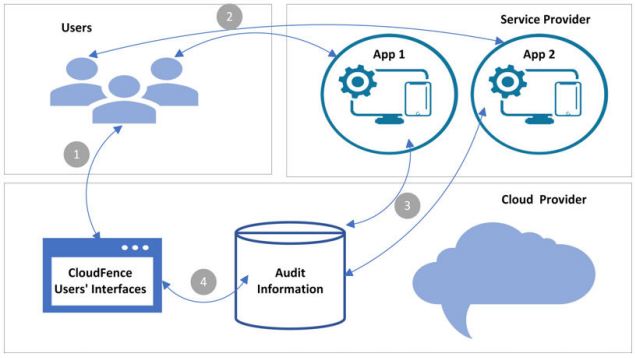

Figure 3: Cloud fence-illustrating the dynamics of advanced cloud security solutions.

Accessing data in the cloud needs to flow in ways that provide secure and resilient access protocols. Some researchers have made contributions toward achieving secure access in the cloud. However, only a few have utilized Information Flow Tracking (IFT) in their studies. Flow introduced a continuous security mechanism for Cloud Service Providers (CSP) using IFT [1]. The technique enforces fine-grained security policies at the application level. The system is tested *via* a framework designed for deploying IFT-aware web applications in the cloud. John investigated the IFT system to reduce the load of understanding the details of data protection for both sides tenants and providers of PaaS [15]. The investigation proposes that DIFT is appropriate for the data protection integrity and confidentiality in the applications of PaaS.

Bowers's research focused on safeguarding cloud data based on its geographical location [16]. Cloud consumers are particularly concerned about the jurisdiction governing their data in the cloud. Similarly, Awani, et al. investigated the use of IFT to oversee data exchanges between various components or applications within the cloud [17]. This research specifically emphasizes labeling or tagging data owned by different users to ensure traffic isolation [18].

Leuprecht thoroughly discussed protecting data shared among different applications using IFT [5]. The researchers argue that IFT-enabled cloud services ensure policy enforcement as data moves across applications, eliminating the need for special sharing mechanisms. Sun investigated a cloud service architecture designed to isolate user activities in the cloud is proposed [8]. The architecture utilizes DIFT ("distributed") to enhance cloud security by preventing malicious users from gaining unauthorized access to cloud applications. Moreover, DIFT limits an individual user's operations or access to particularly dangerous Cloud services that can pose a threat to the consumer's confidentiality, integrity, and intellectual property. DIFT is about how IFT can be employed to control users and limit how Cloud services can be accessed on distributed systems like the Cloud. In other words, DIFT assures the deployment of IFT in distributed systems.

Shyamasundar, et al., have utilized IFT to build secure and privacy-aware hybrid cloud services [19]. The researchers have proven their proposed system is forensic-ready by design. In their demonstrated

case, the IFT provides the minimum necessary forensic information from hybrid services. Another system that uses IFT for securing the environment of the cloud is Secure-ComFlow [20]. Therefore, the model specifically targets the migration of data from local company infrastructures (*i.e.,* consumers) to the cloud. It is user-oriented, providing users with the ability to define IFT policies for their data.

Alqahtani, et al., proposed a framework called Cloud Monitor that was developed to improve IFT efficiency that gives cloud service consumers better control over their data. It uses both centralized and dynamic approaches to prevent data misuse like exfiltration. Experiments showed that the framework maintains performance efficiency even with increasing data volumes, balancing security with resource use. Cloud Monitor and Cloud fence [9] are similar, however, the difference is that the Cloud Fence DFT model does not allow consumers to have rights regarding how the model audits the data (*i.e.,* the audit functions are hard-coded, nonmutable). On the other hand, in the Cloud Monitor, the local on-site user actions are taken into consideration. In the end, the consumers can trust all data that is coming from the CSP to their local site. This implies that consumers will possess the tools to safeguard their data both in cloud storage and on their own premises [21].

Current trends and future directions

Recent trends and future research directions in Information Flow Tracking (IFT) for cloud security include enhancing IFT with artificial intelligence and machine learning for improved threat detection and response, optimizing IFT systems to handle large-scale, distributed cloud infrastructures efficiently, implementing IFT methods that protect user privacy and comply with regulatory standards, and adapting IFT to new technologies like IoT, SDN, and 5G to address unique security challenges. By focusing on these areas, future research can enhance cloud security through more robust and effective IFT solutions.

Conclusion

Information flow tracking presents a promising avenue for bolstering security in cloud computing. By adopting a data-centric approach to security enforcement, IFT enables administrators to exert fine-grained control over data flows and propagation, mitigating security risks and enhancing data privacy. Future research should focus on integrating AI and ML, optimizing scalability, developing user-centric models, ensuring cross-platform compatibility, implementing privacy-preserving techniques, integrating with emerging technologies, and creating forensic-ready services. These advancements will help address evolving security challenges and enhance the overall security of cloud computing environments.

References

1. Bacon J (2014) Information Flow Tracking for secure Cloud computing. IEEE Trans Netw Serv Manag 11: 76-89.
2. Yuan J (2014) Cloud Taint: an elastic taint tracking framework for malware detection in the cloud. J Supercomput 70: 1433-1450.
3. Bohn RB (2011) NIST Cloud computing reference architecture. IEEE.
4. Brunette G, Mogull R (2009) Security guidance for critical areas of focus in Cloud computing v2. 1. Cloud Security Alliance. 1-76.
5. Leuprecht C, DB Skillicorn, VE Tait (2016) Beyond the Castle Model of cyber-risk and cyber-security. Gov Inf Q 33: 250-257.
6. Chess B, West J (2008) Dynamic taint propagation: Finding vulnerabilities without attacking. Inf Secur Tech Rep 13: 33-39.
7. Niu B, Tan G (2013) Efficient user-space information flow control. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. 131-142.
8. Sun Y, Petracca G, Ge X, Jaeger T (2016) Pileus: Protecting user resources from vulnerable cloud services. In Proceedings of the 32nd Annual Conference on Computer Security Applications. 52-64.
9. Vandebogart S (2007) Labels and event processes in the Asbestos operating system. ACM Trans Comput Syst 25: 11-es.
10. Wang H (2019) A high-level information flow tracking method for detecting information leakage. Integra 69: 393-399.
11. Alpernas K, Flanagan C, Fouladi S, Ryzhyk L, Sagiv M, et al. (2018) Secure serverless computing using dynamic information flow control. Proceedings of the ACM on Programming Languages, 2(OOPSLA), 1-26.
12. Khurshid A (2019) Secure-CamFlow: A device-oriented security model to assist Information Flow Tracking systems in Cloud environments for IoTs. Concurr Comput Pract Exp 31: 4729.
13. Gollamudi A, Chong S, Arden O. Information Flow Tracking for distributed trusted execution environments. 2019 IEEE 32nd Computer Security Foundations Symposium (CSF). IEEE.
14. Chou SC (2005) An agent-based inter-application Information Flow Tracking model. J Syst Softw 75: 179-187.
15. John NP, Bindu V (2021) An Optimal Sanitization Algorithm Based Secure Migration of Virtual Machines in Cloud Datacenters. Indian J Comput Sci Eng 12: 1-10.
16. Bowers KD, Juels A, Oprea A (2009) HAIL: A high-availability and integrity layer for cloud storage. In Proceedings of the 16th ACM conference on Computer and communications security. 187-198.
17. Joshi A, Purohit P, Jain R (2015) A Simplified Rule Based Distributed Information Flow Control for Cloud Computing. Int J Comput Sci Inf Technol 6: 1408-1414.
18. Pasquier TFM, Powles JE (2015) Expressing and enforcing location requirements in the cloud using information flow control. In 2015 IEEE International Conference on Cloud Engineering. IEEE 410-415.
19. Shyamasundar RK, Kumar NN, Rajarajan M (2016) Information-flow control for building security and privacy preserving hybrid clouds. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on Smart City; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS). IEEE 1410-1417. IEEE.
20. Wang R (2017) Research on data security technology based on cloud storage. Procedia Eng 174: 1340-1355.
21. Alqahtani F, Almutairi M, Sheldon FT (2024) Cloud security using fine-grained efficient information flow tracking. Future Internet. 16: 110.