Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 11426 – 11434

Research Article

Third Party Audit Integrated Cloud MicroServices Approach for Security and Integrity for Assorted Real Time Applications

Kalluri Rama Krishna[a] and Dr. C.V.Guru Rao[b]

[a]Assistant Professor, Vasavi College Of Engineering, Hyderabad India , kallurirk@hotmail.com
[b]Professor & Dean ,School of computer science & Artificial intelligence ,S.R.University, Warangal, India.

ABSTRACT

Data in the form of files, documents, emails, pictures, videos, etc. is moved from point A to point B. It is also retained for potential retrieval and delivery via a network (typically the Internet). The user is worried about the security of their data since the data may be attacked and corrupted by someone on the outside. Data integrity is important in the business world, therefore a new idea called data auditing has been created which will have a third party auditor that is capable of ensuring the integrity of the data (TPA). This research effort aims to design a robust auditing system that is able to efficiently implement protection for privacy, make public audits possible, maintain data integrity, and protect the confidentiality of the records. To accommodate the various needs, the auditing system was developed. The three elements are the data owner, the TPA, and the cloud server. The data owner uses an assortment of tools including dividing their file into smaller chunks, encrypting the pieces, creating hash values, reassembling the pieces, and creating a digital signature. The TPA is the one that carries out the primary task of data integrity check. It can do tasks like taking hash values from the blocks in encrypted messages sent from the cloud server, joining them, and signing the string of information. On addition, it does a comparison between the signatures to find out whether the data is changed in the cloud. Data integrity is confirmed on demand by the consumers. The encrypted data blocks are the sole thing the cloud server is utilised for. The network is constantly encountering attacks, and many methods have been created to ensure safe and consistent transmission of data packets. A better and dependable architecture is needed to transfer information across a network effectively. A breach or interception is a kind of attack that intentionally tries to do damage to a system and attempts to make it inoperable or to obtain unauthorised information. To get a full picture of what's happening on their networks, professionals may wish to have Intercept Detection Systems collect information about both successful and failed efforts. The development of intercept detection systems must be done with extreme caution, since there is a very real risk of natural and deliberate interference. This research examines the role of third party forensic database upkeep and analysis. To further investigate all the surveillance efforts with the third party audit scheme in cloud environment, it is essential to save all of the data collected in order to immediately discover how it was found. The study explores new techniques to analyse data stored in third party audit integrated forensic databases in order to help identify the many methods used to monitor citizens and to increase the efficiency of current systems.

Keywords – Intercept Detection, Intrusion Detection, Cloud Security, Trust Architecture, E-Transactions, Interception Analysis and Forensics, Forensic Database

INTRODUCTION

Cloud Computing allows businesses to use on-demand, universally available computing resources, with little administrative work. Organizations still aren't moving forward with cloud adoption, even though their hesitance is based on security, dependability, and privacy concerns. With all these challenges, cloud clients have trouble understanding their costs and payouts. Cloud Service Certification (CSC) provides peace of mind and a feeling of safety since it builds confidence and provides a degree of security and compliance. Still, when it comes to being dynamic, multi-year certifications are making certain things uncertain. In order to have complete confidence in the cloud, audits and regular monitoring of all procedures are needed. Nonetheless, earlier research has focused primarily on continuous audit, which has been mostly used for internal purposes. This way, we are opening up third-party auditors to assess cloud services on a continual basis, which keeps things open and provides a measure of security[1].

The next step in the Internet's development is cloud computing, which is the method of delivering computing power, infrastructure, applications, and business processes as a service to companies and individuals. Businesses that rely on cloud service providers (CSP) and their service level agreements (SLA) often utilise them as contracts to describe their anticipated service and the terms of the SLA, which outlines the terms and details of the service, including its availability, performance, and security. In light of recent studies, experts have come to favour using third party auditors (TPAs) to oversee CSPs. This article demonstrates how CSP may fool SLAs and out-compete its competitors, all while avoiding being detected by TPAs[2].

The rapid progression of the cloud has caused new security problems to emerge daily. The exponential increase of data stored in the cloud has prompted businesses to examine how their data can be safeguarded against thieves and attackers as a result. How can you keep your cloud safe? When it comes to service security, you must do an audit by an outside source to check it like any other technology or IT activity. Who's going to audit your cloud? A trained auditor who comprehends cloud computing and technology, as opposed to an ordinary auditor.

Business and defence applications have a need for safe and uniform network architectures to ensure that information packets may be sent without danger in an increasingly globalised world. Building relationships and maintaining trust is essential to an organization's relationships with its customers, suppliers, and workers. Internet communications are becoming faster and faster. It is essential to make network communication's information transmission both quick and efficient by developing protocols that are ideal for both scenarios[3].

A certain amount of implementations must be used to provide both security and privacy in Wireless Sensor Networks. Trust, as described by the ITU-T X.509, Section 3.3.54, is "generally characterised as when an entity assumes that another entity will behave precisely as the first entity anticipates."

In short, a person's trust is the guarantee that something will happen according to what he or she has agreed to. Identification, authentication, accountability, authorization, and availability assist building confidence by having a trust mechanism in place.

Developing the confidence among various parties is helped by offering them a set of guidelines that will lead to enhanced security in the model.

Key Segments in Cloud Audit

When choosing who should perform your cloud audit, you need to focus on finding a cloud expert. Because cloud technology is new and evolving, the industry lacks best practices that are known and understood. That’s why you want an auditing firm that does a thorough job and has auditors that understand the underlying technology. Consider the following questions when determining who should perform your cloud audit:

- Understand the characteristics of cloud computing
- Understand the three service models
- Understand deployment models
- Explain the shared responsibility model to you
- Keep up with the evolution of the cloud
- Understand your compliance obligations
- Determine which information security framework fits your needs
- Specialize in information security and cybersecurity

At KirkpatrickPrice, we hire technologists, then make them auditors – and this increases the value and quality of our cloud audits. Any auditor from KirkpatrickPrice who’s performing a cloud audit understands cloud computing and technology, and proves it through certifications like Certificate of Cloud Security Knowledge (CCSK) or Certified Cloud Security Professional (CCSP). Contact us today to begin working with a cloud expert.

According to McAfee, cyber crime losses reached $1 trillion in 2008, and if nothing is done to combat this issue, the figure would only increase as the economy worsens. Network Intercept creates methods for private citizens and companies who are attempting to discover and escape harmful behaviour online, thereby boosting productivity and privacy in the process[4].

Tracking and Defeating Detection Systems And Associated Threats

To monitor network activity and catch cyber attacks, intrusion-detection systems (IDSs) use tools, techniques, and resources to flag suspicious network behaviour. The name IDS contains a misleading use of terminology since IDSs do not really detect intrusion. Instead, they detect traffic activity, which may or might not constitute an incursion. The installation of intrusion detection in systems or devices is just a component of an overall protection system and is not a self-contained security solution.

IPSs and IDSs are only two of many ways to keep your network secure. In information protection, it is vital to employ layered protection (or "defence in depth") based on risk assessments since a network's

security is only as strong as its weakest link. Thus, networks should have many levels of security built into them with each layer performing different functions to help compliment the overall security strategy of the business.

For small- and large-scale operations, many advantages come from having interception detection and prevention systems: They can conduct threat discovery in a faster, more in-depth manner than using simple methods like regular manual scans. Their well trained staff and huge knowledge bases can assist cope with enormous quantities of data and provide alerts and warnings that help prevent further losses[5].

The actions such disconnecting or deactivating an account or executing scripts to prevent further damage built-in reporting capabilities One example of a frequent danger is something like this: an effort to hack into a system. The introduction of viruses, deletion of data, denial of service attacks, or malicious programming. There are a number of reasons why one would want to use these technologies; nevertheless, there are three factors that make the case for their implementation stronger than any of the others and problems with the law and regulations Intrusion detection and prevention tools have been implemented in the U.S. for the purpose of securing the national infrastructure. In 1998, Presidential Decision Directive 63 (PDD 63) outlined specific methods to raise awareness about this issue and was aimed at raising awareness in the IT security community. British Standard 7799 was released in February 1995 and outlines a detailed series of controls for information security “best practises.” Regulations such as HIPAA and GLBA mandate the use of audit measures to record and investigate any questionable access to data. It depends on your organization's situation as to whether or not the previous rules are required. Further, having an IDS/IPS programme is not necessary to fulfil these criteria, although it may assist in doing so.

With the determining the quantity of assaults Attacks may be calculated by IDS and IPS, and this gives system administrators a chance to understand and provide information to management. Both IDSs and IPSs can establish a profile of the assaults on a network and track various attack types. Security solutions that are frequently difficult to sell in the workplace may become more acceptable when better economic cases are presented for them. If there is the need for litigation, IPSs and IDSs can offer proof against malicious attackers[6].

The creation of a single, comprehensive, and layered defensive IDSs and IPSs have become a key component of a solid defense-in-depth security programme, and their deployment demonstrates the company's good faith since the usage of IDSs and IPSs by the organisation demonstrates its focus on security before, during, and after an incursion. The two systems may aid in identifying and neutralising security flaws in application and network layers, and assist in correlation and validation of information from other devices including antivirus programmes, firewalls, and routers. There are a few key benefits of intercept detection, including Capable of detecting both external and internal assaults on the network[7].

Intrusion-Prevention System (IPS)

In contrast to IDS, IPS applies its logic prior to execution of the action in memory. IPS systems also use file checksums to ensure each file is legitimate, as well as stopping it from running unless its file size is within acceptable margins. IPS systems include a few key pieces: the traffic normalizer, service scanner, detection engine, and traffic shaper[8].

The traffic normalizer will both read the network traffic and complete fundamental blocking tasks, including reassembling packets and interpreting their contents. The service scanner and detection engine process the data from the service scanner and traffic capture. The service scanner creates a reference table which categorises information and enables the traffic manager to control information flow. The detection engine searches the reference database for a pattern match, and the correct answer is assigned[9].

PROPOSED SECURITY TRUST ARCHITECTURE

The proposed architecture consists of various phases which will include algorithms for encryption and decryption of data packet alongwith the technique to analyze the overall interception patterns[10].

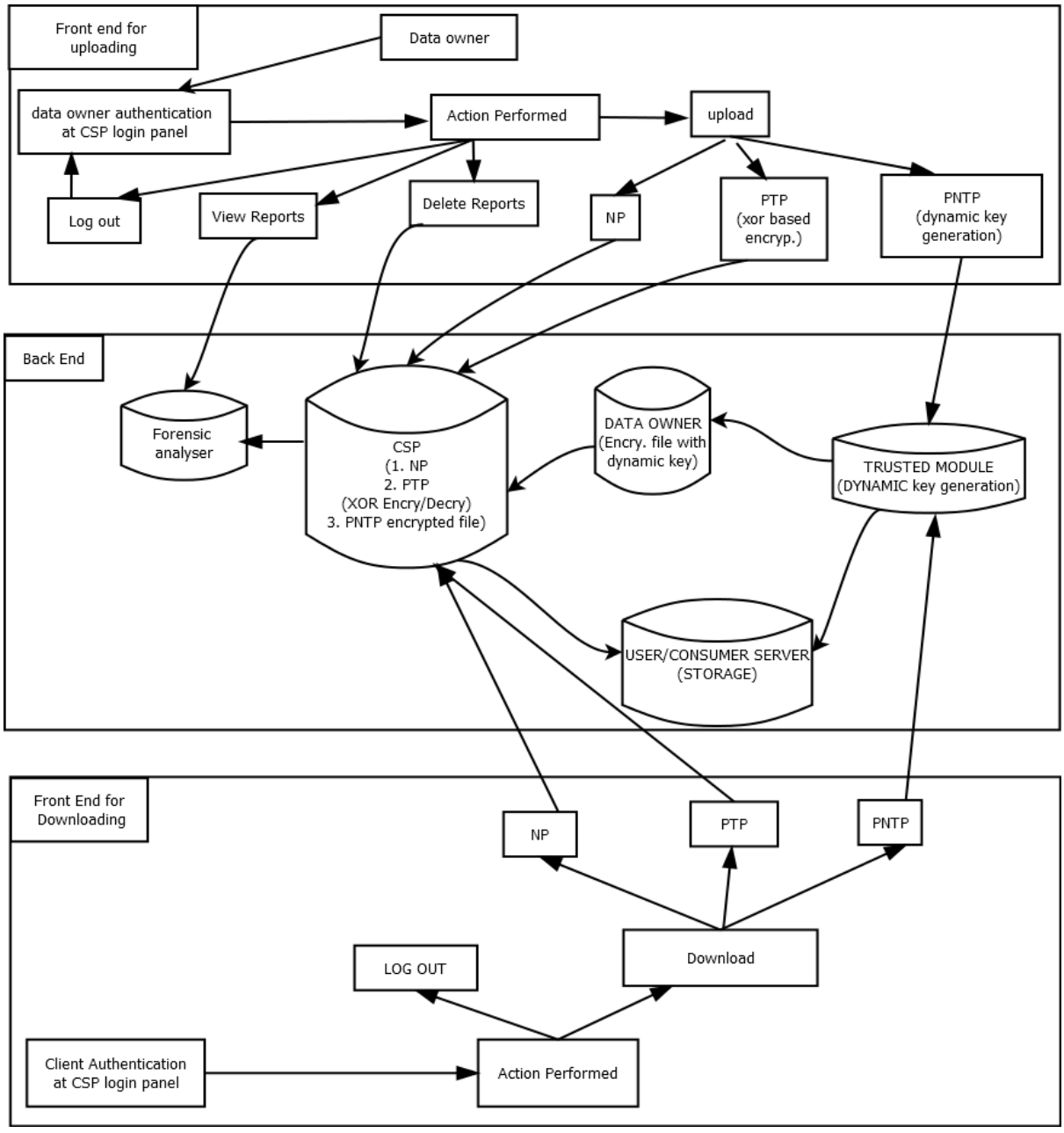

Figure 1 : The Proposed Cloud Audit Scheme with Trust Architecture for Intercept Management

In cloud computing the Security issues deals with all the challenges associated with securing an organization's core IT infrastructure at the network, host, and application levels as well as the vulnerabilities and attacks related to the data security including: Data-in-transit, Data-at-rest, Processing of data including multitenancy, Data lineage, Data provenance. To cover all these security issues possible within the cloud, and in-depth, would be herculean task. Existing efforts look to provide a taxonomy over the issues seen. The Cloud Security Alliance is a non-profit organisation that seeks to promote the best practises for providing security assurance within the cloud computing landscape[11]. In Hubbard, Sutton et al. the Cloud Security Alliance identify seven threats to cloud computing that can be interpreted as a classification of security issues found within the cloud. They are:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service and Traffic Hijacking
- Unknown Risk Profile

The proposed architecture consists of various phases which will include algorithms for encryption and decryption of data packet alongwith the technique to analyze the overall interception patterns[12].

STRUCTURE OF FORENSIC DATABASE

In the proposed architecture, MySQL will be used as forensic database with following fields.

Interception Attempts

ID	*Source IP*	*Destination IP*	*Timestamp*	*Bytes Altered*

ID – Unique Auto-Increment Identification
Source IP – IP Address of Source System from where the packet was transmitted
Destination IP – IP Address of Destination System where the packet was supposed to reach
Timestamp – Time at which the record is inserted in the table
Bytes Altered – Number of bytes altered by the interception attempt

This table will be associated with another table with following fields

Interception Type

ID	*Bytes Altered*	*Occurrences*	*Interception Type*

ID – Foreign Key to Table Interception Attempt
Bytes Altered – Data imported from Table Interception Attempt
Occurrences – The number of similar attempts
Interception Type – Association of a Type to the Interception occurred

Comparison Table of Classical and Proposed Approach in terms of Security

Attempt	Existing	Proposed
1	11	37
2	12	32
3	13	32
4	12	38
5	14	33
6	15	39
7	17	38
8	18	33
9	10	33
10	11	40
11	15	39
12	14	31

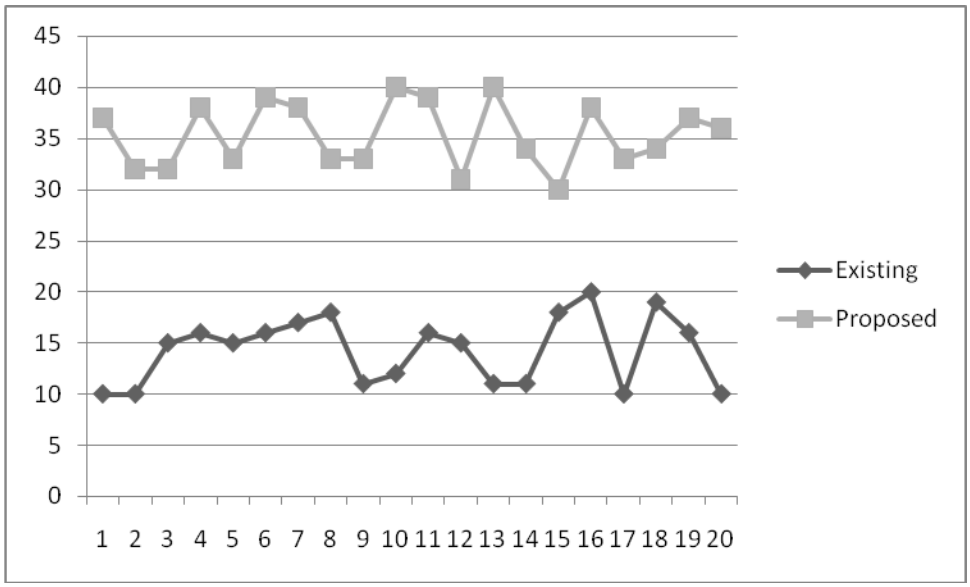

Figure 2 : Third Party Audit Integrated Performance Analytics Patterns

ALGORITHMIC APPROACH FOR THIRD PARTY AUDIT SCHEME

Step 1:

Create Database Connection

Step 2:

Analyze the Field Bytes Altered in the relation Interception Attempt

Step 3:

Associate a Unique Interception Type to the ID and insert a record in the Table Interception Type

Step 4:

if another same record of same Bytes Altered is encountered

Increment Occurrences

Keep other fields same

Step 5:
Full Outer Join Operation on both tables
Generate Detailed Report of the Interception Type and Number of Occurrences

CONCLUSION

To understand cloud security, it's important to know that cloud computing systems hold data that may be vulnerable to many types of loss. Using firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPNs), and avoiding public internet connections are all strategies for ensuring cloud security. Cybersecurity is of many types, including cloud security. Through the Internet, cloud computing delivers many services. Among other things, the listed resources include software, servers, databases, and networking. Cloud storage provides a remote database in which you may store files instead of using a proprietary hard drive or local storage device. Any electronic gadget with online connection will have access to the data and applications required to operate it. A variety of advantages accompany the use of cloud computing in which, notably, include saving money, improving efficiency, and providing better performance and security. For the many individuals worried about the protection of their data stored in the cloud, cloud security is a need. Their data is better protected on their own servers, since they think that they can maintain greater control over the data that way. Cloud service companies have better security and employ specialists in that field, making their data much more safe. Data stored on-premise may be more susceptible to attack and, as a result, is more at risk of being breached. On-site data may be more susceptible since its guards are less skilled in identifying security risks. You must choose a cloud provider that can ensure your data is safe from insider attacks via extensive background checks and security clearances. Employees are often considered less dangerous in comparison to outside hackers, yet their behaviour may pose just as great a threat to cloud security. Workers may make errors when using their personal smartphones to access critical business data since they are not utilising the firm's network. The employees may not even be aware that they are putting the company at risk.

REFERENCES

[1] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent Issued on August 18, 1998
[2] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia
[3] Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security Practice, Sun BluePrints™ OnLine - December 2002, Trust Modeling for Security Architecture Development
[4] Security, Encryption, Acceleration, http://www.networkintercept.com
[5] Youlu Zheng, Shakil Akhtar, Networks for Computer Scientists and Engineers, Oxford University Press, 2009
[6] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004
[7] Kandukuri, B. R., & Rakshit, A. (2009, September). Cloud security issues. In 2009 IEEE International Conference on Services Computing (pp. 517-520). IEEE.
[8] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.

[9] Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.".

[10] Nassif, A. B., Talib, M. A., Nassir, Q., Albadani, H., & Albab, F. D. (2021). Machine Learning for Cloud Security: A Systematic Review. IEEE Access.

[11] Mondal, A., & Goswami, R. T. (2021). Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security. Microprocessors and Microsystems, 81, 103719.

[12] Springer, N., & Feng, W. C. (2021). Thunder CTF: Learning Cloud Security on a Dime. arXiv preprint arXiv:2107.12566.