JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 15, Issue. 2 July 2022 ISSN: 1946-1836

In this issue:

- 4. Examining Cloud Data Security Vulnerabilities During Usage Daniel Amoah, Microsoft Corporation Samuel Sambasivam, Woodbury University
- **17.** Cybersecurity Maturity Model Certification Initial Impact on the Defense Industrial Base

Hala Strohmier, University of North Carolina Wilmington Geoff Stoker, University of North Carolina Wilmington Manoj Vanajakumari, University of North Carolina Wilmington Ulku Clark, University of North Carolina Wilmington Jeff Cummings, University of North Carolina Wilmington Minoo Modaresnezhad, University of North Carolina Wilmington

- 30. The COVID-19 Pandemic's Impact on Information Technology Employment, Salaries, and Career Opportunities Patricia Sendall, Merrimack College Alan Peslak, Penn State University Wendy Ceccucci, Quinnipiac University D. Scott Hunsinger, Appalachian State University
- **39.** A Comparison of Internationalization and Localization Solutions for Web and Mobile Applications

Peng Wang, Pinterest, Inc. Hee Jung Sion Yoon, City University of Seattle Sam Chung, City University of Seattle

- **47. GIS for Democracy: Toward A Solution Against Gerrymandering** Peter Y. Wu, Robert Morris University Diane A. Igoche, Robert Morris University
- 54. Determinants of Health Professionals' Intention to Adopt Electronic Health Record Systems

Jie Du, Grand Valley State University Jenna Sturgill, Grand Valley State University



The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer reviewed academic journal published by ISCAP, Information Systems and Computing Academic Professionals. Publishing frequency is three to four issues a year. The first date of publication was December 1, 2008.

JISAR is published online (https://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (https://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is under 38%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of ISCAP who perform the editorial and review processes for JISAR.

2022 ISCAP Board of Directors

Eric Breimer Siena College President Jeff Cummings Univ of NC Wilmington Vice President

Jennifer Breese Penn State University Director

RJ Podeschi Millikin University Director

Anthony Serapiglia St. Vincent College Director/2022 Conf Chair Amy Connolly James Madison University Director

Michael Smith Georgia Institute of Technology Director/Secretary

Xihui "Paul" Zhang University of North Alabama Director/JISE Editor Jeffry Babb West Texas A&M Past President/ Curriculum Chair

Niki Kunene Eastern CT St Univ Director/Treasurer

Tom Janicki Univ of NC Wilmington Director / Meeting Facilitator

Copyright © 2022 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to Scott Hunsinger, Editor, editor@jisar.org.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

Scott Hunsinger Senior Editor Appalachian State University Thomas Janicki Publisher University of North Carolina Wilmington

Biswadip Ghosh Data Analytics Special Issue Editor Metropolitan State University of Denver

2022 JISAR Editorial Board

Jennifer Breese Penn State University

Amy Connolly James Madison University

Jeff Cummings Univ of North Carolina Wilmington

Ranida Harris Illinois State University

Edgar Hassler Appalachian State University

Vic Matta Ohio University Muhammed Miah Tennessee State University

Kevin Slonka University of Pittsburgh Greensburg

Christopher Taylor Appalachian State University

Hayden Wimmer Georgia Southern University

Jason Xiong Appalachian State University

Sion Yoon City University of Seattle

Examining Cloud Data Security Vulnerabilities During Usage

Daniel Amoah, DCS, CISSP Azure Solutions Architect daamoah@microsoft.com Solutions Architect (Infrastructure and Cyber) Microsoft Corporation Denver, CO 80249

Samuel Sambasivam, PhD Samuel.Sambasivam@Woodbury.edu Computer Science Data Analytics Woodbury University Burbank, CA 91504

Abstract

Cloud computing is a popular computing paradigm with overwhelming benefits, yet there are complex and unresolved cloud data security vulnerabilities in the usage stage of a cloud data life cycle. The purpose of this design science study was to examine cloud data security vulnerabilities during usage by developing a forensic artifact capable of determining cloud data security vulnerabilities. In line with the research question, the study was based on three propositions: 1) that unencrypted data vulnerability is detectable during usage in the cloud, 2) that detectable vulnerable data in the cloud is recoverable using forensics means, and 3) recoverable data is discernable to the extent that it provides value to the data collector. A total of 9 forensics experiments were conducted in three phases using different configurations to collect and analyze the forensic artifacts required to validate or disprove the research propositions. The findings of this design science study showed that both encrypted and unencrypted cloud datasets in memory during cloud data usage are detectable. Detectable unencrypted cloud data during usage is vulnerable, recoverable, and discernable. Encrypted cloud data during usage is also recoverable but not discernable. However, the practicality of homomorphic encryption, which allows the computation of encrypted data, remains a challenge. Therefore, security practitioners must adopt a defense-in-depth strategy that encompasses administrative, physical, and technical controls to minimize the risk of adversary access to volatile memory.

Keywords: Cloud Data Security, Data Lifecycle Security, Data Usage Vulnerability, Cloud Forensics, Memory Forensics.

1. INTRODUCTION

Cloud computing is a new computing paradigm that is more appealing due to benefits such as ubiquitous network access, easy on-demand self-service, rapid resource elasticity, location independence, resource pooling, and usagebased pricing (Sun et al., 2014). The cloud ecosystem can offer better computing services and other benefits such as business agility, cost savings from management, maintenance, and operations than privately owned on-premises data centers (Alam et al., 2018). However, cloud computing has introduced new and complex data security concerns (Khan et al., 2017; Kumar & Goyal, 2019).

Studies have proposed various procedures to achieve the highest data security level for cloud data protection (Kumar & Goyal, 2019; Matloob, 2017; Mazonka et al., 2020; Singh & Chatterjee, 2017). Subramanian and Jeyaraj (2018) emphasized a need for data protection in all data lifecycle stages in cloud computing. Kacha and Zitouni (2017) described a data lifecycle's usage stage as performing computational processing on cloud data, where risks of misuse or abuse are very high due to many customers in the cloud. According to Mazonka et al. (2020), unlike data in transit and data at rest, which could be protected using encryption, data in use, or performing computation on sensitive data in the cloud, is a single point of failure in computing platforms because current processors operate entirely on plaintexts. To compute on encrypted sensitive data, existing computer architectures must first decrypt, operate on the and then re-encrypt. Unencrypted data. computational data in memory is vulnerable to attack (Singh & Chatterjee, 2017).

Verifying or validating the vulnerability of unencrypted cloud data requires the use of cloud forensic tools and methods (Arshad et al., 2018). However, there are unique challenges in conducting forensics in a public cloud computing environment (Nasreldin et al., 2015). There are architectural, access, jurisdictional, and multitenancy challenges associated with a complete forensic analysis of cloud data (Chaudhary & Siddique, 2017). Amato et al. (2020) described a novel semantic approach for conducting digital forensic that enhances evidence discovery and correlation in cloud computing.

This design science research examined the development of a forensic artifact capable of determining cloud data security vulnerabilities during cloud usage. The artifact development consisted of a cloud forensic investigation in different configurations to identify the configurations that offered the most likely source of unencrypted data vulnerability during cloud usage.

Problem Statement

The problem to be addressed in the research study was that the strategies cybersecurity specialists use to mitigate cloud data security vulnerabilities during usage are lacking (Singh & Chatterjee, 2017). Data security and privacy protection concerns remain the most critical issues in cloud computing (Barnwal et al., 2017; ISC2, 2020). According to International Information System Security Certification Consortium (ISC2) 2020 Cloud Data Security report, 69% of organizations are concerned about cloud data loss or leakage (ISC2, 2020). Another report by CloudPassage for Amazon Webservices showed that 63% of organizations are worried about cloud data loss or leakage (CloudPassage, 2020).

Barona and Anita (2017), Kacha and Zitouni (2017), Subramanian and Jeyaraj (2018), and Sun (2020) discussed different types of cloud data security vulnerabilities inherent in the cloud data lifecycle. During the usage stage, when the data is unencrypted, insiders, or outsiders' adversaries with malicious intentions, can gain access to private data used on cloud platforms illegally (Khan, 2016).

Research Question

The research question that guided the study was: What cloud data security vulnerabilities exist during usage? In line with the research question of the study, the following propositions were made:

Prop 1. Unencrypted data vulnerability is detectable during usage in the cloud.

Prop 2. Detectable vulnerable data in the cloud is recoverable using forensics means.

Prop 3. Recoverable data is discernable to the extent that it provides value to the data collector.

2. REVIEW OF THE LITERATURE

This section examined the existing academic and professional literature on cloud data lifecycle security. Cloud computing is a popular computing paradigm with substantial research on multiple interrelated topics, including data security (Barona & Anita, 2017; Kacha & Zitouni, 2017; Subramanian & Jeyaraj, 2018; Sun, 2020). However, as the section illustrates, there are no definitive studies in the literature on cloud data security vulnerabilities in the usage stage (Singh & Chatterjee, 2017).

Security Concerns in Cloud Computing

Over the last ten years, the cloud risk spectrum has expanded due to an increasing growth for cloud-based prospects for business (Kumar & Goyal, 2019). Critical or sensitive cloud storage data can be remotely accessed by attackers who now have the aptitude to utilize users' login information for remote access (Mattoo, 2017; Vumo et al., 2019). Security concerns in the cloud are a significant issue for 94% of organizations (ISC2, 2020). Another cloud security report by CloudPassage showed that 95% of organizations are concerned about the security of their cloud workloads (CloudPassage, 2020).

Cloud Data Lifecycle Vulnerabilities

There is a need for data protection in all data lifecycle stages (Subramanian & Jeyaraj, 2018). The cloud data lifecycle describes the phases in data from creation to destruction (Kumar et al., 2017). The data lifecycle stages are creation, transmission, storage, usage, sharing, archiving, and disposal (Lin et al., 2014). Creation is the generation of new digital content or updating existing content (Kumar et al., 2017). Storing is the act of committing the digital data to some sort of storage repository and typically occurs simultaneously with nearly creation (Subramanian & Jeyaraj, 2018).

The viewing, processing, or using data in some describes the data usage stage activity (Subramanian & Jeyaraj, 2018). Kacha and Zitouni (2017) described data-in-use as performing computational processing on the cloud data, with a very high risk of misuse or abuse due to many customers in the cloud. The share stage describes activities such as exchanging data between users, customers, and partners (Kumar et al., 2017). In the archive phase, data leaves active use and enters longterm storage (Kumar et al., 2017). The disposal phase describes data destruction using physical or digital means (Kumar et al., 2017). Data deleted from storage media is not entirely erased because file systems cannot remove data; therefore, attackers may use data scavenging techniques to recover deleted data (Khan, 2016).

Data in use and remanence are green pastures for research (Subramanian & Jeyaraj, 2018). There are security vulnerabilities within the SaaS, PaaS, and IaaS models and all the cloud data lifecycle stages (Kumar et al., 2017). It is impossible to process encrypted data either in the cloud environment or in on-premises environments (Kumar et al., 2017). Static data used in cloud applications are usually unencrypted because encrypted data prompts for keys during processing (Kumar et al., 2017).

Encryption

Matloob (2017), Mazonka et al. (2020), and Lo'ai and Saldamli (2019) described encryption as one of the well-known and best solutions for securing data in the cloud. Encryption encodes information into a coded structure and transforms it back to the original state (Matloob, 2017). However, it is impossible to protect datain-use with encryption either in the cloud environment or in on-premises environments because existing computer architectures must first decrypt, operate on the data, and then reencrypt (Gaidhani et al., 2017). Other solutions in the academic literature from Alaya et al. (2020), Farokhi et al. (2017), Li et al. (2020), Tran et al. (2020), and Xiong and Dong (2019) focused on using some form of homomorphic encryption schemes to solve the cloud computing data security problems in the usage stage. However, homomorphic encryption has implementation challenges practical for widespread deployment (Alabdulatif et al., 2020; Alloghani et al., 2019; Geng, 2019; Ullah et al., 2019).

Digital Forensics

Digital forensics is a practice that uses scientifically driven and verified methods toward the identification, preservation, acquisition, analysis, interpretation, and documentation of digital data and source analysis and presentation of evidence for reconstructing suspicious events (Palmer, 2001). Digital forensics focuses on forensic procedures, legal approaches, and evidence (Serketzis et al., 2019).

Conducting forensics in a cloud environment is problematic due to the highly distributed and complex cloud architecture (Arshad et al., 2018). Also, established digital forensics practices such as searching and collecting data are not feasible in the public cloud environment due to the lack of individual ownership of devices and the volatile nature of data stored in the cloud (Arshad et al., 2018).

Challenges in Cloud Forensics

There are many unique challenges for conducting digital forensics in a public cloud computing environment (Nasreldin et al., 2015). Some of the cloud forensic challenges include architecture, data collection, evidence analysis, incident first responder, legal, standards, and training (Chaudhary & Siddique, 2017). Other forensic challenges unique to cloud computing jurisdiction, multi-tenancy, are and CSP dependency (Chaudhary & Siddique, 2017). Traditionally, the forensic investigator controls the evidence collection, but in cloud computing forensics, access to the evidence may not be physically available (Chaudhary & Siddique, 2017). The investigator also faces challenges in analyzing available logs and artifacts (Tak et al., 2018). The forensic investigation challenges in the cloud computing environment are also related to evidence control, collection, preservation, and validation (Tak et al., 2018). There are also unique digital forensics challenges within the IaaS, PaaS, and SaaS models (Chaudhary & Siddique, 2017).

Gaps in the Literature

Studies have proposed various procedures to achieve the highest data security level for cloud data protection (Kumar & Goyal, 2019; Matloob, 2017; Mazonka et al., 2020; Singh & Chatterjee, 2017). Mazonka et al. (2020) posited that unlike data in transit and data at rest, which could be protected using encryption, data in use, or performing computation on sensitive data in the cloud is a single point of failure in computing platforms because current processors operate entirely on plaintexts. To compute on encrypted sensitive data, existing computer architectures must first decrypt, operate on the data, and then re-encrypt. Public cloud data usage security remains an unresolved concern affecting critical user information privacy and requires more research (Singh & Chatterjee, 2017).

3. METHOD

Design Science was the most appropriate research methodology for this forensic study. According to Edmondson and McManus (2007), implemented research is a mature theory because components used to create an artifact are meticulously studied and documented in the body of knowledge but lacks a developed artifact for the research purpose. Peffers et al. (2007) stated that design science methodology is used to create a knowledge discovery artifact for a research problem. The result of a design science research study is the purposeful creation of an artifact, which can be a product, process, technology, tool, methodology, technique, procedure, or any combination for achieving some purpose (Lapão et al., 2017; Peffers et al., 2007).

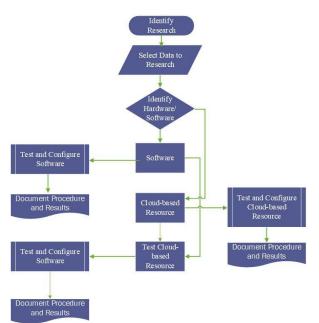
Research Design

The research design was implemented in a standard public cloud operational environment using standard vendor installation instructions. The overall design consisted of two virtual machines (VM) servers hosted in a public cloud, two VM workstations hosted in the public cloud, and a physical workstation. Memory and other research data were collected from the cloud servers using forensics tools and procedures during data computation analysis. The setup of the design allowed for a repeatable process that was easily documented.

Artifact Design

Digital forensics is a practice that uses scientifically driven and verified methods toward the identification, preservation, acquisition, analysis, interpretation, and documentation of digital data and source analysis and presentation of evidence for reconstructing suspicious events (Palmer, 2001). Cloud forensic investigation involves five primary dimensions: data collection, evidence segregation, virtualized environment, preservation of evidence, and reporting and documentation (Chaudhary & Siddique, 2017). Dynamic digital forensics is a forensic data collection and analysis of a running state system or distributed across multiple locations (Arshad et al., 2018). Forensics specialized forensic software includes or hardware that enables a complete digital investigation (Alenezi et al., 2019).

Figure 1 Methodology for Forensic Evaluation



Note. Methodology for forensic evaluation

Forensic methods were used to validate or disprove the research propositions through a rigorous process of data collection. Data collection approaches were tested to identify controlled data from the sets testing environment. The research was conducted in three phases. Phase I of the study involved installing hardware, software, and testing without external or internal manipulations. The VM servers and workstations were deployed in Microsoft Azure public cloud with default settings. Initial data were collected and analyzed

to determine if there were identifiable data to document.

In phase II, controlled use of client-server applications with encrypted cloud data was introduced to the same configuration in phase I. The encrypted data was downloaded to the VM server and opened through a client-server interaction via Simple Message Block (SMB), making the encrypted data available in memory (data-in-use). Data was collected using forensics tools from the Azure VM servers and analyzed. In phase III, the same default configuration settings from phase I was used but with controlled use of client-server applications using unencrypted cloud data to determine data vulnerability in memory. Figure 1 illustrates the methodology used for the forensics evaluation using free and publicly available specialized forensics software (FireEye's Redline) and hardware for the research.

Figure 1 illustrates the basic flow of the methodology used for the forensic evaluation, from identifying the problem, selecting data, identifying hardware and software for testing and configuration, and documenting the procedures and results at each stage.

Collection of Running Memory

Data was collected from the VM servers in the public cloud and examined according to standard forensic guidelines to provide unaltered data supported by documented collection procedures used in each phase of the collection and analysis process. Data were categorized in each phase of the collection process according to data type, date and time collected, test case number, and test case descriptions. Forensics data collection and storage procedures were applied in all data collection for this study.

4. FINDINGS

Description of the Study Sample

The research used random samples of Indicators of Compromise (IOC) obtained from the following publicly available, accessible, and open-source projects:

https://github.com/topics/ioc

https://cyberwarzone.com/download-indicatorsof-compromise/

IOCs are forensic artifacts observed in an operating system or on a network and utilized to indicate a computer intrusion and detect cyberattacks in an early stage (Catakoglu et al., 2016).

The sample IOC data and two non-IOC data were used in the study. Table 1 summarizes the

sample data used to validate cloud data security vulnerabilities during usage.

Results

In phase I, the test environment (two VM servers and two VM workstations) was built on Microsoft Azure public cloud with default settings on Windows operating systems as described in Section Three. Various techniques and tools can be employed in digital forensics to analyze live memory (Al-Sharif et al., 2018). The VM servers and workstations were initially analyzed using Redline forensic software and manual hex searches of the file system to ensure the datasets were not present. Figure 2 shows Redline Command run to capture active memory of VM Server1 during interaction with VM Workstation1 with no dataset on the Server. Volatile memory analysis can be performed using four unique methods: file carving, process-object searching, string search, and file signature search (Thantilage & Jeyamohan, 2017). This study used string searches and process-object searches for the analysis of the collected memory artifacts.

Table 1
Description of Sample Data Sets Used in
Ctool of

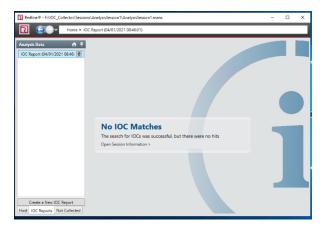
		Study	,	
Dataset	Sou rce	Deploym ent Method	Errors on Client	Operating System
www.ap icola.cl	IOC	Notepad	None	Windows Server 2019
halkban kasi.cf	IOC	Word Documen t	None	Windows Server 2019
paypalll .ga	IOC	Word Documen t	None	Windows Server 2019
quiroga .cl	IOC	Notepad	None	Windows Server 2019
\$Daniel &Amoa h\$	Non - IOC	Word Documen t	None	Windows Server 2019
COVID- 19	Non - IOC	Word Documen t	None	Windows Server 2019

Figure 2 Commands run on VM Server1 to Capture Memory with No Dataset

s PC > Data (F:) > NoSampleCollecto	Date modified Ty	De	Size	✓ Ŏ Search NoSamp
C:\Windows\Svstem32\cmd.exe				
1.1				
ing the proper working d	irectory			
ring the proper working d	irectory pleCollector\\Sessions\A	nalysisSession	n1\Audits" -f "M	emoryzeAuditScript.xml"
uring the proper working d	irectory pleCollector\\Sessions\A	nalysisSession	n1\Audits" -f "M	emoryzeAuditScript.xml"
<pre>C:WindowsSystems2(cmd.exe uring the proper working d x64\xagt.exe" -o "F:\NoSam</pre>	irectory pleCollector\\Sessions\A	nalysisSession	n1\Audits" -f "M	emoryzeAuditScript.xml"
uring the proper working d	irectory pleCollector\\Sessions\A	nalysisSession	n1\Audits" -f "M	emoryzeAuditScript.xml"
uring the proper working d	irectory pleCollector\\Sessions\A	nalysisSession	n1\Audits" -f "M	emoryzeAudítScript.xml"

The captured memory data from VM Server 1 was analyzed, as shown in Figure 3. The forensic analysis showed no indication of the presence of the research dataset in memory during the interaction between VM Workstation 1 and VM Server 1.

Figure 3 Forensics Analysis of VM Server1 Memory with No Dataset in Memory



Note. Figure 3 shows an initial view of the IOC search report for possible matches in the sample_ioc dataset in the collected memory.

Figure 3 shows that the captured memory has no elements of the sample_ioc dataset in the memory of VM Server1.

In phase II, controlled use of a client-server application with encrypted cloud dataset was introduced to VM Server1 using methods described in Section Three. The encrypted data was accessed via VM Workstation1 but not decrypted. VM Server1's live memory was captured and analyzed during the client-server application interaction, as shown in Figure 5.

Figure 4 Forensics Analysis of VM Server1 with No Dataset

inalysis Data 🛛 👘 🖣	Filos #	Enter string to \$		P 2	InAlFide * Deaton	multites Free Next	
System Information 4 Processes	Review Processes Hierarchically	C Process N	nne Pl	Peth		Arguments	Usemane
Handles	Randics This view shows the relationship	System	4				NT AUTHORITIVS ISTEM
Memory Sections Strings	pavent processes	S Regist	y 95				NT AUTHORITIVSYSTEM
Rotex Elementhical Processes		S	• •	•			NUMBER
Fie System		() (P10.0)	. 64	2			NTALTHORT/SYSTEM
Report		🔿 + virkes	men 70	Civit-	Jone apten 22	winlegenase	NT AUTHORITIVE/STEM
Windows Strekes Perikterice		C Logor	Uloe 48	6 Gillin	ions/apster/82	"Logovillese" /lags/bil /state0/bulbd8855 /state1/bi4/c6	NT AUTHORITY/SYSTEM
Lines		🕤 dama	se 50	Citilities	Sowellaythem 32	"domese"	Window Manage1/DWM
Event Logs Texts		C torte	there are an	Contraction of the second	iouri/system/2	Tantinhot.eve	Loct Crier Horty MID
Ports		🕥 + winteg	inusos 20	as ciwin	down/aystem32	winlegen.aue	NT ALTHOR TV SYSTEM
ART Entries		🕤 uluma	ne 19	0 CM	Annalapston 22	"domase"	Window Manageri DWN
Route Ermiss			viex.exe 39	2 0816	iows/system32	"fantdryhostese"	Fort Onker HostsUMPD
Disks		C (1956)	e 12	18			NT AUTHORITY/SYSTEM
Volumes Registry Hives			noRign. St	is copies	aged PLg of Microsoft AssetD	"DeporterPlug new" DeporterPlug in-Shindown Switt D.	NUMERONITY/SYSTEM
Browser USL History		🔘 conha	stava 73	Cilline Cilline	dowel/aystam32	\7%C5Windows\aystem22conhost.exe 0x4	NT ALTHOR TV SYSTEM
Brower UKL Hatory Tensing		🐑 🔸 Marik	without 48	4 GPub	apol Plagini Microsoft AvenuD.	"CPackages/Pagin/Microsoft.Acore.Diagnostics.ladDiagn.	NT AUTHORITIVE/STEM
Tags and Comments		Non	AgentMan. 8	CIPECK	aged PLgind Microsoft Asure D.	-serviceShutdownMonAgentShutdownEvent.4844 -parent 4.	NT AUTHORITIVISISTEM
Arguntus likitay		S 140	Agentical and	a czewa	aget M. good Microsoft Acure D.	-deploymental: 123/Reliaged/Regint/Microsoft/Journ Dag-	NT AUTOOPTION STOR
		🕥 conh	orteon 38	6 Cylin	iow/gyteen32	V7XCSWindows/system323conhost.exe 0x4	NT ALTHORITY/SYSTEM
		🚫 + Esplore	.DE 62	S CiWie	lows	C/Window/Explorer.E/E	dal/Moever/Indexcah
		Bullin	eon G	4 GPres	ram Files (x86)/Red inc	"CIP ogram Files (d6) RecEnc/Red ins one"	dat/MonverTrakenoph
			Sartholki 13	4 CIProp	ram Files (x80)/Aed ine Mandia	"CP og an Files (ddf/Recline/Mand ant/bolkd/Mandiant).	dai/Moener/Ldamoah
		• • • • • • • • • • • • • • • • • • •		a come	rem Film (MRA) with ref Lines	Tophogram Files (alth) (Section), //opent/site/.org/.ese1.co.Ti-	dell'Americani della d
		0 00	shortese 30	a cana	iowijeyteen32	V7X59Undows/system32.conhost.exe 0x4	del/Moenverlindemoch
			tos 97.	12 Cifres	ram Files (x00)/Red incl Agentia	"CIP-ogram Files (ddf/RecEne/Agent/s/Hoagtase"mod	dal/Muerver/Indexeah
			tox 0	2 CiPres	ram Files (x86)/Red incl Agentiv.	"CIP og an Files (df) RecEnclagent's 64 sagt esc" - mod.	dai/Muerver/Ndamoah
		() con	loter 65	S CIMA	Stand System 32	V7CI0Mindows/system32/conhost-exe 0x4	dai/Meever/\damoah

Note. Figure 4 shows that while no sample_ioc data was found in memory, other data elements not considered were available in memory.

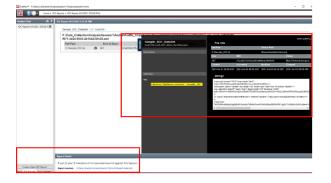
Figure 5 Forensics Analysis of VM Server1 Memory with Encrypted Dataset Match

	Hone + H	ost • Herarchisal Processes	_						
Analysis Duta		Filters #	100	plejoc	P	te All Failule - One Color	er Elleren Preizr Naut 1 matub found		
System Information Review Processes Hierarchically 4 Processes	0	Process Name	PID.	740.	Argumenta	Usemane			
Handles		This view shows the relationship between all of the processes and their	õ	* Tablic as	6872	C/Program Files/Common Files/micros	/Quite/s 000000000000000000000000000000000000	dal/MorrierTidamoal	
Memory Sections Strings		parent processes.	1 S	TabTip32.eve	2944	C/Program Files (x863/Common Files)	/cadhooks /Parent00000000001ad8	daVMserver?tdamoal	
Ports			0	lass.eve	840	C/Windowslavstern32	C18Indowd pytters32/sass.eve	NT AUTHORITY/SYST	
P file System			18	C0105.414	606			NT AUTHORITY/SYST	
Registry			0	+ winlogon.exe	756	C1Windownlaystem52	wintogon.ava	NT AUTHORITY/SYST	
Windows Services Persistence			0	foreduriostasa	1520	C/Window/uystem32	"fontdryhost.eve"	Ford Driver Host UM	
Users			6	Logorillese	1054	C/Windowslaystem32	"Loponial ever" /flags/bi2 /statel/bia?bd1855 /state1/bi41c6	NT AUTHORITY/SYST	
Event Logs 1 Tasks			0	dumeie	1072	C/Windowsloystem32	'dwnee'	Window Manager/D	
Ports			6	+ Diagnostic/Regin_	3060	C/Packages/Plugins'MicrosoftAzureD	"DisgnosticsPupinese" DisgnosticPlugin-ShutdownEvent D.	NT AUTHORITY/SYST	
ARP booves			0	conhost.exe	3040	C1Windowdaystem32	VITC/Windowshaystem312conhost.eve 0x4	NT AUTHORITY/SYST	
Route Entries			0	+ ManAgenthiast	5256	C/Packages/Progins/MicrosoftAgureD	*C1Packager/Plugin/MicrosoftAgure.Diagnostics.lasSDiagn	NT AUTHORITY/SYST	
Registry Hives			0	conhostere	3372	C/Window/aystem32	V7/C/Windows/system32/controltave 0x4	NT AUTHORITVISYST	
Browser URL History Turneline			0	Monligentilian.	5176	C/Packaged/Pugins/MicrosoftAzureD	-serviceShutdown MonAgentShutdownEvent.3956 -parent 5	NT AUTHORITVISYS	
Tanging Tags and Comments	- 1		0	MonAgentCon.	6116	C/Packaget/Pugint/MicrosoftAzuraD	-deploymental "CiPackaget/Pugint'Microsoft.Azure.Dag	NT AUTHORTY/SYST	
Acquisition History					0	+ winlogon.eve	4532	C:Windowskystem52	winlogon.exe
			0	fortdn/host.ese	1108	CNWindows/system32	"fontdh/host.eve"	Fore Driver Hosti LIM	
			0	dwm.exe	6052	C//Windows/system32	'dvmexe'	Window Manager/D	
				0	LogonUlese	8748	CNWindowslaystem32	"LogonUlexe" /Reps/hi0 /statelh/ha248e855 /state10x41c5	NT AUTHORITY/SYST
			0	CP35-EHE	6868			NT AUTHORITY/SYST	
	_		0	A Desires Diff	21/15	C.Wadna	Cillingue Labor Dil	del Marrie Colonia	
			0	NOTENALEXE	4565	C///Vedow/aystam32	ChWedowhaystaw320/01EMD-DE* Crategory be	daVMserver7;damoa	
			V	 Refinere 	7552	C/Grogram Files (c04)/Redline	"C/Program Files (x84)/Redine/Redine.exe"	daVMserver?tdamoa	
			0	 MandiardTopki 	6404	C/Uropan Files (s86)/Redine/Mandia	"ChProgram Files (x84)/Redine'MandiantTookit/MandiantT	daVMserver?tdamoa	
			0	conhoit.eve	6035	C/iWindows/system32	VTVC//Windows/system32/controls.eve 0x4	daVMserverTidamoa	
			0	 xagtese 	8072	C:Program Ries (xM)/Aedine'/Agent.x	"C1Program Ries (d81)/Redinel./Agent/s64/xagt.eve" -a "P	da/Mserver?/damoa	
			0	conhostene	1100	CNWndows/system32	\271C/Windows/system321conhost.eve 0x4	deVMserver%damoa	
			0	sagt.eve	6132	C/Program Files (s06)/Redline/Agentics	*C1Program Files (s86)/Redline/Agent/u64/wagt.exe*mod	daVMserver?tdamoa	
			0	saptese	8168	CVProgram Files (x66)/Redine/Agentix	"ChProgram Files (x8E)/Redline'Agent/u64xagLexe"mod	de/Moerver?/damoa	

Note. As shown in Figure 5, the forensics analysis showed the encrypted sample IOC dataset in memory.

A search for "sample_ioc" on hierarchical processes in memory returned one match, but the dataset file was encrypted and, therefore, not discernable. Encrypted dataset elements were detected in the memory analysis of VM Server1 during the client-server interaction.

Figure 6 Forensics Analysis of VM Server1 Memory with Encrypted Dataset Match Details



Note. In Figure 6, the memory analysis of VM Server1 with the encrypted dataset match was expanded to show the contents of the dataset file.

As shown in Figure 6, the contents of the sample_ioc encrypted dataset were not discernable.

Figure 7 Forensics Analysis of VM Server1 with Search Terms for IOC Dataset Elements

elysis Data 🏾 🕐 🔻	Filters #				
stee lafe maties		COVID-19	P In All Fields Char Colu	ann Titless Prev Next No matches found	
competi	Review Processes Hierarchically	Process Name	PID Path	Arguments	Usemane
Handles	This view shows the relationship between all of the processes and their	· + agenterap.eve	5172 CIProgram Files/Microsoft Dependenc.	CIProgram Files/Microsoft Dependency Agent/bir/agentw.	NT AUTOCRITOSYSTEM
Memory Sections Strings	parent processes.	MicrosoftDep.		"CIProgram File/Microsoft Dependency Agent/bin/Micros	
Porta marihiral Processes		Surfact and	5632 CTWindow/Sistem32	C/Windows/Sustem32/suchost.exe -k LocalServiceNoNetwo.	
dine* - F/Data_Collection/And	ysisSession/AnalysisSessionLowns				
Garan a Marrie M	ost + Herarchical Processes				
vis Data 👩 🔻	film #	psypsiliga	P In All Fields Cour Color	na Fillers Prov Not. No matches found	
ten Information	Review Processes Hierarchically	Process Name	PID Path	Arguments	Usemame
Handles	This view shows the relationship between all of the processes and their		5172 C/Program Files/Microsoft Dependenc	"C/Program File/Microsoft Dependency Agent binlagentw	NTAUTHORITY/SYSTEM
Memory Sections Strings	parent processes.	MineroffDea.	4929 C/Program Filer/Microsoft Dependenc.		
Ports wanthing Provenues		C actuates	5632 C1Windows/System32	C/Window/SintemS2ievchost.exe -k LocalServiceNoNetwo	NT AUTOORTOLOGY IS
vis Deta 🖷 🖷	Filten #	hukhankasi.cf	P M In All Fields * Cherr Cole	was filtern Prov. Next. No matches found	1
tem information	Review Processes Hierarchically	C. Process Name	PD bib	Arguments	Username
cesses Handles	This view shows the relationship	D + agenturap.eut		. 'CliProgram Files/Microsoft Dependency Agent/bin/agentu.	
Memory Sections Strings	between all of the processes and their parent processes.	NicrosoftDep.		 CiProgram Files/Microsoft Dependency Agent/bin/Micros. 	
Ports sechical Processes		C scholler	5632 CI/Windows/System32	C1/Window/System32/archostese -k LocatieniceNoNetuo.	
	lysisSesienTAnalysisSesienTunans	0			
G Bone + H	ost + Herarchical Processes				
	Films #				
de Data 🚓 🔻					
	Benders Benners (Bennethauth)				
tem Information Cestes	Review Processes Hierarchically This view shows the relationship	Process Name		- games	
ds Dota n 7 7 tem Information cestes Handles Memory Sections Strings		Process Name	5172 C/Program File/Microsoft Dependenc	*C/Program File/Microsoft Dependency Agent Ibin/Agents *C/Program File/Microsoft Dependency Agent Ibin/Microsoft	
		\$DarriefBiAmoah\$	P in Al Reids · Over Gela	an Filmers Prev Next No matches found Arguments	University

Note. In Figure 7, the forensics analysis of VM Server1 Memory was further expanded with specific search terms for known IOC dataset elements in the sample_ioc dataset.

The dataset elements "COVID-19", "paypall.ga", "halkbankasi.cf", and "\$Daniel&Amoah\$" were used individually at different times as search criteria on the captured memory of VM Server1. Each of the searches resulted in "no matches found." The results clearly showed that an encrypted dataset in memory is not discernable. In phase III, the unencrypted sample dataset was introduced to VM Server2 with the same default configuration settings as in phases I and II. A client-server application interaction was initiated from VM Workstation2 to VM Server2 to access and use the unencrypted datasets. A live memory of VM Server2 was captured with the forensic tool and analyzed, as shown in Figure 9.

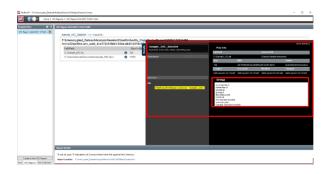
Figure 8 Forensics Analysis of VM Server2 Memory with Unencrypted Dataset

ndysh Data 📫 🖣	Film #	sample, isc	p	17	In All Fields + Cleve Column 1	max Prev Next 2 metches found	
System Information	Review Processes Hierarchically	D Poces	s Nave	PID	Fats	Arguments	Usename
Herarchical Processes	This view shows the relationship instrument all of the processes and their	0 .	chestere	7340	CliWindows/System32	C/Windows/Josters32/avchast.exe -k network-p -s NetSet.	NT AUTHORITY/SISTEM
File System	parent processes.	0 14	0.010	848.	CitWindowslaysters32	C/Windowslaystem32/sassleve	NT AUTHORITINSISTEM
Registry Windows Services		() + m	logon.eve	5216	ClWindows/aystem32	wriogonaa	NT AUTHORITY/SISTEM
Persistence		5 de	nee	4952	C1Windowelaystem32	"dum.eve"	Wedge Manage/DIM
Users Event Loss		O 14	individualitative	4964	Clilledows/aythen32	"fortdy-heat ava"	Fort Driver HestigMFD
Tanks		Par a la	and the second s	1.014	Collination .	Citized and a second se	destal and descel
Ports DNS Pertner		O M	TEMPERE	420	Cital/Indover/aystem32	COMedawingstani20A0TEND DB* Committee Based	del/Hiener2idamosh
ABP Entries Route Entries		ō .	NROMENIA			*COngram Flas (JdR) Internet Explorer/3009.CRI.001* S.,	
Daka			PLOPLETS			Compton rate party and a spectra and a second secon	
Volumes Registry History						Concern net obtaineret batter (DRUME DE SUE SUE SUE SUE SUE SUE SUE SUE SUE SU	
Browser URL History			APLORE FUE			Conspan resident and an an appendix and a second se	
Tinution			NEGRATIA				
Tags and Comments			SPICIELE		CliProgram Nes (x80) Internet bu- CliProgram Files (x80) Redine	"C:Program Files (JAR) Internet Explorer/IEXPLOREEXE" S., "C:Program Files (JAR) Archite/Red/incerer*	devisioner?danceh
Acquisition History					CProgram Nes (dd)/Redine	C/Program Files (dB) Redire Pedire Evel "C/Program Files (dB) Redire/MandardTook//Mandard.	
			and an look college.			C:Program Film (dD) And iner Mandaer Crucket Mandaert, 'C:Program Film (dD) And iner/, Appent/old (appl ener) -o "	
				420			
					CliWindewslaysten32	177/CIWedowslaysten32/conhost.exe 0x4	deVHServer2idanceh
		2	ngtere			"C/Program Files (dB)/Red ine'Agent u64/segt.ess" - mo	
		0	saytese	2426	CiProgram Files (xMC/RedFine)Ag.	"ClProgram Files (d6) Red inc'Agent add augteur" - ma-	devMServer2idamoah
		-			Contract of the second	and the second s	
		0 w	INCREMENT.	8030	CliProgram Filed/Microsoft Office	"Cr/Program Files/Microsoft Office/Dfice15W/8W040.EX.	deVillaner2idanoah
		12					

Note. As shown in Figure 8, the forensics analysis showed the unencrypted sample IOC dataset in memory with a search for "sample_ioc on hierarchical processes.

The search returned two matches for sample_ioc datasets in Notepad and Microsoft Word, representing a match for each deployment method for the sample_ioc dataset. However, further trace analysis of the sample_ioc on the captured memory showed all the unencrypted sample_ioc dataset in memory, as shown in Figure 9.

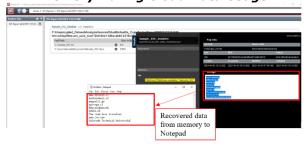
Figure 9 Forensics Analysis of VM Server2 Memory with Unencrypted Dataset Match Details



Note. In Figure 9, the complete unencrypted sample_ioc dataset was discernable and accessible in memory.

As shown in figure 9, the IOC search report on the captured memory image returned one match, but the dataset file was encrypted and not discernable. The unencrypted dataset elements were detected in the memory analysis of VM Server2 during the client-server interaction and usage of data.

Figure 10 Forensic Data Recovery from VM Server2 Memory During Cloud Data Usage



Note. Figure 10 shows a detectable and discernable sample_ioc dataset that was easy to highlight and copy into the Notepad application on a standalone forensic workstation. The copied dataset provides great value to the data collector because it reveals secret information.

The collected artifacts' examination and analysis reviewed three significant themes: data detectability in memory, discernability of data in memory, and recoverability of data in memory.

Data is Detectable During Cloud Data Usage

The collected memory artifacts' analysis showed that both encrypted and unencrypted datasets were detectable in memory during cloud data usage. The artifacts in phases I, II, and III indicate that encrypted and unencrypted data is detectable in memory during usage in the cloud. In phase I, where no sample data was introduced in the examination, collection, and analysis, other non-sample data were observed in memory, as shown in the captured forensic memory analysis in Figure 4. In phase II, encrypted sample ioc data was introduced to VM Server1, and the encrypted data was accessed via a client-server interaction. The collected live memory analysis showed the encrypted sample_ioc dataset, as shown in Figures 5 and 6. In phase III, the unencrypted sample_ioc dataset was also observed and captured in the analysis shown in Figures 8 and 9. The finding in the three phases addresses the first research proposition: that unencrypted data vulnerability is detectable during usage in the cloud.

Data is Recoverable During Cloud Data Usage

The collected artifacts' analysis showed that detected cloud data in memory could be recovered using forensic tools, as shown in

Figure 10. The forensic examination and analysis showed that both encrypted and also unencrypted data could be recovered in memory. However, encrypted data in memory does not provide immediate value to the data collector because data confidentiality is not compromised. On the other hand, unencrypted data in memory is vulnerable and provides immediate value to the data collector because there is no data confidentiality, as shown in Figure 10. The forensic artifact in Figure 10 supports the second research proposition: detectable vulnerable data in the cloud is recoverable using forensic means.

Data is Discernable During Cloud Data Usage

Data discernability describes the ability to identify specific or unique datasets in memory valuable to the data collector. In phase II, the forensic analysis showed that encrypted data in memory is not discernable, as shown in Figure 6. Encrypted data does not reveal any specific data elements and, therefore, retains data confidentiality. Unencrypted cloud data during usage, on the other hand, is discernable in memory, as shown in the collected and analyzed artifacts in Figure 10. Unencrypted data in a file system can be viewed and recovered (Shashidhar & Novak, 2015). The collected forensic artifacts showed that unencrypted cloud data during usage is discernable and, therefore, vulnerable.

5. DISCUSSION

The purpose of the design science study was to examine cloud data security vulnerabilities during usage by developing a forensic artifact capable of determining cloud data security vulnerabilities. The study determined whether unencrypted data vulnerability was detectable, recoverable, and discernable during usage in the cloud.

Theme 1: Defense-in-Depth Strategy to Safeguard Data Detectability in Memory

As indicated by the collected memory artifacts, encrypted and unencrypted cloud datasets in memory during cloud data usage are detectable. The ability to detect datasets in memory during cloud data usage means data is vulnerable while in memory. Since data in memory is detectable, unencrypted data in memory is a serious threat to data security. There is, therefore, a need for cybersecurity specialists and practitioners to consider strategies and technologies to protect data in memory. There are different strategies and approaches for safeguarding datasets in memory. According to Mazonka et al. (2020) and Lo'ai and Saldamli (2019), one of the well-known and best solutions for securing datasets in the cloud is encryption. Encryption is a process that converts plaintext data into cyphertext. However, it is currently impractical to protect data-in-use with encryption (Gaidhani et al., 2017; Kumar et al., 2017; Miyan, 2017). Homomorphic encryption is an encryption scheme that allows computation on encrypted data without first decrypting the data (Gaidhani et al., 2017). However, homomorphic encryption has practical implementation challenges widespread for deployment and adoption (Alabdulatif et al., 2020; Alloghani et al., 2019; Geng, 2019; Ullah et al., 2019).

A significant part of the data detectability in memory vulnerability is access to the volatile computer memory. It is, therefore, critical for cybersecurity specialists and practitioners to adopt comprehensive layers of different controls (defense-in-depth) to minimize the risk of access to the vulnerable memory (Mazonka et al., 2020; Rocha et al., 2013). Controls such as policies, identity and access management, personnel security, physical security, network security, host-based security, and application among other controls, security, effectively reduce the risk (Jeganathan, 2018). Cybersecurity specialists can implement layers of technical and administrative controls to reduce the risk of vulnerabilities (Kumar & Goyal, 2019).

Theme 2: Use Available CSP Tools and Controls to Reduce Recoverability of Data in Memory

Recoverability of data in memory was the next theme from the findings of the collected and analyzed artifacts in phase III. The forensic examination and analysis showed that both encrypted and unencrypted data could be recovered in memory. The study artifacts provides that encryption showed data confidentiality because recovered encrypted datasets from memory remained encrypted and did not reveal any data secrets to the data collector. The study has shown that encrypted cloud data remained encrypted when accessed through client-server interaction. However, performing a computation or using encrypted data in computing platforms remains a challenge because current processors operate entirely on plaintexts (Mazonka et al., 2020).

The study also showed that unencrypted cloud data in use are vulnerable and recoverable. It is, therefore, critical for cybersecurity specialists and practitioners to adopt available cloud service provider (CSP) tools and strategies to secure cloud data during usage. For instance, within the Azure cloud platform, enabling Just-in-Time VM access restricts the VM's management ports and grants access on-demand for a limited time to only pre-approved IP addresses. Using a bastion service to connect the VMs also protects the VMs against exposing the public IP on the VM. Using conditional access policies to restrict access and auto-shutdown VMs also reduces the risk of data recoverability in memory. There are multiple administrative and technical controls and strategies to safeguard unencrypted data in memory to prevent unauthorized recoverability (Subramanian & Jeyaraj, 2018). There is no silver bullet when it comes to protecting unencrypted data in use. No single technology ultimately provides the required protection (CSA, 2017). However, using available CSP tools and controls to enforce administrative and technical controls reduces the risk of recovering unencrypted data from memory.

Theme 3: Device Management and Isolation to Reduce Discernability of Data in Memory

The study artifacts showed that collected encrypted cloud data usage in memory is not discernable, as demonstrated in phase II. It is impossible to identify unique data elements from encrypted cloud data collected from memory without decrypting the data, as shown in Figure 6. On the other hand, unencrypted cloud data in use is vulnerable, recoverable, and discernable without decrypting the collected data, as shown in Figure 10 in the study artifacts. Unencrypted discernable data in memory is vulnerable to bus snooping attacks (Tavana et al., 2017). The risk of volatile memory vulnerability depends on access to the cloud-based resources memory; therefore, cybersecurity specialists and practitioners should implement strona authentication mechanisms through identity and access control, device management, zero-trust security model principles, and device isolation as part of broader layers of controls to minimize the risk to unencrypted data in use.

6. CONCLUSIONS

The results of the design science study showed that data could be detected during cloud usage in memory. The results also indicated that cloud data detected during usage could be recovered from memory. Finally, the results showed that encrypted cloud data usage in memory was not discernable while unencrypted cloud data in use was vulnerable, recoverable, and discernable.

The findings of this study apply to all information technology settings that use sensitive data in public cloud computing. A quantitative or qualitative study on cloud data usage security would add to the body of knowledge a comprehensive list of practical approaches cybersecurity professionals can use to minimize the risk of cloud data usage vulnerability. The practicality of homomorphic encryption also requires more research.

7. ACKNOWLEDGEMENTS

I want to acknowledge the support, encouragement, and guidance I received from my research supervisor, Dr. Samuel Sambasivam. Thank you, Dr. Sambasivam. Your counsel made the path to success on the doctoral journey clearer.

8. REFERENCES

- Alabdulatif, A., Khalil, I., & Yi, X. (2020). Towards secure big data analytic for cloudenabled applications with fully homomorphic encryption. *Journal of Parallel and Distributed Computing*, *137*, 192-204. https://doi.org/10.1016/j.jpdc.2019.10.008
- Alam, S., Muqeem, M., & Suhel, A. K. (2018). Review on security aspects for cloud architecture. International Journal of Electrical and Computer Engineering, 8(5), 3129-3139. http://doi.org/10.11591/ijece.v8i5.pp3129-3139
- Alaya, B., Laouamer, L., & Msilini, N. (2020). Homomorphic encryption systems statement: Trends and challenges. *Computer Science Review*, *36*, 100235. https://doi.org/10.1016/j.cosrev.2020.1002 35
- Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness Framework for organizations. *Journal of Cloud Computing*, 8(1), 1-14. http://doi.org/10.1186/s13677-019-0133-z
- Alloghani, M., Alani, M. M., Al-Jumeily, D., Baker, T., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2019). A systematic review on the status and progress of homomorphic encryption technologies. *Journal of*

Information Security and Applications, 48, 102362. https://doi.org/10.1016/j.jisa.2019.102362

- Al-Sharif, Z. A., Bagci, H., Zaitoun, T. A., & Asad, A. (2018). Towards the memory forensics of MS word documents. In: Latifi S. (eds) Information Technology - New
 - Generations. Advances in Intelligent Systems and Computing, vol 558. Springer, Cham. https://doi.org/10.1007/978-3-319-54978-1_25
- Amato, F., Castiglione, A., Cozzolino, G., & Narducci, F. (2020). A semantic-based methodology for digital forensics analysis. *Journal of Parallel and Distributed Computing*, *138*, 172-177. https://doi.org/10.1016/j.jpdc.2019.12.017
- Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. *Journal of Information Processing Systems*, 14(2). https://doi.org/10.3745/JIPS.03.0095
- Barnwal, A., Pugla, S., & Jangade, R. (2017). Various security threats and their solutions in cloud computing. https://doi.org/10.1109/ccaa.2017.8229923
- Barona, R., & Anita, E. A. M. (2017). A survey on data breach challenges in cloud computing security: Issues and threats. https://doi.org/10.1109/iccpct.2017.807428 7
- Catakoglu, O., Balduzzi, M., & Balzarotti, D. (2016, April). Automatic extraction of indicators of compromise for web applications. In *Proceedings of the 25th international conference on world wide web* (pp. 333-343). https://doi.org/10.1145/2872427.2883056
- Chaudhary, O., & Siddique, A. S. (2017). Cloud computing application: Its security issues and challenges faced during cloud forensics and investigation. *International Journal of Advanced Research in Computer Science*, 8(2). http://www.ijarcs.info/index.php/Ijarcs/articl e/view/2916
- CloudPassage. (2020). AWS Cloud Security Report.
- https://pages.cloudpassage.com/rs/857-FXQ-213/images/2020-AWS-Cloud_Security-Survey-Report.pdf

- CSA. (2017). *Cloud Controls Matrix*. https://cloudsecurityalliance.org/research/cc m/
- Edmondson, A. C., & McManus, S. E. (2007). Methodological fit in management field
- research. Academy of management review, 32(4), 1246-1264. https://doi.org/10.5465/amr.2007.2658608 6
- Farokhi, F., Shames, I., & Batterham, N. (2017). Secure and private control using semihomomorphic encryption. *Control Engineering Practice*, 67, 13-20. https://doi.org/10.1016/j.conengprac.2017. 07.004
- Gaidhani, D., Koyeerath, J., Kudu, N., & Mehra, M. (2017). A survey report on techniques for data confidentiality in cloud computing using homomorphic encryption. *International Journal of Advanced Research in Computer Science, 8*(8). https://doi.org/10.26483/ijarcs.v8i8.4746
- Geng, Y. (2019). Homomorphic encryption technology for cloud computing. *Procedia Computer Science*, *154*, 73-83. https://doi.org/10.1016/j.procs.2019.06.01 2
- ISC2. (2020). 2020 Cloud Security Report. https://www.isc2.org/resourcecenter/reports/2020-cloud-security-report

Jeganathan, S. (2018). Practical approaches to overcome security challenges in cloud Computing. *ISSA Journal*, *16*(12), 30–41.

- Kacha, L., & Zitouni, A. (2017, September). An overview on data security in cloud computing. In Proceedings of the Computational Methods in Systems and Software (pp. 250-261). Springer, Cham. https://doi.org/10.1007/978-3-319-67618-0_23
- Khan, H., Ahamad, M. V., & Samad, A. (2017). Security challenges and threats in cloud computing systems. *International Journal of Advanced Research in Computer Science*, *8*(2).
- Khan, M. A. (2016). A survey of security issues for cloud computing. *Journal of Network* and Computer Applications, 71, 11-29. https://doi.org/10.1016/j.jnca.2016.05.010

- Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1-48. https://doi.org/10.1016/j.cosrev.2019.05.0 02
- Kumar, S., Verma, R. S., & Mohan, K. (2017). Survey on data security issues in cloud computing. *International Journal of Advanced Research in Computer Science*, 8(3)
- Lapão, L. V., da Silva, M. M., & Gregório, J. (2017). Implementing an online pharmaceutical service using design science research. *BMC Medical Informatics and Decision Making*, *17*(1). https://doi.org/10.1186/s12911-017-0428-2
- Li, J., Kuang, X., Lin, S., Ma, X., & Tang, Y. (2020). Privacy Preservation for Machine Learning Training and Classification Based on Homomorphic Encryption Schemes. *Information Sciences*. https://doi.org/10.1016/j.ins.2020.03.041
- Lin, L., Liu, T., Hu, J., & Zhang, J. (2014, December). A privacy-aware cloud service selection method toward data lifecycle. In 2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS) (pp. 752-759). IEEE. https://doi.org/10.1109/PADSW.2014.7097 878
- Lo'ai, A. T., & Saldamli, G. (2019). Reconsidering big data security and privacy in cloud and mobile cloud systems. *Journal* of King Saud University-Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2019.05.0 07
- Matloob, G. (2017). A Survey on cloud computing security issues and its possible solutions. *International Journal of Advanced Research in Computer Science*, *8*(2).
- Mattoo, I. A. (2017). Security issues and challenges in cloud computing: A conceptual analysis
- and review. International Journal of Advanced Research in Computer Science, 8(2).

- Mazonka, O., Sarkar, E., Chielle, E., Tsoutsos, N. G., & Maniatakos, M. (2020). Practical datain-use protection using binary decision diagrams. *IEEE Access*, *8*, 23847-23862. https://doi.org/10.1109/ACCESS.2020.297 0120
- Miyan, M. (2017). FHE implementation of data in cloud computing. *International Journal of Advanced Research in Computer Science*, 8(3).
- Nasreldin, M. M., El-Hennawy, M., Aslan, H. K., & El-Hennawy, A. (2015). Digital forensics evidence acquisition and chain of custody in cloud computing. *International Journal of Computer Science Issues (IJCSI)*, 12(1), 153-160.
- Palmer, G. (2001). *A roadmap for digital forensics research*. Report for the First Digital Forensics Research Workshop (DFRWS), DTR-T0010-01, DFRWSDTR-T0010-01.
- Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302
- Rocha, F., Gross, T., & Van Moorsel, A. (2013). Defense-in-depth against malicious insiders in the cloud. In 2013 IEEE International Conference on Cloud Engineering (IC2E) (pp. 88-97). IEEE. https://doi.org/10.1109/IC2E.2013.20
- Serketzis, N., Katos, V., Ilioudis, C., Baltatzis, D., & Pangalos, G. J. (2019). Actionable threat intelligence for digital forensics readiness. *Information and Computer Security*, 27(2), 273-291. https://doi.org/10.1108/ICS-09-2018-0110
- Shashidhar, N. K., & Novak, D. (2015). Digital forensic analysis on prefetch files. *International Journal of Information Security Science*, 4(2), 39-49.
- Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, 88-115. https://doi.org/10.1016/j.jnca.2016.11.027
- Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing.

Computers & Electrical Engineering, 71, 28-42. https://doi.org/10.1016/j.compeleceng.201 8.06.006

- Sun, P. J. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, 102642. https://doi.org/10.1016/j.jnca.2020.10264 2
- Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, https://doi.org/10.1155/2014/190903
- Tak, V., Kachhwaha, R., & Mahia, R. N. (2018). Secure log forensics as a service in cloud computing. *International Journal of Advanced Research in Computer Science*, 9(1). http://doi.org/10.26483/ijarcs.v9i1.5373
- Tavana, M. K., Fei, Y., & Kaeli, D. R. (2017). Nacre: Durable, secure and energy-efficient non-volatile memory utilizing data versioning. *IEEE Transactions on Emerging Topics in Computing*. http://doi.org/10.1109/TETC.2017.278762 2
- Thantilage, R., & Jeyamohan, N. (2017, September). A volatile memory analysis tool for retrieval of social media evidence in windows 10 OS based workstations. In 2017 National Information Technology Conference (NITC) (pp. 86-88). IEEE. https://doi.org/10.1109/NITC.2017.828566 4
- Tran, J., Farokhi, F., Cantoni, M., & Shames, I. (2020). Implementing homomorphic encryption based secure feedback control. *Control Engineering Practice*, *97*, 104350. https://doi.org/10.1016/j.conengprac.2020 .104350
- Ullah, S., Li, X. Y., Hussain, M. T., & Lan, Z. (2019). Kernel homomorphic encryption protocol. *Journal of Information Security and Applications*, *48*, 102366. https://doi.org/10.1016/j.jisa.2019.102366
- Vumo, A. P., Spillner, J., & Köpsell, S. (2019, July). A Data security framework for cloud computing adoption: Mozambican

government cloud computing. In *European Conference on Cyber Warfare and Security* (pp. 720-XX). Academic Conferences International Limited.

Xiong, L., & Dong, D. (2019). Reversible data hiding in encrypted images with somewhat

homomorphic encryption based on sorting block-level prediction-error expansion. *Journal of Information Security and Applications*, 47, 78-85. https://doi.org/10.1016/j.jisa.2019.04.005