Cybersecurity Threat Modelling: A Case Study of An Ecommerce Platform Migration to the Public Cloud

Bamidele Ola and Iyobor Egho-Promise

Abstract **— The emergence of ecommerce almost three decades ago has completely transformed the approach to purchasing goods and services across various countries in the world. Almost every country in the globe, now have some form of ecommerce operations, this has further been enhanced by the stay at home COVID-19 induced lockdowns. The value and volume of transactions has also increased in transactions. However, there has been security concerns impacting ecommerce operations, which has in part, led to increasing adoption of hosting ecommerce systems in the public cloud. Threat modelling offer mechanisms to enhance the security of information technology (IT) systems. In this paper, we apply different threat modelling techniques to decompose the migration of an on-premise hosted ecommerce system to the public cloud and also evaluate these threat modelling techniques.**

Index Terms **— cloud; cybersecurity; ecommerce; threat modelling.**

I. Introduction

The advent of Information Technology (IT) has altered the way individuals and organizations accomplish various tasks such as buying goods and services, referred to as ecommerce [20]. Ecommerce entails buying goods and service over the internet, and typically involve, customers searching for items to buy, adding items to shopping cart or basket, checking out the items, and making payments; thereafter the seller confirms the order and ship items to their customers [10]. In the late nineties and early part of this century, most of the IT infrastructure involved in ecommerce were hosted on-premise, the emergence of public cloud computing is changing the hosting arrangement. Cloud computing provides much more flexibility, lower ongoing costs, enhances scalability and elasticity, improves agility, and faster time-to-market [7], however, there are concerns about maintaining security and compliance in public cloud environments such as but not limited to unauthorized access to cloud instances, account hijacking, shared technology vulnerabilities, denial of service, user credentials compromise, data corruption and compromise, and compromise of Application Programming Interfaces (APIs) keys [5], [11].

This paper addresses these research questions: (i) which threat modelling techniques can be applied to decompose ecommerce system migration to the public cloud? (ii) which functionalities are requisite for a threat modelling technique to adequately decompose the secure migration of ecommerce systems to the public cloud? and (iii) how can we compare the relative strengths and weaknesses of these threat modelling techniques available to decomposing the secure migration of ecommerce systems to the public cloud?

This paper presents the considerations of migrating an ecommerce system from on-premise infrastructure to the public cloud, a secure implementation plan for the migration, and threat models for this scenario using three threat modelling approaches (i) Architecture, Threats, Attack Surfaces, and Mitigation (ATASM) threat modelling methodology [17], (ii) Open Web Application Security Project (OWASP) threat modelling methodology [14], and (iii) Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges (STRIDE) threat modelling framework [18] and lastly we evaluate these three techniques using the evaluation framework in [2].

II. Literature Review

A. Migration to Cloud Considerations

Typical IT and architectural components that make up an ecommerce system, according to Schoenfield [17], include web servers, web applications, application servers, databases, network components such as firewalls and load balancers. These ecommerce components are historically hosted on-premise, however, with the ever-increasing adoption of public cloud services like Amazon web services (AWS®) and Microsoft Azure®, ecommerce providers have options to migrate their ecommerce solution to the cloud using various cloud migration approaches. These migration approaches according to [13], include: rehosting (migrating current applications and dependencies to the cloud as-is to the cloud provider compute infrastructure platform), refactoring (migrating applications but using existing cloud managed services such as containers and relational database systems) and rebuild (redesigning entire ecommerce system and dependencies to work with cloud native applications).

The rehosting migration option forms the basis of the discussion in this paper and assumes public cloud hosting in AWS or Azure.

B. Threat Modelling Techniques

Threat modelling is a practice of viewing or decomposing an application through the perspective of a malicious user or an attacker, to determine if the application is can resist malformed or hostile inputs [18]. This section briefly describes the three threat modelling techniques.

ATASM: The Architecture, Threats, Attack Surfaces, and Mitigation (ATASM) threat modelling methodology [17] otherwise referred to as ATASM is an emerging technique for modelling threats from a security architect's perspective.

Published on August 31, 2020.
Bamidele Ola, University of the Cumberlands, KY, USA.
(corresponding e-mail: olawest@technobeacon.com)
Iyobor Egho-Promise, Glo Mobile Limited, Ghana.
(e-mail: eghopromise@yahoo.com)

According to [17], ATASM [17] consists of four high-level security architecture activities which include: the architectural decomposition of system components and interconnections, identifying possible threats for the system and attack methods for every feasible threat agents, cross-referencing attack methods for threats against system inputs resulting in a list of credible attack surfaces, and enumerating security controls to mitigate the threat agents and threats to credible attack surfaces. We chose ATASM [17] as a candidate technique because its roots are in modelling security architecture activities. More importantly, it is inherently threats and attacks focused and can easily reveal potential threats, threat agents, and attacks that can result in security incident or data breach in an ecommerce system.

OWASP Threat Modelling: The OWASP threat modelling technique [14] leverages the 2017 OWASP Top 10 vulnerabilities [15]. It primarily entails identifying tangible assets and their capabilities, identifying various threat agents and their potential attacks, listing existing controls, identifying vulnerabilities that are exploitable, prioritizing identified risks by determining their likelihood and impact, and lastly identifying controls to reduce the risk to acceptable levels. Our choice of selecting OWASP threat modelling technique is because ecommerce solutions are inherently and natively web applications hence the need to apply it this paper to decompose the ecommerce migration to the public cloud.

STRIDE: The STRIDE threat modelling technique [18] is a developer focussed threat modelling technique with the objective of supporting an application system to satisfy the security principles of integrity, availability, confidentiality, authentication, authorization, and non-repudiation [18]. STRIDE [18] enables subject matter experts to decompose and model application systems against the six STRIDE [18] threat model components. We selected STRIDE [18] as a candidate threat modelling technique for the scenario in this paper, because of its widespread popularity and usage, versatility in threat modelling various IT systems and applications, and extensive support and documentation.

C. Related Work

There have been various research efforts in the topic areas of this paper ecommerce, threat modelling, cloud security and cloud risk assessments.

With reference to threat modelling [2] carried out a review of some threat modelling techniques applicable to securing cloud computing, presented their own threat modelling technique, and an evaluation framework to compare cloud computing threat modelling techniques, while [20] carried out a comprehensive review and comparative analysis of 26 threat modelling techniques available to modelling software systems using five criteria, and [22] carried out an in-depth review of fifty-four threat modelling research papers, categorised them into three clusters and conducted a comparative analysis using three criteria.#

With respect to ecommerce, [9] discussed various critical high-level design and low-level design issues at different stages in designing ecommerce systems, while [23] discussed some common security vulnerabilities in ecommerce reputation systems, and [10] conducted a qualitative analysis of some formal specification methods available to specifying ecommerce transactions.

With regards to cloud security, [5] enumerated and discussed twelve top cloud computing threats, [1] presented nine data security challenges affecting cloud computing and their solutions, [8] carried out a comprehensive literature review of seventeen categories of cloud security issues and six categories of proposed security models to address these issues, while [11] discussed security issues in inter-cloud migrations and proposed a new model to facilitate and ensure much more secure and efficient inter-cloud migrations.

With regards to cloud risk assessments, [6] addressed five key questions relating to cloud security risk management whilst reiterating eight distinguishing characteristics of cloud computing, [21] presented some ISO 27001 information security management system (ISMS) based risk assessment use cases for various cloud computing deployment models and the three common cloud computing service models, [7] presented a conceptual cloud attack and risk assessment taxonomy for assessing security risks and threats for cloud computing deployment models and cloud computing service models, [4] presented a new asset based quantitative cloud risk assessment methodology, which assesses for each asset, their vulnerabilities and threats and calculates the specific risks associated with each asset, while [12] presented a Bayesian network based security risk assessment methodology for assessing and prioritizing cloud computing security risks and used an existing scenario to illustrate their methodology.

III. Methodology And Analysis

A. Secure Implementation Plan

The proposed migration secure implementation plan encompasses three phases: pre-migration, migration, and post-migration phases. We shall discuss the various implementation activities in rehosting the migration of the ecommerce system along these lines: network security, data encryption at rest and transit, access control, monitoring and logging, compliance, and business continuity planning and disaster recovery [13].

During the pre-migration phase, we reviewed existing on-premise network security components and explore public cloud network security capabilities such as AWS virtual private cloud (VPC) and AWS network security groups (NSG) or Azure firewalls and ensuring their correct configuration to provide better security, as the public cloud presents wider attack surface. Secondly, we reviewed the data encryption capabilities from the cloud providers such as AWS server-side encryption, AWS key management service (KMS) or Azure storage service encryption, Azure disk encryption, Azure key vault to ensure adequate security and protection of data at rest, motion and transit. Thirdly, we reviewed the monitoring and logging capabilities from the potential cloud providers such as AWS CloudTrail, AWS CloudWatch, and AWS Guard Duty or Azure Sentinel, Azure Application Insights, and Azure Monitor to ensure potential anomalies and security incidents can be captured from events and logs from the various ecommerce system

components. Fourthly, we reviewed the access control capabilities from the potential cloud providers such as AWS Identity and Access Management (IAM) or Azure Active Directory to ensure there exist mechanisms to securely allow or deny access to ecommerce system components. Fifthly, we reviewed the compliance pages of AWS or Azure to ensure they comply with industry standards such as Payment Card Industry Data Security Standard [16] level 1 certification and the General Data Protection Regulation (GDPR) to ensure continuous secure processing of customer credit card payments and protection of customer personal information. Lastly, we reviewed the business continuity planning and disaster recovery offerings of the public cloud providers such as AWS Availability Zones, AWS Simple Storage Service (S3), AWS Route 53, and AWS Elastic Block Store (EBS) or Azure Site Recovery and Azure Storage to ensure ongoing timely recovery and continuity of business-critical ecommerce operations when incidents, failures and disasters occur.

The migration phase involves the implementation of the different security solutions, configurations, rules relating to network security, data encryption, monitoring and logging, access control, compliance, and business continuity planning and disaster recovery for the public cloud providers. The post-migration phase entails ongoing review, monitoring, and testing of the various security solutions, configurations, and rules. Table I captures the secure implementation plan for the ecommerce system migration to the public cloud in a tabular form.

TABLE I: SUMMARY SECURE IMPLEMENTATION PLAN FOR ECOMMERCE SYSTEM MIGRATION TO PUBLIC CLOUD

Summary secure implementation plan for ecommerce system migration to public cloud			
	Pre-migration	**Migration**	**Post-migration**
Network Security	Review network security capabilities.	Implement network security rules.	Continuously review network security by conducting penetration testing and red team assessments.
Data encryption	Review data encryption capabilities.	Implement data encryption security capabilities.	Continuously review and test the effectiveness of data encryption security capabilities.
Monitoring and logging	Review events and logs monitoring capabilities.	Implement events monitoring and logging capabilities.	Continuously review alerts and reports from events monitoring and logging solutions.
Access control	Review identity and access management mechanisms.	Implement access control permission mechanisms for users, groups and resources.	Continuously review access control permissions for users, groups and resources.
Compliance	Check the public cloud provider complies with industry standards such as PCI DSS level 1 certification and data protection such as GDPR.	Ensure settings are configured with most secure options, and hardened images are used.	Continuously review and track cloud provider's compliance to industry frameworks and security configurations.
Business continuity planning and disaster recovery (BCP & DR)	Review BCP & DR offerings of providers and chose appropriately based on recovery time objectives.	Implement BCP & DR capabilities.	Test and review BCP & DR capabilities at scheduled intervals.

B. Threat Modelling

This section presents threat models for rehosting the ecommerce system migration to the cloud using the ATASM [17], STRIDE [18], and OWASP threat modelling [14] techniques. We applied three different threat modelling techniques approaches to ensure overall completeness and robustness of the threat modelling exercise.

B.1 ATASM Threat Model

This section addresses presents a threat model and attack simulation of an ecommerce migration to public cloud platforms using the ATASM methodology [17]. Table II shows the ATASM threat model and attack simulation for the ecommerce system rehosting in the public cloud using three typical architectural components (network, web application, web server) in an ecommerce solution.

B.2 STRIDE Threat Model

This section presents a threat model and attack simulation of an ecommerce migration to public cloud platforms leveraging the STRIDE threat modelling technique [18]. STRIDE [18] is a popular threat modelling framework applicable to modelling threats and attacks to various systems ecommerce solutions. Table III below shows the STRIDE [18] threat model and attack simulation for ecommerce solution rehosting in public cloud.

B.3 OWASP Threat Model

This section presents a threat model and attack simulation of an ecommerce migration to public cloud platforms based on the 2017 OWASP Top 10 vulnerabilities [15] and leveraging the OWASP threat modelling [14] technique and the principles in AWS whitepaper [3].Table IVa below and its continuation (Table IVb) in page 7 both show the OWASP threat model and attack simulation for ecommerce solution rehosting in public cloud using the 2017 OWASP top 10 vulnerabilities [15] relevant to an ecommerce solution.

TABLE II: ATASM THREAT MODEL FOR ECOMMERCE SOLUTION REHOSTING IN PUBLIC CLOUD

ATASM threat model for ecommerce solution rehosting in public cloud				
Architecture Component	**Threat Agents**	**Threats**	**Attack Surface**	**Mitigating controls for ecommerce solution rehosting in public cloud**
Network	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers.	Denial of service attacks, IPv4 addresses spoofing attacks, IPv6 addresses spoofing attacks, address resolution protocol spoofing attacks, routing tables poisoning attacks, authentication bypass attacks, domain name system (DNS) spoofing attacks.	Network security groups, firewalls, load balancers, compute instances.	Implement distributed denial of service (DDOS) mitigation solutions such as AWS Shield or Azure DDOS protection service. Implement packet filtering and IP whitelisting using AWS security groups/virtual private cloud or Azure firewall. Implement network and application performance monitoring metrics for possible denial of service scenarios.
Ecommerce web application	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers, malicious insiders.	SQL injection attacks, cross site scripting attacks.	Web client, user web sessions, login page, shopping cart, APIs.	Implement web application firewall (WAF) rules on AWS WAF or Azure WAF to mitigate matching SQL injection attacks and mitigate matching cross site scripting attacks. Perform server-side code level input validation and apply parametrized queries. Enforce code level XSS escaping and HML encoding.
Web server	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers, malicious insiders.	Directory traversal attacks, remote file inclusion attacks, local file inclusion attacks.	Web server directories, files, configurations.	Enforce rate limiting on APIs and controller access, turn off web server path listing, log failed logins, implement implicit deny on permissions to non-public resources.

TABLE III: STRIDE THREAT MODEL FOR ECOMMERCE SOLUTION REHOSTING IN PUBLIC CLOUD

STRIDE Threat Model for ecommerce solution rehosting in public cloud.				
STRIDE Component	**Threat Agents**	**Threats**	**Attack Surface**	**Mitigating controls for ecommerce solution rehosting in public cloud**
Spoofing	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers, malicious insiders.	IPv4 and IPv6 spoofing attacks, authentication bypass attacks, domain name system spoofing attacks, iptables and routing tables manipulation attacks, address resolution protocol spoofing attacks.	Network layer, wide area network.	Implement packet filtering, IP whitelisting, geo-blocking. Enforce end to end and strict HTTPS connection using TLS 1.2 and strong ciphers on AWS or Azure.
Tampering	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers, malicious insiders.	Web parameter attacks, SQL injection attacks, cross site scripting attacks, path traversal attacks -in-the-middle attacks.	Product catalog, app database.	Implement web application firewall, perform code level input validation, use parametrised queries. Verify and validate SSL/TLS certificates with AWS Certificate Manager or Azure App Service certificates. Enforce database level and application level encryption, hashing, and anonymization.
Repudiation	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers, malicious insiders.	log truncation and erasure, tracks covering, log tampering.	Web application, web server.	Enforce logging and monitoring with AWS CloudWatch and CloudTrail or Azure Monitor and Application Insights. Enforce integrity checking mechanisms such as digital signatures and time stamps on logs.
Information Disclosure	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers, malicious insiders.	Banner grabbing attacks, source code disclosure attacks, file path and name disclosure attacks, bucket information disclosure attacks, directory listing attacks.	Web server, web application,	Enforce adequate access controls and authorizations, turn off information disclosure settings, robust exception and error handling and avoid hard coding sensitive data. Encrypt transactional personal and financial data at rest and in transit using AWS server-side encryption with key management service (KMS) or Azure storage service encryption with key vault.
Denial of Service	Cyber security researchers, cyber criminals, hacktivists, state sponsored attackers, malicious insiders.	Zero-day DDOS attacks, HTTP flooding attacks, ping of death attacks, volume-based attacks, SYN flooding attacks.	Network, web server, application load balancer, network load balancer, web application firewall.	Implement distributed denial of service (DDOS) solution such as AWS Shield or Azure DDOS protection service. Implement network and application performance monitoring metrics for possible denial of service scenarios.
Elevation of Privileges	Cyber security researchers, cyber criminals, hacktivists, state sponsored attackers, malicious insiders.	Vertical privilege elevation attacks, horizontal elevation attacks, lateral movement attacks.	Web application, web server, database.	Implement privilege access management (PAM) solution such as Azure Active Directory PAM or AWS Identity and Access Management (IAM) permissions, roles, and groups.

TABLE IVA: OWASP THREAT MODEL FOR ECOMMERCE SOLUTION REHOSTING IN PUBLIC CLOUD

OWASP threat model for ecommerce solution rehosting in public cloud				
OWASP 2017 Top 10 Component	**Threat Agents**	**Threats**	**Attack Surface**	**Mitigating controls for ecommerce solution rehosting in public cloud**
A1 – SQL Injection	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers, malicious insiders.	Blind SQL injection attacks, input validation attacks, NoSQL injection attacks, hostile data attack.	Web application, user database, product catalog.	Implement web application firewall (WAF) rules on AWS WAF or Azure WAF to mitigate matching SQL injection attacks. Perform server-side code level input validation and apply parametrized queries.
A2 - Broken Authentication and Session Management	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers, malicious insiders.	Session management attacks, credential stuffing attacks, automated brute force attacks, dictionary attacks, password spraying attacks.	Web client, user web sessions, login page, shopping cart.	Implement multi factor authentication (MFA) using Azure Active Directory or AWS Identity and Access Management (IAM) permissions, roles, and groups. Disable default credentials, enforce strict session timeouts, restrict failed login attempts, log and alert admin login failures and a use a secure server-side session manager that can generate unique session IDs.
A3 - Sensitive Data Exposure	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers, malicious insiders.	Password database attacks, personal identifiable information (PII) theft attacks, cardholder credit/debit number theft attacks.	Web application, app database.	Encrypt sensitive credit card/debit card holder's information and personal data at rest and in transit with AWS server-side encryption or AWS key management service (KMS) or Azure storage service encryption or Azure key vault. Always use strong and yet to be deprecated cryptographic algorithms, protocols, and associated keys. Store passwords with hashing functions with salting or peppering. Enforce end to end and strict HTTPS connection using at least TLS 1.2 and strong ciphers on AWS or Azure.
A4 – XML External Entities (XXE)	Cyber security researchers, cyber criminals, script kiddies, hacktivists, state sponsored attackers.	XML uploads attacks, XML documents attacks, denial of service attacks	Web services, web application.	Use simpler data formats like JSON, ensure XML processors and libraries are running latest secure and stable versions. Implement XML input validation, XML data filtering and XML data sanitization on server-side.
A5 – Broken Access Control	Cyber security researchers, cyber criminals, hacktivists, state sponsored attackers, malicious insiders.	Unauthorized API access attacks, metadata manipulation attacks, privilege escalation attacks, directory listing attacks, remote file inclusion attacks, local file inclusion attacks.	Network, web server, web applications, APIs.	Enforce rate limiting on APIs and controller access, turn off web server path listing, log failed logins, implement implicit deny on permissions to non-public resources. Implement web application firewall (WAF) rules on AWS WAF or Azure WAF to block malicious HTTP requests that can indicate directory traversal attacks and file inclusion attacks.

TABLE IVB (CONTINUATION): OWASP THREAT MODEL FOR ECOMMERCE SOLUTION REHOSTING IN PUBLIC CLOUD

OWASP threat model for ecommerce solution rehosting in public cloud				
OWASP 2017 Top 10 Component	**Threat Agents**	**Threats**	**Attack Surface**	**Mitigating controls for ecommerce solution rehosting in public cloud**
A6 – Security Misconfiguration	Cyber security researchers, cyber criminals, hacktivists, state sponsored attackers, malicious insiders.	Security misconfigurations attacks, default settings attacks, default credentials attacks.	Web server, web application, network, load balancers, database.	Implement secure hardening configurations using AWS hardened machine images or Azure hardened machine images. Disable unrequired services, features and frameworks, regularly review cloud storage permissions on AWS S3 buckets or Azure blob storage.
A7 – Cross Site Scripting (XSS)	Cyber security researchers, cyber criminals, hacktivists, state sponsored attackers, malicious insiders.	Reflected XSS attacks, stored XSS attacks, document object model (DOM) XSS attacks, web page hijack and defacement attacks.	Web application, app database, product catalog.	Implement web application firewall (WAF) rules on AWS WAF or Azure WAF to mitigate matching cross site scripting attacks. Enforce code level XSS escaping and HML encoding, and apply parametrized queries.
A8 – Insecure Deserialization	Cyber security researchers, cyber criminals, hacktivists, state sponsored attackers, malicious insiders.	Data structure attacks, object attacks, data tampering attacks.	Web applications, APIs.	Implement data integrity checks like digital signatures on serialized data structures and objects, isolate and execute code that deserializes in low privilege scenarios, log failed deserialization attempts. Restrict inbound and outbound network connections from deserializing containers such as AWS Elastic Kubernetes Service (EKS) or Azure Kubernetes Service (AKS).
A9 – Using Components with Known Vulnerabilities	Cyber security researchers, cyber criminals, hacktivists, state sponsored attackers, malicious insiders.	Unsupported software and components attacks, vulnerable APIs attacks, out-of-date content management systems (CMS).	Web applications, APIs, app database, web server.	Use the most up to date, secure and stable versions of ecommerce date content management systems (CMS) such as Magento, Volusion, and Shopify. Use components, libraries and APIs from official websites and packages with digital signatures, uninstall unrequired dependencies, services, features, libraries, components, and files.
A10 – Insufficient Logging and Monitoring	Cyber security researchers, cyber criminals, hacktivists, state sponsored attackers.	Unmonitored logs, inadequate and unclear log messages, inadequate alerting thresholds, audit trail not turned on, application without logging capability.	Web applications, APIs, app database, web server.	Enforce logging and monitoring with AWS CloudWatch and CloudTrail or Azure Monitor and Application Insights. Monitor and log successful and failed logins, failed access control mechanisms, and failed server-side input validation, ensure logs are generated in Security Information and Events Management (SIEM) compatible formats.

B.4 Evaluation of Threat Modelling Techniques

This section shows the results of our qualitative evaluation of the three threat modelling techniques used to model the ecommerce system leveraging our experience in applying these techniques to the work in this paper and prior corporate experience using the threat modelling evaluation criteria in [2]. Table V below shows the outcome of our evaluation of the three techniques using the evaluation framework and criteria in [2].

TABLE V: QUALITATIVE EVALUATION OF 3 THREAT MODELLING TECHNIQUES

Characteristics of threat modelling approach	Threat modelling approaches		
	ATASM	OWASP	STRIDE
Identifying and classifying assets	x	X	x
Establish user's role			
Identifying security domains	x		
Estimating trustworthiness			
Scanning domain security			
Identifying threats	x	X	x
Identifying vulnerability	x	X	x
Implementing countermeasures	x	X	x
Ranking and measuring threats	x	X	x
Ranking and measuring vulnerabilities	x	X	x
Defining new assets, threats or vulnerabilities	x		x

IV. CONCLUSION

This paper presents a brief overview of ecommerce, security considerations of migrating ecommerce platforms from on-premise to the public cloud using the rehosting cloud migration option, a secure implementation plan for the migration, and develop threat models of the migration using ATASM, OWASP, and STRIDE modelling techniques and a thereafter provide qualitative evaluation of these three approaches.

In the future, we hope to apply some further threat modelling techniques to other cloud computing use cases and scenarios, apply a quantitative evaluation framework, and develop a threat modelling technique to specifically model cloud computing use cases.

REFERENCES

[1] I. Ahmed, "A brief review: security issues in cloud computing and their solutions," Telecommunication, Computing, Electronics and Control (Telkomnika), 17(6), pp. 2812-2817, 2019. https://doi.org/10.12928/telkomnika.v17i6.12490.

[2] A. Amini, N. Jamil, A. R. Ahmad, & M.R. Z`aba, "Threat Modeling Approaches for Securing Cloud Computing," Journal of Applied Sciences, 15: 953-967, 2015. https://doi.org/10.3923/jas.2015.953.967.

[3] awsstatic.com. (2017). Using AWS Web Application Firewall (WAF) to mitigate OWASP Top 10 vulnerabilities. Retrieved from https://d0.awsstatic.com/whitepapers/Security/aws-waf-owasp.pdf.
[4] S. Basu, A. Sengupta, & C. Mazumdar, "A Quantitative Methodology for Cloud Security Risk Assessment", In Proceedings of the 7th International Conference on Cloud Computing and Services Science, pages 120-131, 2017. https://doi.org/10.5220/0006294401200131.
[5] cloudsecurityalliance.org. (2018). CSA – The Dirty Dozen: 12 top cloud security threats. Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf.
[6] cloudsecurityalliance.org. (2020). CSA's Perspective on Cloud Risk Management. Retrieved from https://cloudsecurityalliance.org/research/artifacts/.
[7] K.R. Choo & N.V. Juliadotter, "Cloud Attack and Risk Assessment Taxonomy," IEEE Cloud Computing, 2(1), 14-20, 2015. https://doi.org/10.1109/MCC.2015.2.
[8] R. Doshi, & V. Kute, "A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models," International Conference on Emerging Trends in Information Technology and Engineering, pp. 1-4, 2020. https://doi.org/10.1109/ic-ETITE47903.2020.37.
[9] S.A. Ehikioya & E. Guillemot, "A critical assessment of the design issues in e-commerce systems development," Engineering Reports, 2(4), e12154, 2020. https://doi.org/10.1002/eng2.12155.
[10] S. A. Ehikioya & B. Ola, "A Comparative Study of Specification Methods for Electronic Commerce Systems," 3rd ACS/IEEE International Conference on Computer Systems and Applications, 108-110, 2005. https://doi.org/10.1109/AICCSA.2005.1387097.
[11] I. Khalil, I. Hababeh & A. Khreishah, "Secure inter-cloud data migration," 7th International Conference on Information and Communication Systems, 62-67, 2016. https://doi.org/10.1109/IACS.2016.7476087.
[12] I. M. A. Khogali, & P. H. Ammar, "A Scenario-Based Methodology for Cloud Computing Security Risk Assessment," International Journal of Innovation Education and Research, 5(12), 127-155, 2017. https://ijier.net/ijier/article/view/875.
[13] D. C. Marinescu, Cloud computing: theory and practice, Morgan Kaufmann, 2017.
[14] owasp.org. (n.d). OWASP Threat Modeling. Retrieved from https://owasp.org/www-community/Threat_Modeling.
[15] owasp.org. (2017). Open Web Application Security Project (OWASP) Top 10 2017. Retrieved from https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/.
[16] pcisecuritystandards.org. (2019). Payment Card Industry Data Security Standard (PCI-DSS). Retrieved from https://www.pcisecuritystandards.org/.
[17] B.S.E. Schoenfield, Securing Systems: Applied Security Architecture and Threat Models. CRC Press, 2015.
[18] A. Shostack, Threat Modeling: Designing for Security. Wiley, 2014.
[19] K. Tuma, G. Çalikli, & R. Scandariato, "Threat analysis of software systems: A systematic literature review," Journal of Systems and Software, 144, 275-294, 2018. https://doi.org/10.1016/j.jss.2018.06.073.
[20] J. Warsinske, M. Graff, K. Henry, C. Hoover, B. Malisow, S. Murphy, C.P. Oakes, G. Pajari, J. T. Parker, D. Seidl, & M. Vasquez, The Official (ISC)2 Guide to the CISSP CBK Reference, 5th edition, Wiley, 2019.
[21] T. Weil, "Risk Assessment Methods for Cloud Computing Platforms, IEEE 43rd Annual Computer Software and Applications Conference," Milwaukee, WI, USA, pp. 545-547, 2019. https://doi.org/10.1109/COMPSAC.2019.00083.
[22] W. Xiong, & R. Lagerström, "Threat modeling – A systematic literature review," Computers & security, 2019. https://doi.org/10.1016/j.cose.2019.03.010.
[23] Y. Yao, S. Ruohomaa, & F. Xu, "Addressing common vulnerabilities of reputation systems for electronic commerce," Journal of theoretical and applied electronic commerce research, 7(1), 1-20, 2012. Retrieved from https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-18762012000100002.