INFORMATION SECURITY CONSIDERATIONS FOR CLOUD-BASED ENTERPRISE RESOURCE PLANNING SYSTEM AND BEST PRACTICES FOR ITS RETIREMENT PHASE

Co-authored by Padmini Gottipati

Bobby Swar

Pavol Zavarsky

Project report

Submitted to the Faculty of Graduate Studies,

Concordia University of Edmonton

in Partial Fulfillment of the

Requirements for the

Final Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

April 2020

INFORMATION SECURITY CONSIDERATIONS FOR CLOUD-BASED ENTERPRISE RESOURCE PLANNING SYSTEM AND BEST PRACTICES FOR ITS RETIREMENT PHASE

Padmini Gottipati

Approved:

Bobby Swar [Original Approval on File]

Bobby Swar　　　　　　　　　　Date: April 20, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci　　　　　　　　　　Date: April 20, 2020

Dean, Faculty of Graduate Studies

Information Security Considerations for Cloud-based Enterprise Resource Planning System and Best Practices for its Retirement phase

Padmini Gottipati
Information System Security Management
Concordia University of Edmonton
Edmonton AB, Canada
paddu0908@gmail.com

Bobby Swar
Information System Security Management
Concordia University of Edmonton
Edmonton AB, Canada
bobby.swar@concordia.ab.ca

Pavol Zavarsky
Information System Security Management
Concordia University of Edmonton
Edmonton AB, Canada
pavol.zavarsky@concordia.ab.ca

Abstract—**Enterprise Resource Planning (ERP) system is an integrated solution that has been revolutionizing the business processes in a collective and distributed way. These systems are designed to fasten communication between various departments within an organization and empower its employees in making better business decisions with the help of data, improve reporting and planning which increases total visibility. It also improves the efficiency, quality and customer service. There is an increase in the cloud ERP software adoption by small businesses keeping up with the competition, also cloud ERP systems are cost-effective solutions for small enterprises. In this age of ERP systems on the cloud, organizations are skeptical in terms of ERP adoption on cloud due to security-related issues and malicious intentions from both inside and outside the organization. To address the security-related issues in ERP, this paper identifies various attacks an ERP system is prone to using literature review, identifies what security controls are to be in place considering NIST 800-53 R5 and ISO/IEC 27001:2013 to create a more secure environment and also mapped the identified security controls to facilitate PIPEDA compliance of Canada along with the best practices to be followed to clear/purge/destroy the various media types used considering NIST SP 800-88 in the retirement phase of ERP systems.**

***Keywords**—Enterprise Resource Planning, Retirement phase, attacks, PIPEDA, cloud ERP, ERP Security.*

I. INTRODUCTION

Enterprise Resource Planning (ERP) systems are the software applications that integrate company data and support organizational functions or departments like accounting, marketing, manufacturing, finance, human resource, supply chain, etc. [1]. The central database is the core of ERP architecture. It collects data from and feeds data into various applications supporting virtually all the company's business activities. When new information is entered in one place, related information is automatically updated. ERP systems help the organization to gain competitive advantages by letting them to (a) View and track information/data regarding business processes across several departments, (b) Store data centrally in a common database, (c) Analyze the data in real-time for business intelligence, (d) Provide e-commerce integration and enhanced security of transactions [1]. As a result of this, efficiency would be increased by eliminating information search and duplication of information in different systems [2]. An additional advantage of the ERP system is that it will be in favor of customization. Customization of an ERP system is usually the process of fitting the chosen ERP between the system and the business processes of an organization. Customization options range from setting parameters in the system to developing new functionality by modifying source code [3].

There are two types of ERP systems: Traditional/On-premise ERP systems and Cloud-based ERP systems. There are several existing issues to traditional On-premise ERP implementation. The first thing would be the cost. Due to this factor, there is a rising trend of ERP vendors sourcing for alternative cloud-based computing. The migration to cloud-based ERP has been proven by many researchers that it overcomes the most issues faced by on-premise ERP such as improve mobility, improve scalability, high reliability. However, information security could be a considerable issue in cloud-based ERP.

There are several free and open-source ERP software like ERPNext, Odoo, MixERP, iDempiere, etc [4]. Some small and medium-sized enterprises (SME) which cannot afford very expensive and top ERPs like SAP, Oracle, Microsoft adopt these open source and less expensive ones. 'Industry Canada' defines a small business as one with fewer than 100 paid employees and a medium-sized business as one with at least 100 and fewer than 500 employees [5]. Examples of few SMEs using less expensive/open ERP software are Abitare Kids with around 50 employees, 1000 Miles ltd. with around 200 employees and Advanced Biological Laboratories (ABL) with around 50 employees use Oddo ERP software.

With the growing number of data breaches and attacks on industries like manufacturing, hospitality, healthcare and education which uses ERP software, hackers are increasingly looking out to target ERP systems to disrupt and steal data from the companies. Just the traditional controls of ERP application security are ineffective to prevent or detect the observed TTP

(Tactics, Techniques, Procedures) used by attackers. Hence there is an enormous need for security controls to respond to evolving security threats and to protect confidentiality, integrity, and availability of data when many organizations are adopting cloud-based ERP systems. Also, there are six phases in the ERP lifecycle and very minimal importance has been given to the Retirement phase. The substitution of the selected ERP system will become necessary in the retirement stage when innovations show up or the ERP system gets deficient in the business prerequisites. Any organization needs to follow proper data sanitization methods to ensure security.

This research studied the security controls from NIST 800-53 R5 and ISO/IEC 27001:2013 which are to be in place to safeguard the ERP system from possible attacks that it might be prone to and also mapped the identified security controls to facilitate PIPEDA compliance of Canada along with the best practices that are to be followed for clear/purge/destroy the media types in the Retirement phase of an ERP system.

II. Review of Related Work

A. ERP Information Security related considerations

Authors in [6] presented that Compliance, Network, and Security are the concerns that are under the control of a cloud vendor and the factors that have an impact on the successful implementation of cloud ERP. The paper [6] discusses user involvement, selection of vendor, project team, top management support, training of user and trust on the vendor. The compliance issues like cloud-based data archiving, cloud-based segregation of duties and global compliance standards and regulations; security issues like confidentiality of data, encryption, accountability, and maintenance are introduced in [6]. The model proposed in [6] is vague and did not specifically mention how each attribute can be achieved for attaining success in the implementation of the ERP system. The network and security concerns and the solutions provided in the name of success factors are generalized [6]. Whereas a survey on security issues in cloud computing has been discussed in paper [7] where authors elaborated and analyzed the numerous unresolved issues threatening the cloud computing adoption and diffusion affecting various stakeholders linked to it. The paper [7] elaborated on the barrier to cloud computing like Privacy and Security; Performance, Latency & Reliability; Portability and Interoperability; data breach through fiber-optic networks and data storage over IP networks. Authors classified various security threats to cloud computing as Basic Security, Network level security and Application level security. However, this paper did not discuss the security controls that are to be in place to create a more secure environment with minimum threats.

Authors in [8] and [9] mainly focussed on the security challenges and possible advantages of ERP delivered as cloud services from the user perspective and security issues and concerns for an organization by moving ERP systems to cloud. The current security issues of conventional ERP and the cloud computing technologies were evaluated like Data security, authentication and authorization, system architecture, threats, implementation of the ERP, network and web application security, compliance, and system reliability [8]. In the paper [8], it was concluded that the cloud ERP could bring a solution to mitigate some of the issues of the conventional ERP such as dealing with a complex ERP architecture, saving time and money during the implementation phase, enhancing data center security and control, which are provided by the cloud ERP vendor and significant security enhancements of network and the application security, which is provided by the cloud ERP provider [8]. The paper [9] discussed the emergence of Software-as-a-Service (Saas) ERP systems as an alternative approach to traditional ERP systems. It was emphasized that the data security issues are to be taken care of before moving the enterprise applications to the cloud. The specific concerns like confidentiality and integrity of data that is stored in the cloud were raised. A hybrid solution where the enterprises can choose to keep their confidential and sensitive applications on-premise and while experiencing the benefits of the cloud ERP has been proposed as an effective solution. Uncertainty around how the data is stored and lack of authority and control over the security controls and standards when their sensitive data is stored at external cloud service providers are stated as two main data security issues for confidentiality [9]. However, these papers did not cover how security can be implemented carefully into the system. [8] [9] just discussed a few threats and measures to mitigate them but did not provide a checklist of security policies and controls that are to be in place in order to safeguard the system from various threats and attacks.

Authors in paper [10] examined the services consulting the cloud architecture and deployment models and the main factors in the provision of security requirements of all those models as well as points to be taken into consideration are described in detail. Besides, the methods and tools considering how security, confidentiality, and integrity of the information or data that forms the basis of modern technology is implemented in cloud computing architecture are examined. Finally, the use of data hiding methods in terms of access security in cloud computing architecture and how the security of the stored data would be very effective in securing information has been proposed. However, the information security requirements in [10] document have significant limitations. Firstly, the paper [10] does not mention the solutions in order to achieve confidentiality, integrity, availability, and audit which was quoted in the abstract of the document. Also, the model proposed concentrated only on the data hiding model and how is it used for the security of stored data. The other option of safeguarding the data while storing it have not been concentrated upon.

B. Cloud-based ERP Security model

Authors in paper [11] presented a new framework for the ERP on Cloud. Based on this model, cloud security needs to be enforced at the Physical, Network, Data and Application level. Since social engineering is on the rise, while providing physical security, the cloud provider must define and enforce rules of conduct and social guidelines for employees. Network security should protect all virtual access points to the cloud by employing well-managed security rules and procedures to block attacks. Data security should ensure that both the data in storage as well as data in transit are protected from unauthorized third parties. Since most applications are built to be run in the context of an enterprise data center, the lack of physical control over the networking infrastructure might mandate the use of encryption in the communication between servers of an application that processes sensitive data to ensure its confidentiality. The paper [11] discusses how can physical security be attained by certain rules and guidelines; how to access security can be achieved through employing Firewall and Intrusion Detection System; how a data storage security can be attained by Encryption, Privacy, and Backup and how application software management can be achieved through identity management. In paper [12], authors identified and classified the benefits and drawbacks of cloud-based ERP systems versus traditional ERP systems. The paper [11] was first published in 2012 and reflects the state of knowledge almost 7 years ago. ERP system and cloud technology have evolved with next-generation cloud-based ERPs and multi-tenant cloud ERPs hence some of the proposed methodologies may be inadequate or no longer hold. Secondly, this paper does not talk in detail about how each module proposed would conclude the complete security of cloud ERP systems. This framework does not address the complete security issues faced by a cloud-based ERP system.

C. Enterprise Resource Planning system vendors

In paper [13], the authors presented an as-is ERP research model and the implementation life cycle will change with the social networks and cloud computing. Major ERP vendors will have their methodologies of implementation. For example, SAP follows Accelerated SAP (ASAP) methodology, Oracle ERP follows the Application Implementation Methodology (AIM) methodology and several other open-source ERP systems follow their methodologies. This paper provides a comprehensive list of critical success factors based on the literature review did not cover all the success factors for an ERP implementation.

According to the Onapsis report [14], SAP and Oracle are the two leading ERP vendors in the space and their systems are the most at risk. As per the Onapsis report, the top three most common attack vectors on SAP systems that threaten ERP security are:

1. A low-security customer Web portal;
2. Malicious accounts being used in customer or supplier portals; and
3. Vulnerabilities in the underlying database protocols.

All three of these issues contribute to the technical debt in securing an SAP system.

In the first vector, for example, a lower-security customer Web portal that is exposed to the Internet could be set up to allow customers to connect from anywhere to place orders. However, this customer Web portal can be used as part of an attack, with the attacker pivoting from the lower-security system to other more critical systems, and eventually the entire SAP system.

In the second attack vector, customer and supplier portals could potentially be infiltrated; backdoor users could pivot the SAP portals and other platforms to continue and attack the internal network.

In the third attack vector, an attacker can exploit insecure database protocol configurations that would allow them to execute commands on the operating system. At this point, the attacker has complete access to the operating system and can potentially modify or disrupt any information stored in the database.

Researchers stated there appears to be a disconnect between enterprise information security teams and SAP operations teams; the SAP vulnerabilities identified to support this assertion given the vulnerabilities are basic information security issues that have likely been addressed in other parts of an enterprise's information security program.

Given the critical nature of SAP systems, one major concern for ongoing security controls has been the potential for downtime from security. If an SAP system can't be "down" for business reasons, plans should be in place on how to apply patches or make other security changes without disrupting operations. This might include ensuring a high-availability system is in place, such as a backup system that automatically takes over when the primary system is being patched or is having changes made. There is an observation that 100% increase of public exploits for SAP and Oracle ERP applications over the last three years, and a 160% increase in the activity and interest in ERP-specific vulnerabilities from 2016 to 2017 [14].

A white paper [15] released by SAP ERP discusses the SAP's standards, processes and guidelines for Protecting Data and Information. It talks about general and physical security at SAP, SAP's security management framework – PDCA cycle, certain policies and controls, existing security standards at SAP and to make their working methods, guidelines, and processes more transparent for customers concerning security and data protection.

A white paper [16] released by Oracle ERP describes the security practices implemented according to Oracle's Corporate security program and adhered to by Oracle for its operational and services infrastructure under its control, including Oracle's corporate network and systems. It includes controls for Organizational security, Asset classification and control, Human Resources Security, Physical Security, Communications and Operations Management, Access Control, Incidence Response, Audit and Customer Data Retention. These two documents are the motivation behind this research paper. There are certain gaps in both the white papers as they did not touch base on all the security controls for complete security. The ones which are missing would be explained in this research. Also, this research states security controls that are specific to most common attacks that a cloud ERP system is prone to due to the vulnerabilities and attack vectors. The best practices which are to be followed in the retirement life cycle phase of an ERP system to maximize its security would also be proposed in this research.

D. Information security control standards, publications, and PIPEDA

NIST 800-53 revision 5 is a special publication responds to the need by leaving on a proactive and systemic way to develop and make available to a broad base of public and private sector organizations, a set of safeguarding measures for all types of computer platforms, including cyber-physical systems, cloud, and mobile systems, industrial/process control systems and Internet of Things (IoT) devices. Those safeguarding measures include security and privacy controls to protect the critical and essential operations and assets of organizations and the personal privacy of individuals. The ultimate objective is to make the information systems we depend on more penetration resistant to attacks; limit the damage from attacks when they occur and make the systems resilient and survivable [17].

ISO/IEC 27001 is a standard that covers all types of organizations (e.g. commercial enterprises, government agencies, non-profits), and all industries or markets (e.g. retail, banking, defense, healthcare, education, and government). The specific information risk and control requirements may differ in detail but there is a lot of common ground, for instance, most organizations need to address the information risks relating to their employees plus contractors, consultants and the external suppliers of information services [18].

PIPEDA [19] sets the ground rules for how private-sector organizations collect, use, and disclose personal information in the course of for-profit, commercial activities across Canada. It also applies to the personal information of employees of federally-regulated businesses such as banks, airlines, telecommunications companies. If the ERP system is adopted by any organization including the Human Resource sub-system has to adhere to PIPEDA as this subsystem mainly contains personal information of employees like age, marital status, employment history, financial information, Social Insurance Number, etc. PIPEDA and its 10 principles outline the responsibilities that organizations subject to Canadian legislation must follow. They come from a national standard called CSA model code for the protection of Personal Information.

NIST 800-88 [20] is published by the National Institute for Standards and Technology. It talks about the media sanitization categories of clear, purge and destroy. Its standards can apply to flash-based, magnetic and several other storage technologies. Media sanitization alludes to a procedure that renders access to target information on the media infeasible for a given degree of exertion. This guide will help organizations and system owners in making practical sanitization choices dependent on the order of privacy of their data.

In conclusion, it is clear from the literature review that the attack vectors or vulnerabilities which lead to cyber-attacks on ERP system are not discussed and the security policies and controls to minimize the risk of attacks are not yet explored. Most of the papers in the literature review did not concentrate on the best controls and policies side of it. Hence there is a wide gap in that area which is a motivation for this research paper. This research aims to study and determine the vulnerabilities which lead to cyber-attacks on Enterprise systems and what are the security controls that minimize the risk of each attack in detail combining the NIST 800-53 framework and ISO/IEC 27001 standards. Furthermore, this research paper recommends the best practices to be followed in the Retirement life cycle phase of the ERP system after reviewing SAP and Oracle security controls.

III. Methodology

This section describes the methodology followed for this research in below steps:

- Identified the list of major security attacks a cloud-based ERP system is prone to through literature review and the vulnerabilities which lead to the attack and their possible threats.
- Based on the identified attacks on the cloud ERP system, appropriate security controls from NIST 800-53 R5 publication and ISO/IEC 27001:2013 standard are mapped in order to mitigate the identified attacks. Hence the best practices and controls from both the mentioned standards are considered and integrated into the research to gain additional security effectiveness for an ERP system.
- Based on the security controls identified, mapped them to the 10 principles of PIPEDA compliance of Canada to verify if the identified controls are compliant to any of the principles of PIPEDA in whichever industry (where personal information is collected, used or disclosed) it applies to.
- Reviewed and identified the security practices and controls that are currently recommended by SAP and Oracle ERP software vendors and consolidated them.
- Finally, the best practices to clear/purge/destroy the various media types used in the ERP system is proposed for the retirement phase such that it minimizes the risk of cyber-attacks and maximizes the security effectiveness in the Enterprise system even after its retirement/disposal.

IV. Results

The identified security attacks for a cloud-based ERP system are listed below in Table I with their vulnerabilities and threats that could occur with a description of the attacks. After conducting the literature review, the following attacks are the most common attacks that a cloud-based ERP system is usually prone to.

The threat mentioned in the below table is an occasion or condition that has the potential for causing asset loss and the undesirable outcomes or impact from such loss. The basis of asset loss constitutes all forms of intentional, inadvertent, unintentional, accidental, abuse, misuse, error, mistake, shortcoming, defect, fault, weakness and/or failure events and associated conditions.

TABLE I. ATTACKS-DESCRIPTION, ITS VULNERABILITIES AND THREATS

S.No	Attacks – Description	Vulnerability	Threats
1.	SQL Injection Attack: In this attack, a malicious code will be inserted into a standard SQL code through which the attackers gain unauthorized access to a database and all its sensitive and confidential information [21].	Code (when programmers neglect to appropriately escape strings that are used in SQL queries) [22]	Software Threat – Unauthorized access [22]
2.	Cross-Site Scripting Attack: an attacker redirects the user to websites where attackers can steal the data from them. It has been observed quite often these days that some web-pages or pop-ups get opened with the request to click to view the content contained in them [23].	Web application/ Code (Java, CSS, ActiveX, Flash and VBS scripts)	Software Threat – Sniffing
3.	Man-in-the-middle attack: In this attack, an intruder tries to listen to an ongoing conversation between a sender and receiver and even can be able to change the information [24].	Host's ARP table / Spoofing DNS [25]	Network Threat – Spoofing
4.	DNS Spoofing: When a DNS server has received false information and caches it as usual for its performance optimization, it is considered as poisoning and it returns false data to the clients like false IP addresses and diverts the traffic to attacker's computer [26].	DSN Server / Open transmission of DNS traffic [27]	Unauthorized Modification [27]
5.	Sniffer Attack: This attack is occurred by the application that captures packets flowing in a network and when data is not in an encrypted format. There are chances that it can be read and important information traveling in the network can be captured. A sniffer program through the NIC (Network Interface Card) makes sure that the data linked to other systems on the network also gets recorded [28].	Border Gateway Protocol (BGP) [29]	Web-based mail issues, Denial of Service attacks, Authentication-based attacks [30]
6.	Brute Force attack: It is a trial and error method utilized by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through thorough exertion instead of utilizing intellectual methodologies [31].	Unexpired session tokens [32]	Software threat – Unauthorized access [32]
7.	Denial of Service attack & Distributed Denial of Service attack: The server providing the service is flooded by many requests and hence the service becomes inaccessible to the authorized user. In DDoS, the attack is relayed from different dynamic networks that have already been compromised, unlike DOS. The attackers can control the progression of data by permitting some data accessible at certain times [31].	Misconfigured network devices (Firewall, IDPS, etc.) [33]	Network threat – Essential communication failure [32]
8.	Hidden field manipulation: While accessing a site page, certain fields are covered up and contain the page related data and essentially utilized by developers. These fields are highly prone to hacker attacks as they can be modified easily and posted on the website page. This may bring about serious security infringement [7].	Unvalidated input [34]	Software threat – Spoofing
9.	Cookie Poisoning: It includes changing or adjusting the contents of the cookie to make unapproved access to an application or a website. Cookies contain the user's identity-related credentials and once these cookies are accessible, the contents of these cookies can be forged to impersonate an authorized user [35].	Cookie, Insecure channel [36]	Network threat – Spoofing
10.	Backdoor and Debug options: Regular propensity for the developers is to empower the troubleshoot/debug option while publishing a website. This empowers them to rollout any enhancements in the code and gets them actualized on the site. These unnoticed debug options enable easy entry to hacker into the website and let him make changes at the site level [7].	Code	Software Threat – Unauthorized access
11.	Ransomware attack: Ransomware is a sort of malware and attack that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid [37].	People/Employees	Personal/Administrative threat – Theft of Resources

Table II below lists the identified attacks mapped to relevant controls (specifically from NIST 800-53 R5 [17] and ISO/IEC 27001:2013 [18]) to be in place in order to minimize/safeguard from the effect of listed threats along with the description of the respective controls along with the relevant principle of PIPEDA [19] mapped to.

TABLE II. ATTACKS, CONTROLS WITH DESCRIPTION & PIPEDA

S.No	Attacks	Controls (NIST 800-53 R5)	Description (NIST 800-53 R5)	Controls (ISO/IEC 27001:2013)	Description (ISO/IEC 27001:2013)	PIPEDA principle
1.	SQL Injection attack	SI-15	Information Output Filtering: This control focusses on identifying superfluous content, keeping such unnecessary content from being shown and then alarming the monitoring devices that peculiar behavior has been found.	A.18.1.4*	Privacy and Protection of personally identifiable information: Privacy and security of personally recognizable data will be guaranteed as required in relevant regulation and legislation available.	Safeguards
		SI-10	Information Input Validation: This control focusses on checking the legitimate syntax and semantics of system inputs like character set,	-	-	Safeguards

			numerical range, length, etc. Pre-screening inputs prevent the content from being unintentionally deciphered as commands.			
		AC-23	Data mining protection: Limiting the types of responses provided to database queries; limiting the number and the frequency of database queries to increase the work factor needed to determine the contents of such databases and notifying organizational personnel when typical database queries or accesses occur [5].	A.18.1.3 A.18.1.4**	Records will be shielded from loss, devastation, misinterpretation, unauthorized access and unauthorized release under legislator, administrative, authoritative and business necessities.	Limiting collection
		SI-11	Error handling: Configure proper error reporting and handling on the webserver and in the code such that that database error messages are never sent to the client web browser [26]	-	-	
2.	Cross-site scripting	CM-3	Configuration Change Control: This control deals with automated documentation, notification, the prohibition of changes, testing, validation along with automated security response and cryptographic management where a process is implemented to address the expiration of the certificates used for identification and authentication.	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4	Operating procedures and principles for engineering secure systems will be documented and made available to all users who need them. When operating platforms are changed, business-critical applications will be investigated and tried to guarantee there is no adverse effect on organizational tasks or security.	Individual Access
		SI-10	Information Input Validation: This control focusses on checking the legitimate syntax and semantics of system inputs like character set, numerical range, length, etc. Pre-screening inputs prevent the content from being unintentionally deciphered as commands.	-	-	Safeguards
		CM-5	Access Restrictions for Change: This control focusses on automated access enforcement and auditing, dual authorization, privilege limitation. It also prevents the installation of organization-defined software and firmware components without confirmation that the part has been digitally signed using a certificate that is recognized and affirmed by the organization.	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1	Development, testing and operational situations will be isolated to diminish the dangers of unapproved access or changes to the operational condition. Methods will be actualized to control the establishment of programming on operational systems. Access to program source code, business processes that affect information security will be controlled.	Accountability
3.	Man-in-the-middle attack	SC-13	Cryptographic Protection: This control deals with the protection of classified data and controlled unclassified information, arrangement and implementation of digital signatures; and implementation of information partition when approved people have fundamental clearances yet do not have the conventional access approvals. Cryptography can likewise be utilized to help arbitrary numbers and hash generation.	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5	A policy on the utilization of cryptographic controls for security of data will be created and actualized. Information associated with application services passing over public networks shall be protected from fraudulent activity, unauthorized disclosure, and modification. Cryptographic controls shall be utilized consistent with all relevant agreements.	Safeguards
		SC-23 (1) (3) (5)	Session Authenticity: Dependence on Certificate Authorities (CAs) for establishing secure sessions, for instance, the utilization of Transport layer Security (TLS) certificates. These certificates after confirmation by their respective CAs encourage the establishment of protected sessions between web clients and web servers.	-	-	
		AC-12 (1) (2) (3)	Session Termination: This control tends to the termination of user-initiated logical sessions with a time-out warning and termination messages.	-	-	
		IA-2(1) (2) (5) (8) (10) (12)	Identification and Authentication: Exceptionally identify and authenticate organizational users or processes following up for the benefit of organizational users.	A.9.2.1*, A.9.4.2*	Conventional user registration and de-registration process shall be implemented to enable the assignment of access rights. Where required by the access control policy, access to systems and applications shall be constrained by a protected log-on procedure.	Individual Access
4.	DNS Spoofing	SC-20(2)	Secure Name/Address Resolution Service (Authoritative Source): This control empowers external clients including, for instance, remote Internet	A.13.1	Networks shall be managed and controlled. Security mechanisms, service levels, and management requirements of	Safeguards

			clients, to get origin authentication and integrity verification affirmations for the host/service name to network address resolution information obtained through the service.		all network services shall be distinguished and included in-network services agreements, whether these services are provided in-house or outsourced.	
		SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver): DNS client resolvers either conduct validation of DNSSEC signatures or clients utilize authenticated channels to recursive resolvers that conduct such validations.	-	-	
5.	Sniffer attack	PE-18(1)	Location of System Components: Position the components inside the system facility to limit the potential harm from physical and environmental damage and to limit the open door for unauthorized access.	A.11.1.4, A.11.2.1	Physical protection against catastrophic events, malicious attacks, accidents will be planned and applied. Equipment shall be sited and shielded to diminish the risks from ecological dangers and open doors for unauthorized access.	Safeguards
		SI-20(4)	De-identification: The direct identifiers will be removed using an advanced encryption standard. Using a different key for each identifier provides a higher security and privacy.	A.8.2.3 A.18.1.4**	According to the information classification scheme of organization, asset handling procedure shall be developed. The personally identifiable information shall be protected, and its privacy is ensured as per legislation and regulation.	
6.	Brute-force attack	SC-23(3)	Session Authenticity: Dependence on Certificate Authorities (CAs) for establishing secure sessions, for instance, the utilization of Transport layer Security (TLS) certificates. These certificates after confirmation by their respective CAs encourage the establishment of protected sessions between web clients and web servers.	-	-	Safeguards
		AC-7(1) (3) (4)	Unsuccessful Logon Attempts: Authorize a limit of successive invalid login endeavors by a user during a defined time-span and consequently lock the account/node for defined timeframe; lock the account/node until released by an administrator; delay next login prompt per delay algorithm; take an action when the extreme number of unsuccessful attempts is surpassed.	A.9.4.2	Where required by the access control policy, access to systems and applications shall be controlled by a protected log-on procedure.	
7.	Denial of service attack & Distributed Denial of Service attack	SC-5(1) (2) (3)	Denial of Service Protection: This control is to protect against or limit the effects of the types of denial of service attacks by restricting the internal users through detection and monitoring; manage capacity, bandwidth, or redundancy to limit the effects of information flooding denial of service attacks.	A.12.1.3	The utilization of resources will be monitored, tuned and projections made of future capacity requirements to guarantee the necessary system performance.	Safeguards
		AC-10	Concurrent Session Control: Organizations may define a limit for concurrent sessions for system accounts globally, by account type, by account, or a mix/combination thereof.	-	-	
8.	Hidden field manipulation	SI-3	Malicious Code Protection: This control focusses on configuring malicious code protection mechanisms to perform periodic scans of the system, block malicious code and send an alert to the administrator in response to the malicious code detection and eradication by employing these mechanisms at system entry and exit points.	A.12.2.1	Identification, prevention and recovery controls to secure against malware will be implemented, combined with appropriate user awareness.	Safeguards & Openness
		CM-5	Access Restrictions for Change: This control focusses on automated access enforcement and auditing, dual authorization, privilege limitation. It also prevents the installation of organization-defined software and firmware components without confirmation that the part has been digitally signed using a certificate that is recognized and affirmed by the organization.	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1	Development, testing and operational situations will be isolated to diminish the dangers of unapproved access or changes to the operational condition. Methods will be actualized to control the establishment of programming on operational systems. Access to program source code, business processes that affect information security will be controlled.	Accountability
		SI-10	Information Input Validation: This control focusses on checking the legitimate syntax and semantics of system inputs like character set, numerical range, length, etc. Pre-screening inputs prevent the content from being unintentionally deciphered as commands.	-	-	

9.	Cookie Poisoning	AC-6(1)	Least privilege-authorize access to security functions: This control focusses on allowing authorized access intrusion detection parameters, filtering rules for routers/firewalls, cryptographic key management.	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5	Users authorization will be provided to specific users only on network and network services. The access rights and access to program source code shall be restricted and controlled. The use of utility programs shall be controlled.	Accountability
		CM-5	Access Restrictions for Change: This control focusses on automated access enforcement and auditing, dual authorization, privilege limitation. It also prevents the installation of organization-defined software and firmware components without confirmation that the part has been digitally signed using a certificate that is recognized and affirmed by the organization.	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1	Development, testing and operational situations will be isolated to diminish the dangers of unapproved access or changes to the operational condition. Methods will be actualized to control the establishment of programming on operational systems. Access to program source code, business processes that affect information security will be controlled.	Safeguards
10.	Backdoor and Debug options	SI-3(1) (4) (6) (8) (10)	Malicious Code Protection: This control focusses on configuring malicious code protection mechanisms to perform periodic scans of the system, block malicious code and send an alert to the administrator in response to the malicious code detection and eradication by employing these mechanisms at system entry and exit points.	A.12.2.1	Identification, prevention and recovery controls to secure against malware will be implemented, combined with appropriate user awareness.	Safeguards & Openness
		PL-8(1) (2)	Security and Privacy Architectures: Through this control, organizations deliberately allot security safeguards (procedural, technical or both) in the security architecture such that adversaries must overcome different multiple protections to accomplish their objective which is defense in depth considering supplier diversity.	A.14.1.1*, A.18.1.4**	The information security-related requirements will be remembered for the necessities for new information systems or improvements to existing information systems. Privacy and protection of personally recognizable information shall be guaranteed as required in relevant legislation and regulation where appropriate.	Safeguards
11.	Ransomware attack	SI-4	System Monitoring: This control focusses on to connect and configure individual intrusion detection tools to system-wide intrusion detection system; monitor inbound and outbound communication traffic and system-generated alerts in peculiar situations; restrict non-privileged users; automated response to suspicious events; visibility of encrypted communications; analyze communication traffic anomalies and event patterns, etc.	A.18.1.4**	Privacy and protection of personally recognizable information shall be guaranteed as required in relevant legislation and regulation where appropriate.	Safeguards
		CP-9	System backup: This control focusses on conducting backups of user-level and system-level information contained in the system and also protects the confidentiality, integrity, and availability of the backup information at the storage locations.	A.12.3.1 A.17.1.2 A.18.1.3	Backup copies of information, software, system images shall be taken. The processes ensure the required level of continuity for information security in adverse situations. Records shall be protected from loss, destruction, unauthorized access.	Safeguards
		CM-5	Access Restrictions for Change: This control focusses on automated access enforcement and auditing, dual authorization, privilege limitation. It also prevents the installation of organization-defined software and firmware components without confirmation that the part has been digitally signed using a certificate that is recognized and affirmed by the organization.	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1	Development, testing and operational situations will be isolated to diminish the dangers of unapproved access or changes to the operational condition. Methods will be actualized to control the establishment of programming on operational systems. Access to program source code, business processes that affect information security will be controlled.	Safeguards
		AT-2	Awareness and Training Policy and Procedures: This control mainly focusses to facilitate the implementation of training and awareness programs for the system users and employees of the organization relevant to their job function.	A.7.2.2 A.12.2.1 A.18.1.4**	All employees and contractors of the organization shall receive appropriate awareness education and training relevant to their job function. Detection, prevention, and recovery controls to protect against malware shall be provided with appropriate user awareness.	Safeguards

Note: *An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control [17].*
A double asterisk (**) indicates that the NIST control can be used to support the requirement for privacy protection in 18.1.4, but given the general and broad-based nature of 18.1.4, the NIST control in isolation does not provide the breadth and depth of coverage needed for adequate protection of privacy [17].

As per the article published by Oracle [38], it is compliant to ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018/2014, NIST 800-171, PCI DSS, PIPEDA, HIPAA, GDPR, etc. As per an article on SAP website [39], it is compliant to ISO/IEC 9001 quality management system, ISO/IEC 27001 Security Management system, ISO/IEC 22301 Business Continuity Management system, ISO/IEC 27018, ISO/IEC 27017, PCI DSS, C5, CSA, etc. Some small and medium-sized enterprises (SME) which cannot afford very expensive and top ERPs like SAP, Oracle, Microsoft adopt open-source ERP software like ERPNext, Odoo, MixERP, iDempiere, etc and less expensive ones. Table III lists the various security controls which are currently in place in Oracle and SAP ERP software.

TABLE III. LIST OF CONTROLS CURRENTLY IN USE IN SAP & ORACLE ERP SYSTEMS

S.No	ORACLE	S.No	SAP
1	**Asset Classification and Control [16]**	**1**	**OS and Database Security [41]**
1.1	Responsibility, Inventory, and Ownership of Assets	**2**	**Secure Operation [41]**
1.2	Asset Classification and Control	2.1	User and Authorization Management
2	**Human Resources Security [16]**	2.2	Security Incident monitoring using audit logs
2.1	Employee Screening	**3**	**Security Compliance [41]**
2.2	Security Awareness Education and Training	3.1	Security Auditing
2.3	Enforcement	3.2	Emergency and Backup processes
3	**Physical Security [16]**	**4**	**Physical Security [42]**
4	**Communications and Operations Management [16]**	4.1	Multi-factor authentication-photo IDs, key cards, personal ID numbers (PIN), biometric authentication
4.1	Segregation of Duties	**5**	**Network Security [42]**
4.2	Protection Against Malicious Code	5.1	Multitier network architecture
4.3	Network Security Management	**6**	**Application Security [42]**
4.4	Monitoring and Protection of Audit Log Information	6.1	Enforce segregation of duties
5	**Access Control [16]**	6.2	Protect applications from insider threats, with tight encryption through a 256-bit Secure
5.1	Access Control	6.3	Avoid risky plug-ins and downloads
5.2	User Access Management	6.4	Guard against “phishing” and “pharming”
5.3	Network Access Controls	6.5	Protect against improper logins
5.4	Access grant approval	**7**	**Data Segregation, Limited Data Access, and Encryption [42]**
5.5	Access Termination	7.1	Role-based Access Controls
6	**Information Systems Acquisition, Development, and Maintenance [16]**	**8**	**Security Audits [42]**
6.1	Access Control To Program Source Code	**9**	**Custom code Security**
6.2	Technical Vulnerability Management	**10**	**Secure system Logon [15]**
7	**Information Security Incident Response**	**11**	**Encryption [15]**
8	**Audit**	11.1	Security zone encryption
9	**Customer Data Retention**	11.2	Email encryption
10	**Automated Monitoring [40]**	11.3	Hard disk encryption
10.1	Firewall/Intrusion Monitoring	11.4	Protection against malware
10.2	Access and SOD Monitoring	**12**	**Corporate continuity in crisis situations [15]**
11	**Periodic Reviews [40]**	**13**	**Security awareness trainings [15]**
11.1	User Access Review		
11.2	Role/Responsibility/Group review		
11.3	Critical access review		
11.4	Security Configuration review		
11.5	Segregation of Duties review		
12	**Configuration [40]**		
12.1	Password settings		
12.2	Workflow		

Best practices proposal for the Retirement phase of ERP system:

The substitution of the picked ERP system will become necessary in the retirement stage when innovations show up or the ERP system gets deficient in the business prerequisites. For any organization, it is important to follow proper data sanitization methods to ensure security. Data sanitization is the process of purposely, permanently irreversibly evacuating or pulverizing the data stored on a memory device to make it unrecoverable. A device which has been sanitized has no residual data, even with the help of advanced forensic tools, the data won’t ever be recouped. Below are the steps which are to be followed before actual sanitization.

1. When an organization finishes an assessment of its system confidentiality, it should determine the need for data sanitization.
2. Upon competition of sanitization decision making, the organization should document the decision and guarantee that a process and legitimate resources are set up to help these decisions.
3. Verifying the chose data sanitization and disposal process is a fundamental step in maintaining confidentiality. The

table below contains the list of media used in an ERP system and what process each media type can follow in Clear, Purge and Destroy sanitization methods.

Information summarizing in table IV has been partially considered from NIST SP 800-88 [20].

TABLE IV. SANITIZATION METHODS VERSUS MEDIA TYPE

S.NO	Media Type	Clear	Purge	Destroy
Network Devices				
1.	Router	Perform a full manufacturer's reset to reset the router back to its factory default settings.	Perform a full manufacturer's reset to reset the router back to its factory default settings.	Shred/Disintegrate/Pulverize/Incinerate.
2.	Firewall	Delete data using PowerShell or Netsh tools.	Data can be purged using an API call.	Shred/Disintegrate/Pulverize/Incinerate.
3.	Network Switch	Perform formatting options/reset the entire system using clear config commands.	Perform formatting options/reset the entire system using clear config and write erase commands.	Shred/Disintegrate/Pulverize/Incinerate.
4.	Gateway	Delete the gateway after deleting the end-points connected to it.	Delete the gateway after deleting the end-points connected to it.	Shred/Disintegrate/Pulverize/Incinerate.
Hardware Devices				
1.	Hard disks	Overwrite media by using validated and approved overwriting technologies.	Overwrite/Cryptographic erasure/Degausser.	Shred/Disintegrate/Pulverize/Incinerate.
2.	Processor			
3.	Cell Phones	Manually delete all information then perform a full hard reset to reset back to factory default settings.	Manually delete all information then perform a full hard reset to reset back to factory default settings.	Shred/Disintegrate/Pulverize/Incinerate.
4.	Fax Machines	Perform a full reset to reset fax machines back to default settings	Perform a full reset to reset fax machines back to default settings	Shred/Disintegrate/Pulverize/Incinerate
5.	RAM	Power-off and remove the battery	Power-off and remove the battery	Shred/Disintegrate/Pulverize.
Other Storage Devices				
1.	Paper	Refer to destroy Methods.	Refer to destroy Methods.	Shred.
2.	Personal Digital Assistant	Perform a hard reset to reset PDA back to the factory default state.	Perform a hard reset to reset PDA back to the factory default state.	Shred/Pulverize/Incinerate.
3.	USB Removable Media	Overwrite media by using validated and approved overwriting technologies.	Purge using any secure erase software and the hard disks are to be purged using NSA/CSS approved degausser. The degaussing technique will make the hard disk permanently unusable.	Disintegrate/Shred/Pulverize/Incinerate.
4.	CDs/DVDs	Refer to destroy methods.	Refer to destroy methods.	• Remove the information containing layers of CD/DVD using a commercial optical disk grinding device. • Incinerate. • Shredders/Disintegrators.
5.	Flash drives/SD Card	Overwrite media by using validated and approved overwriting technologies	Refer to destroy methods.	Shred/Disintegrate/Pulverize/Incinerate.
6.	ROM	Refer to destroy methods.	Refer to destroy methods.	Shred/Disintegrate/Pulverize.

Table IV: Sanitization methods versus Media type

The description of the terminologies used in the above table is discussed here.

Clear: This process included rewriting with a new value or resetting to the factory state when rewriting is not supported. It is generally applied through standard Read/Write commands to the storage device. However, it does not address hidden or unaddressable locations.

Purge: This process offers a more thorough level of sanitization than clear and is used for more confidential data. Degaussing is an acceptable method for purging where the magnetic media is exposed to the magnetic field to disrupt the recorded data.

Destroy: This process includes physical techniques to completely damage. Disintegration, pulverization, Incineration, and Shredding are the different types of procedures and techniques for media destruction.
Disintegrate-Breakup into small parts.
Pulverize-Reduce to fine particles.
Incinerate-Destroy by burning.

V. Conclusion

The proposed research would contribute to a study of security controls that are to be in place to be resistant to vulnerabilities and attacks generally a cloud-based enterprise resource planning system is prone to. The security controls identified from NIST 800-53 R5 and ISO/IEC 27001:2013 could be in place to prevent/mitigate the attacks and verify if these identified controls are compliant with PIPEDA or not for applicable industries. Additionally, the paper provides an overview of the best practices to clear/purge/destroy the various media types used in the Enterprise Resource Planning system is for the retirement phase of the ERP system. Hence, contributing knowledge about different controls to be in place to prevent/mitigate the attacks on the ERP system along with the best practices for the retirement phase. So, if any small and medium-sized enterprises which cannot afford expensive and top ERP software but wants to adopt ERP, this could be used as an easily available checklist.

The future scope for this research could be adding the controls for any novel attacks that might occur for both traditional and cloud-based ERP systems. Any specific industry which uses ERP system can be chosen and researched upon in-depth and solutions can be proposed/developed.

References

[1] S. Wibowo, S. Grandhi, M. Wells, and P. Balasooriya, “Multicriteria group decision making for selecting human resources management information systems projects,” 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 2016.

[2] M. J. Lee, “Next Era of Enterprise Resource Planning System,” IEEE Conference on Systems, Process, and Control (ICSPC 2017), Dec. 2017.

[3] E. Uppström, C. M. Lonn, M. Hoffsten, and J. Thorström, “New Implications for Customization of ERP Systems,” 48th Hawaii International Conference on System Sciences, 2015.

[4] A. Marder, “8 Best Free, Open Source Enterprise Resource Planning (ERP) Software,” 8 Best Free, Open Source Enterprise Resource Planning (ERP) Software, 26-Jul-2019. [Online]. Available: https://blog.capterra.com/free-open-source-erp-software/. [Accessed: 02-Dec-2019].

[5] “Small and medium-sized enterprises,” Wikipedia, 22-Nov-2019. [Online].Available:https://en.wikipedia.org/wiki/Small_and_medium-sized_enterprises. [Accessed: 02-Dec-2019].

[6] S. Gupta and S. C. Misra, “Compliance, network, security and the people related factors in cloud ERP implementation,” International Journal of Communication Systems, vol. 29, no. 8, pp. 1395–1419, 2016.

[7] R. Bhadauria and S. Sanyal, “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques,” International Journal of Computer Applications, vol. 47, no. 18, pp. 47–66, 2012.

[8] Nazli Yasemin Sahin, “Cloud ERP Security: Guidelines for Evaluation,” Department of Computer and Systems Sciences, 2013.

[9] P. Saa, A. C. Costales, O. Moscoso-Zea, and S. Lujan-Mora, “Moving ERP Systems to the Cloud - Data Security Issues,” Journal of Information Systems Engineering & Management, vol. 2, no. 4, 2017.

[10] M. Yesilyurt and Y.Yalman, “New approach for ensuring cloud computing security: using data hiding methods,” Indian Academy of Sciences, vol. 41, no. 11, Nov. 2016.

[11] S. Binu and M. J, “A Security Framework For An Enterprise System On Cloud,” Indian Journal of Computer Science and Engineering, vol. 3, no. 4, 2012.

[12] J. Duan, P. Faker, A. Fesak, and T. Stuart, “Benefits And Drawbacks Of Cloud-Based Versus Traditional Erp Systems,” Advanced Resource Planning, 2013.

[13] A. Elragal and M. Haddara, “The Future of ERP Systems: look backward before moving forward,” Procedia Technology, vol. 5, pp. 21–30, 2012.

[14] N. Lewis, “ERP security: How to defend against SAP vulnerabilities,” SearchSecurity. [Online]. Available: https://searchsecurity.techtarget.com/tip/ERP-security-How-to-defend-against-SAP-vulnerabilities. [Accessed: 30-Oct-2019].

[15] SAP team, “SAP’s Standards, Processes, and Guidelines for Protecting Data and Information”, 2016. [Online]. Available: https://intelligencegroup.com/wp-content/usermedia/white-paper-sap-sap-standards-processes-guidelines-glo-en.pdf.

[16] Oracle team, “Oracle Corporate Security Practices”, version 1.5, 2018. [Online]. Available: https://www.oracle.com/assets/corporate-security-practices-4490843.pdf.

[17] Joint Task Force, “Security and Privacy Controls for Information Systems and Organizations,” CSRC, 15-Aug-2017. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft. [Accessed: 26-Nov-2019].

[18] IsecT Ltd., “ISO/IEC 27001:2013 - Information technology - Security techniques – Information security management systems – Requirements (second edition),” ISO/IEC 27001 security techniques. [Online].Available:https://www.iso27001security.com/html/27001.html. [Accessed: 27-Nov-2019].

[19] Office of Privacy commissioner of Canada, “A guide for individuals protecting your privacy”, 2015. [Online]. Available: https://www.priv.gc.ca/media/2036/guide_ind_e.pdf.

[20] NIST, “Guidelines for Media Sanitization”, revision 1, 2014. [Online]. Available:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

[21] P. A. Sonewar and S. D. Thosar, “Detection of SQL injection and XSS attacks in three tier web applications,” 2016 International Conference on Computing Communication Control and automation (ICCUBEA), 2016.

[22] “What is SQL Injection and How to prevent it”, Acunetix [Online] Available: http://www.acunetix.com/websitesecurity/sql-injection/. [Accessed: 08-Mar-2020]

[23] K. Pranathi, S. Kranthi, A. Srisaila, and P. Madhavilatha, “Attacks on Web Application Caused by Cross Site Scripting,” 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2018.

[24] R. Parsamehr and S. F. H. Nezhad, “Mutual authentication protocol to share files in cloud storage,” 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2016.

[25] Y. Mirsky, N. Kalbo, Y. Elovici, and A. Shabtai, “Vesper: Using Echo Analysis to Detect Man-in-the-Middle Attacks in LANs,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1638–1653, 2019.

[26] V. Gupta, S. Shah, and S. Shrivastava, “Secure domain name service in software defined network,” 2017 20th International Conference of Computer and Information Technology (ICCIT), 2017.

[27] A. A. Maksutov, I. A. Cherepanov, and M. S. Alekseev, “Detection and prevention of DNS spoofing attacks,” 2017 Siberian Symposium on Data Science and Engineering (SSDSE), 2017.

[28] A. Elgargouri and M. Elmusrati, “Analysis of Cyber-Attacks on IEC 61850 Networks,” 2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT), 2017.

[29] S. Truth, “How to Test for Sniffing Vulnerabilities,” Security Innovation Application and Cybersecurity Blog. [Online]. Available: https://blog.securityinnovation.com/blog/2011/07/how-to-test-for-sniffing-vulnerabilities.html. [Accessed: 09-Mar-2020].

[30] M. Shema, “Breaking Authentication Schemes,” Seven Deadliest Web Application Attacks, pp. 91–108, 2010.

[31] A. Patil, A. Laturkar, S. V. Athawale, R. Takale, and P. Tathawade, “A multilevel system to mitigate DDOS, brute force and SQL injection attack for cloud security,” 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC), 2017.

[32] “A2-Broken Authentication,” OWASP. [Online]. Available: https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication.html. [Accessed: 09-Mar-2020].

[33] S. Weisman, “What are Denial of Service (DoS) attacks? DoS attacks explained,” Norton. [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html. [Accessed: 09-Mar-2020].

[34] “Web Parameter Tampering,” OWASP. [Online]. Available: https://owasp.org/www-community/attacks/Web_Parameter_Tampering. [Accessed: 09-Mar-2020].

[35] H. Al-Amro and E. El-Qawasmeh, “Discovering security vulnerabilities and leaks in ASP.NET websites,” Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012.

[36] J. Jussila, “HTTP Cookie Weaknesses, Attack Methods and Defense Mechanisms: A Sys-tematic Literature Review,” 2018 University of Jyvaskyla Faculty of Information Technology, 2018.

[37] H. Turaev, P. Zavarsky, and B. Swar, “Prevention of Ransomware Execution in Enterprise Environment on Windows OS: Assessment of Application Whitelisting Solutions,” 2018 1st International Conference on Data Intelligence and Security (ICDIS), 2018.

[38] “Oracle Cloud Compliance,” Cloud Compliance - Oracle Cloud SaaS, PaaS, and IaaS | Oracle Canada. [Online]. Available: https://www.oracle.com/ca-en/cloud/cloud-infrastructure-compliance/. [Accessed: 30-Mar-2020].

[39] “Certifications and Compliance: SAP Trust Center,” SAP. [Online]. Available:https://www.sap.com/canada/about/trust-center/certification-compliance.html. [Accessed: 30-Mar-2020].

[40] A. Parisian, “Access Controls in Oracle EBS: Know enough to be dangerous!,” Fastpath.[Online].Available:https://www.gofastpath.com/blog/know-access-controls-oracle-ebs. [Accessed: 30-Mar-2020].

[41] “Security Recommendations: A Practical Guide for Securing SAP Solutions,” *SAP*.[Online].Available:https://www.sap.com/documents/2017/03/14cf06b2-af7c-0010-82c7-eda71af511fa.html. [Accessed: 29-Mar-2020].

[42] “How SAP® SuccessFactors® Solutions Support Best Practices for Data Privacy and Cloud Security,” *SAP*. [Online]. Available: https://www.successfactors.com/content/dam/successfactors/en_us/resources/brochures-product/how-sap-successfactors-solutions-support-best-practices-for-data-privacy-and-cloud-security.pdf. [Accessed: 29-Mar-2020].