IBIMA Publishing
Journal of Information Assurance & Cyber security
https://ibimapublishing.com/articles/JIACS/2021/164568/
Vol. 2021 (2021), Article ID 164568, 14 pages, ISSN: 2165-9923
DOI: 10.5171/2021.164568

Research Article

A novel e-Government Framework using Blockchain

Haitham ASSIRI[1], Priyadarsi NANDA[2] and Manoranjan MOHANTY[3]

[1]University of Technology Sydney, Sydney, Australia and Jazan University, Jazan, Saudi Arabia

[2,3]University of Technology Sydney, Sydney, Australia

Correspondence should be addressed to: Haitham ASSIRI; haitham.assiri@student.uts.edu.au

Received date:3 November 2020; Accepted date:10 February 2021; Published date: 23 June 2021

Abstract

The e-Government system leverages Information and Communication Technology (ICT) to transform the relationship between government bodies and citizens, businesses and other government ministries, departments, and agencies. The primary aim is to make government services more seamless, efficient and timely for every citizen and organisation. However, e-Government systems are now faced with security threats and cyber attacks, and these challenges have raised concerns about users' privacy as well as the confidentiality and integrity of user data. Therefore, this paper assesses the degree of risk and vulnerability associated with websites used for e-Government function. This paper considers one such website, the Saudi's e-government website Yesser, by using three penetration test tools namely Zap, Rapid7, and Nessus. The results show that the Yesser website does not have critical vulnerabilities; however, it has severe and medium-level vulnerabilities. The paper proposes a new framework which can integrate blockchain based scheme into the Saudi e-Government system. The framework represents a hierarchical model and involves the use of blockchain between the De Militarized Zone (DMZ) and the Secured Intranet zone.

Keywords: Blockchain, e-Government, Cyber threats, Penetration Test Tools.

Introduction

Technology has shaped the world and turned the universe into a global village. The developments in information technology cut across both public and private sectors. Basically, the integration of IT into business to provide public services online as well as to increase government's efficiency is called e-Government. However, as promising and great as e-Government is, it faces the challenge of cyber threats. According to Rehman *et al.* (2016), concerns about cyber threats have affected users' acceptability of e-government systems. Users perceive that hackers or third parties may have access to

Cite this Article as: Haitham ASSIRI, Priyadarsi NANDA and Manoranjan MOHANTY (2021), "
A novel e-Government Framework using Blockchain", Journal of Information Assurance & Cyber security, Vol. 2021 (2021), Article ID 164568, DOI: 10.5171/2021.164568

confidential information like credit card details.

Meanwhile, it is the government's responsibility to protect user data and strengthen the e-Government system against any form of security threat. Blockchain technology is a good option to secure e-Government. Blockchain technology, the concept behind cryptocurrencies such as Bitcoin, Ethereum etc., can be used for the benefit of the public sector. It can make government operations and services more secured and more efficient, and guarantee improved public service delivery. Ultimately, there will be an increase in public trust. Blockchain is a distributed ledger shared among parties participating in a network. The majority of the participants must agree before a transaction can be approved.

Ølnes and Jansen (2017) noted that blockchain technology can be easily mastered, adopted and adapted by a large number of people. The study revealed that the blockchain technology is now an emerging technology for new innovations and development not only in the financial systems but also in the government agencies and organizations.

This study takes a closer look at identifying the vulnerabilities and risks associated with the present e-Government systems around the world. A case study is conducted on the e-Government system created and implemented by the government of Saudi Arabia. In Saudi Arabia, the government has embraced a new technological era in which technology is utilised as an instrument to make communication, government services, and connectivity more seamless. Saudi's e-Government system, Yesser, is pivotal to the realization of the Saudi Vision 2030. As a result, it is important that Yesser website has adequate security. This paper aims to determine the level of security of Yesser website by utilizing three penetration test tools to scan the website. The tools include Zap, Rapid7 and Nessus. Based on the analysis, this paper proposes a new framework with the use of blockchain into **Yesser.** The framework represents a hierarchical model and involves the use of blockchain between the De Militarized Zone (DMZ) and the Secured Intranet zone.

The specific objectives of this paper include the following:

a. To determine the degree of vulnerability of e-government services to breach of privacy, trust, confidentiality and security.
b. To determine the degree of vulnerability of the Saudi e-government system (Yesser) to cyber attacks.
c. To propose a new framework that leverages blockchain to secure the Saudi e-Government system.

The structure of the paper is as follows: Section II presents a review of the existing literature. In Section III, the methods used in the study are discussed. Section IV presents the results and discussion. Finally, Section V concludes the study while setting the stage for further research works.

Literature Review

Vulnerability of e-Government Services

According to AlGarni (2015), hacking, terrorism and software error constitute the major types of vulnerabilities of Saudi e-government systems. On the part of the government and employees dealing with e-government services, there are issues like lack of professionalism and accountability, poor IT infrastructure, lack of awareness of security perspectives at customer level, and inadequate laws and policies guiding e-Government services.

Choejey *et al.,* (2015) noted that the lack or limited use of a standard web security policy and risk management practices have led to cyber security threats like malware, phishing scams and hacking in Bhutan. Alsmadi and Abu-Shanab (2016) used Rapid7 security and penetration testing tools to explore the vulnerabilities of major e-government websites in Jordan. The outcomes of the tests carried out indicated that most of the websites are prone to attacks.

Also, having realised that only little efforts were made towards evaluating the security level of Saudi Arabia's e-government websites, Al-Sanea and Al-Daraiseh (2015) assessed 150 websites owned by financial, governmental, academic and commercial organisations. The paper noted that vulnerabilities in e-government websites are caused by wrong configuration, weaknesses in programming, or lack of updates. The result of the assessment revealed that the websites are faced with low, medium and high impact vulnerabilities. For instance, 61% are vulnerable to Clickjacking, 17.5% are vulnerable to SQL injection and 13.5% are vulnerable to Shell injection. Based on the number of vulnerabilities found, a comparison was made between government and commercial websites. The result of this comparison showed that commercial websites are more secure than government websites.

Using tools like Google Speed Insight, Pingdom, Acunetix, and w3c Checker, Elisa (2017) assessed the accessibility, usability, and web security vulnerabilities of seventy-nine (79) selected e-government websites in Tanzania. The outcomes on web security vulnerabilities showed that forty (50.6%) out of the 79 websites assessed have one or more high-severity vulnerabilities (cross site scripting-XSS or SQL injection) while fifty-one (64.5%) have one or more medium severity vulnerabilities (Denial of Service or Cross site request forgery).

Bissyandé *et al.* (2015) carried out an empirical assessment of e-government websites' security in Burkina Faso. A systematic scanning of the websites for simple and well-known vulnerabilities showed that there are serious security issues calling for urgent attention. For example, it was possible to crawl all information (including hostname and password) from temporary backup files in a government website to directly read and write in the database, thereby impersonating the website's administrator.

Murah and Ali (2018) evaluated 16 Libyan e-government websites using a penetration testing framework. A content analysis was also carried out to determine how far the privacy and security policies have been implemented on the websites. The results of the test revealed that nine out of the sixty websites have high to medium vulnerabilities. Most of these vulnerabilities were due to miss-configuration of the systems and outdated software. Only two of the websites have their privacy and security policies published.

Pandya and Patel (2017) explored the relationship between technology in relation to the vulnerability severity and vulnerability type in 26 e-government applications and websites of Gujarat, India. Most of the websites made use of Microsoft technology while some used Apache technology. It was observed that there are more medium to low vulnerabilities in websites using Apache technology compared to those using Microsoft technology. Meanwhile, informational vulnerabilities and validation-type vulnerabilities are higher in Microsoft technology than Apache technology.

Use of Blockchain for e-Government Systems

As noted by Choejey et al. (2015), the existing e-government services are highly centralised, making them vulnerable to outside attacks. Due to their reliance on human controls, the likelihood of errors is high. Inside rogue users can compromise the data for selfish purposes. Since blockchain is completely descentralised, it becomes a strong option. Yang *et al.* (2018) proposed a framework of descentralised, privacy preserving and secure e-government system using artificial intelligence and blockchain technology. The paper noted that intrusion detection and blockchain technology can complement each other. Blockchain will ensure security, trust and privacy while intrusion detection will help in detecting anomalies during blockchain transactions.

In their own research, Diallo *et al.* (2018) proposed the use of Decentralised Autonomous Organisation (DAO) and

blockchain technology to improve the e-government system. A high-level architectural description of the model was made, after which a detailed design was carried out. The design involves user registration, preparation of contract, monitoring contract execution, and auditing. Through this, the researchers were able to demonstrate that a blockchain-based government DAO can allow monitoring and analysing e-Gov services as well as provide accountability, transparency, better national resource management and immutability.

In another research, Elisa *et al.* (2018) noted that information security and privacy can be further improved by data encryption and distribution over the entire network. A blockchain-based peer to peer exchange and transactions of an e-government system was proposed by the authors. In the scheme, G2C means Government to Citizens, G2G means Government to Government, while G2B means Government to Business. The scheme typically presents how citizens and businesses interact with government services in a blockchain-based e-government system.

According to Swan (2015), blockchain technology can be used for information exchange and any transaction that occurs in the government. The study noted that blockchain can be implemented in asset registry, information exchange, inventory, intangible assets (like votes, patents, health data, reputation, information, etc.) and hard assets like physical property. With blockchain, government agencies can keep track of a ledger and the immutable history of transactions. Swan (2015) noted that blockchain applications in the government include keeping record of judicial decisions, marital status, digital identity, e-voting, criminal records, tracing money, tax records, passports, business licenses, etc.

Challenges and Difficulties of applying Blockchain to e-Government Systems

Carter and Ubacht (2018) noted that the challenges facing the adoption of blockchain in e-Government include scalability, flexibility and security. From an organisational perspective, the challenges are related to acceptability and the necessity of a new governance model. Meanwhile, from an environmental perspective, lack of regulations is the main challenge. Carter and Ubacht (2018) also referred to the lack of an overall application platform where the scalability, flexibility, security, reliability, and interoperability of blockchain technology for e-Government system are dealt with calls for the need to make a proper design solution. In addition, the adoption of blockchain technology will lead to organisational transformation leading to significant changes in process, structure, culture and strategy.

Hou (2017) noted that the application of blockchain in the Chinese e-government system offers some benefits like greater accessibility and transparency of government information; improvements in the quality and quantity of government services; and development of information-sharing across different organizations. However, the system still faces the problems of reliability and information security (Hou, 2017). Therefore, it is important to create a general application platform of blockchain technology, while also developing management standards to ensure an effective integration of blockchain into e-government.

Analysis Methods

Research Objective 1: PRISMA format for a Systematic Literature Review (SLR)

To determine the degree of vulnerability of e-Government services to breach of privacy, trust, confidentiality and security, this research leverages the outcomes of existing related literature by carrying out a Systematic Literature Review. The SLR follows the PRISMA format (Mohrer, 2009). The steps adopted include Database Search, Exclusion and Inclusion Criteria, Quality Evaluation and Data Analysis. The search sources used are EBSCO Information Sciences (www.ebsco.com/), IEEE Xplore (www.ieexplore.ieee.org/Xplore/), Elsevier

ScienceDirect (www.sciencedirect.com/) and Google Scholar (www.scholar.google.com.au/). The search terms entered into the databases include "e-government frameworks", "effectiveness of e-Government", "cyber security of e-Government systems", "blockchain technology" and "blockchain in e-Government".

Research Objective 2: Use of Penetration Testing tools on Yesser's website

This research leverages three penetration testing tools to determine the degree of vulnerability of Yesser's website (www.yesser.gov.sa) to cyber threats and attacks. The three tools used include the following:

1. Rapid7
2. Nessus
3. Zap

These penetration testing tools are used because they make it easy to bypass local network restrictions in order to scan from external IP addresses. They also make it possible to create reliable proof-of-concepts to prove the risk of vulnerabilities. After scanning the Yesser website using each of the three tools, the results have been collected and analysed.

Research Objective 3: New e-Government Framework

e-Government systems are vulnerable to external and internal threats and attacks due to various reasons as discussed before in this review. Watching for such attacks and taking appropriate remedial steps is necessary. Based on this, this paper proposes a new framework which integrates blockchain technology into e-Government for security and privacy protection of the system and users. This directly addresses the research's third objective. The framework is shown in Figure 1 below.

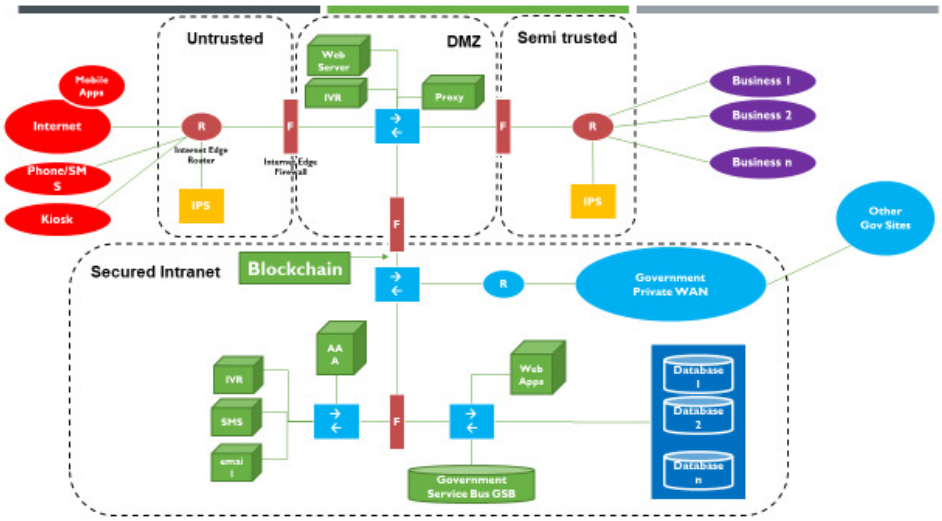

Figure 1: A Proposed Framework with Integration of Blockchain for e-Government

In Figure 1, "R" represents Blocks, "F" represents router firewall, and"→" represents switches in an enterprise government network. IPS is a standard intrusion prevention system.

Looking at the schematic presented, the left side is termed as "untrusted" as this is public internet where the end users' system security policy is open and cannot be regulated as per government organisations' mandates. The right-hand side involves the connection to different businesses which are required to make the e-government system meet users' service requests. The in-between zone is DMZ (de

militarized zone), which is acting as a connection termination point for both the untrusted and semi-trusted zones. DMZ is secured with three firewalls acting as a perimeter security system and two individual IPS for any malicious traffic. The Blockchain technology is put between the DMZ zone and the Secured Intranet zone. Adding blockchain between the two secure zones will create a high level of confidentiality, trust, data integrity, privacy, and access control. Blockchain technology protects security and privacy through separate personal keys and public keys for access, distributed blocks of the database, consensus rules for authentication, peer-to-peer endorsements, and decentralisation.

Results and Discussion

This section discusses the research findings, addressing directly the three research objectives mentioned in the previous section of this paper. The first research objective relates to analysing various works on e-government adopted by different countries. This gives scopes to move to the next research objective in which, the authors of this paper demonstrate how different penetration tools are being used to assess the risks and vulnerabilities in one specific e-government website, Yesser. Based on the findings, a new e-government framework is proposed to address the third research objective.

PRISMA format for a Systematic Literature Review

After the search terms were entered into the search sources, 138 papers were identified. Out of these papers, 36 duplicates were found, thereby reducing the number of papers to 102. The remaining papers were then screened to determine their relevance based on titles, abstracts and full texts. At the end of this screening, 66 studies were eliminated, resulting in 36 articles. These 36 papers are then evaluated for quality, and the results approved 10 papers that are ultimately included in this SLR as provided in Table 1 below.

Table 1: Summary of Papers on Privacy and Security of e-Governance

Paper	Description	Method	Weakness & Limitations	eGov Security Requirements		
				Confidentiality	Trust / Privacy	Integrity
Zhao, J. and Zhao, S. (2010)	Carried out an assessment of e-government sites owned by the United States to look for the opportunities and the threats the sites offer to the users. Less than half of the sites clearly stated their security measures. 98% of the sites used SSL encryption to secure user accounts.	Information Security Auditing, Computer network security mapping and Web content analysis.	Paper identified a lot of security lapses but failed to provide solutions for all.	No	Yes	No
Alshehri, M. and	The paper identified the challenges and	Online Survey and	Paper did not explore the	Yes	Yes	No

Drew, S. (2010)	barriers affecting the adoption of e-government by Saudi citizens.	Data Analysis	security requirements of eGovt. in detail.			
Bertot, J. *et al.* (2014)	The paper examined the ways the current information policy framework failed to address different policy challenges in e-government. The paper then offered recommendations as a starting point to revise the policy.	Survey	The paper is limited to the US only	No	Yes	No
Rehman, M., Esichaikul, V. and Kamal, M. (2012)	The study explored the factors that promote end-user adoption of e-government services in Pakistan. The factors revealed by the findings include user data privacy, performance expectancy, awareness, and social influence.	Unified Theory of Acceptance and Use of Technology (UTAUT) model, Online survey, and Statistical descriptive analysis.	Data sample used is small as the survey had 115 respondents	No	Yes	No
Rodrigues, G., Sarabdeen, J. &Balasubramanian, S. (2016)	The research identified the factors that influence the adoption of e-government services in UAE. Factors identified include confidentiality, users' attitude, and trust.	UTAUT model, Exploratory factor analysis, Regression analysis, and Correlation analysis.	The study failed to provide the ways the factors identified can be addressed.	Yes	Yes	Yes
Osman, I. H., Anouze, A. L., Irani, Z., Al-Ayoubi, B., Lee, H., Balcı, A., . . . Weerakkody, V. (2014)	The study proposed a COBRAS (Cost; Opportunity; Benefit; Risk; Analysis for Satisfaction) framework which balances user's risk and cost of engaging with an e-government service with the associated opportunity and benefit.	Proposed COBRAS framework, 79 questionnaires were filled by 2785 users of Turkey e-govt portal, Utilized structural equation modeling &	The security requirements of e-government were not thoroughly explored.	No	Yes	No

		confirmatory factor analysis.				
AlKalbani, A., Deng, H. and Kam, B. (2015)	This examined how the organisational security culture affects information security compliance in public agencies and organisations in relation to e-government development. The study showed that information security awareness, accountability, social pressure and management commitments positively influence information security compliance in public organisations.	Developed an information security model and hierarchical regression analysis.	No insight was provided on how to improve accountability, information security awareness and management commitments, which were the factors identified to have a positive influence on information security compliance.	Yes	No	Yes
Botchwey, G. (2018)	This paper assessed the level of public trust and confidence in the integrity of data and systems exchanged on Ghana's e-Government platform, with a specific focus on data protection and integrity. The study showed that there is a huge weakness concerning the issues of confidentiality, services' continuous availability and data integrity on e-Government platforms.	Cross sectional survey with respondents drawn from four regions with a high concentration on e-government services.	While the study identified major challenges that need to be addressed like the lack of a national database to verify information, service exclusion, poor internet etc., it did not provide any solutions.	Yes	Yes	Yes
Riswan, M. M. and Rajandran, K. V. R., (2017)	The study examined the causes of low participation in e-Government in Thanjavur district and found out that the causes include the level of awareness, acceptance, and attitude towards	120 respondents selected on the basis of random sampling, regression and correlation	Sample is small; the study noted that e-Government web security needs to be improved but did not state the specific	No	Yes	No

	sustainable development and security of e-Government.	analysis.	improvements to be made and how.			
Haran, M. (2016)	The study identified the relevant stakeholders who are insiders as far as the e-Government IT infrastructure is concerned and listed the threats that may be caused by these insiders. The paper then provided ways to mitigate such threats.	Proposed a robust framework mechanism for early detection and mitigation of insider threats.	The paper is limited to insider threats only.	No	Yes	No
Choejey, P., Fung, C. C., Wong, K. W., Murray, D. and Xie, H. (2015)	An assessment of factors affecting the implementation of the cyber security program in government agencies in Bhutan was carried out. The research showed that several organisations are affected by cyber security threats like hacking, phishing scams and malware. The recommendations provided include technological and managerial practices to improve people's level of confidence and trust in e-government services.	Survey with 157 respondents.	Sample for the survey is small.	Yes	Yes	No

Use of three Penetration Testing tools on Yesser's website

Three different penetration tools are used; Rapid7, Zap and Nessus, to analyse the risks and vulnerabilities associated with e-government websites.

1) Rapid7

The Yesser website was scanned using InsightVM from Rapid7 LLC on February 24, 2020. The website was found to be active and its vulnerabilities by severity are represented by Figure 2. The vulnerabilities by severity are divided into three parts; critical, severe and moderate.

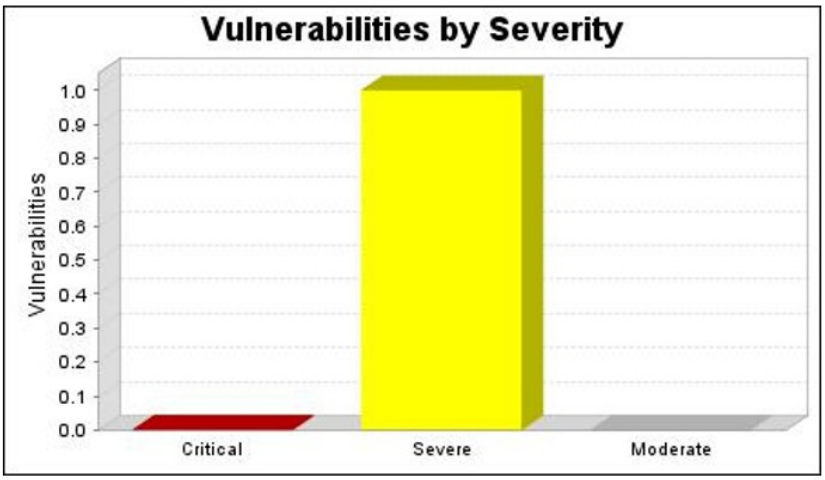

Figure 2: Yesser Vulnerabilities by Severity

As shown in Figure 2, there were no critical vulnerabilities found during the scan of Yesser website. In addition, there were no moderate vulnerabilities discovered. However, there was one severe vulnerability. The severe vulnerability detected was that the subject common name (CN) field in the X.509 certificate is different from the name of the entity providing the certificate.

By vulnerability categories, the Rapid7 scan found 1 vulnerability instance in both the HTTP and Web categories, thereby making them the most common vulnerability categories as shown in Figure 3.

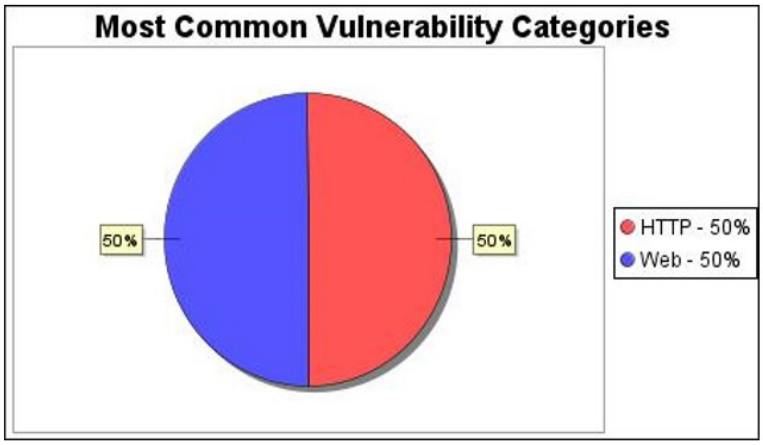

Figure 3: Yesser's Most Common Vulnerabilities

The HTTP and HTTPS services were found on the Yesser website, making them the most common services (Figure 4).

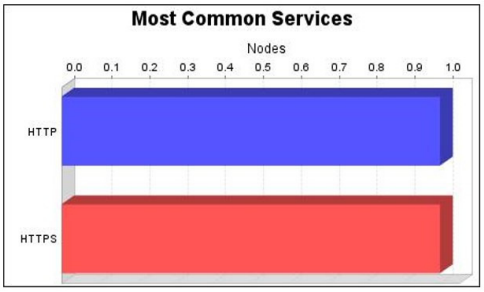

Figure 4: Yesser's Most Vulnerable Services

2) Zap

The Zap scan of the Yesser website was carried out on June 13th, 2020. The summary of the scan is provided in Table 2 below:

Table 2: Summary of Zap Scan of Yesser Website

Risk Level	Number of Alerts
High	0
Medium	1
Low	10
Informational	2

The medium alert received showed that the X-frame options header is not set. The simple solution for this is to ensure that X-frame options HTTP header is set on all the pages of the Yesser website. The low impact vulnerabilities detected by the scan include Absence of Anti-CSRF Tokens, Cookie Without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion, Cookie Without Secure Flag, Cookie No HttpOnly Flag, Web Browser XSS Protection Not Enabled, Incomplete or No Cache-control and, Secure Pages Include Mixed Content, as well as Private IP Disclosure.

The following are the two informational vulnerabilities detected by the scan:

(a) Information Disclosure - Suspicious Comments. The solution for this is to remove all comments that return information capable of helping, and solve any underlying problems.

(b) Timestamp Disclosure – Unix. Here, the solution is to manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

3) Nessus

The Nessus penetration test tool was used to scan www.yesser.gov.sa on February 24th, 2020. The results (Figure 5) showed that there were no critical or high

vulnerabilities in Yesser. However, two medium-level vulnerabilities were found. Also, 22 informational vulnerabilities were detected.

Figure 5: Results of Nessus Scan of Yesser Website

The first medium vulnerability is F5 Big-IP Cookie Remote Information Disclosure. The remote load balancer suffers from an information disclosure vulnerability. The second medium vulnerability is that the web application is potentially vulnerable to Clickjacking.

Proposed e-Government Framework

The current e-government framework in Saudi Arabia (Yesser) uses a centralised database; thereby it has a low level of confidentiality and trust (Al-Mushayt*et al.,* 2012). The proposed model (shown in figure 1) offers better security as it is completely based on a descentralised database.

In the proposed framework, there are three different access scenarios. These include Consumer to Government (C2G), Government to Business (G2B), and Government to Government (G2G). For C2G and G2B, the customer node and business node made lightweight nodes. However, for G2G, the node becomes a full node. In C2G, the government service bus connects directly with internet, mobile apps, kiosk etc. (consumers); in G2B, it connects with business providers; and in G2G, it connects with a government website (which can be owned by a government agency or ministry). As shown in Figure 1, these three relationships are secured by putting the blockchain technology between the DMZ zone and Secured Intranet zone. Adding the blockchain technology to the new framework will make the GSB more secure by distributing GSB across multiple sites and running blockchain, preventing any website's security compromise from affecting the information integrity as a whole. The benefit of using blockchain is that it is decentralized which does not rely on a central point of control, hence, blockchain is resistant to the modification of data. Blockchain brings Trust in a trustless world, since its benefit is beyond securing Financial Transactions.

Conclusion and Future Work

The study presented in this paper explores the most existing literature on securing e-Government systems in different countries. This study reveals that there are several security and privacy issues (particularly regarding confidentiality, trust and integrity) which the existing e-government frameworks have not been able to address thoroughly. While many researchers have made efforts to address security challenges in e-Government system, this study shows that there are still some loopholes that need to be blocked. For example, most of the existing frameworks and models do not capture the necessary e-government security requirements; having a lack of trust in internet-mediated transactions, and in unauthorized access to systems with the help of insiders. In particular, this paper showed that the Yesser website has a few security issues which are majorly categorised as severe, medium-level and low-impact vulnerabilities. Also, this paper proposes a new framework that leverages blockchain to secure the Saudi e-Government system. This proposed model brings decentralisation, access control, confidentiality, privacy and trust into the e-Government service. Future researchers can explore the extent to which blockchain integration has helped in solving the

current issues of Yesser and improved the Saudi e-government services in general.

References

- AlGarni, K., 2015. Information Security Policy for E-government in Saudi Arabia: Effectiveness, Vulnerabilities and Threats.
- AlKalbani, A., Deng, H. and Kam, B., 2015, July. Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure. In *PACIS* (p. 65).
- Al-Mushayt, O.S., Perwej, Y. and Haq, K., 2012. Electronic-government in Saudi Arabia: A positive revolution in the peninsula. *arXiv preprint arXiv:1205.3986*.
- Al-Sanea, M.S. and Al-Daraiseh, A.A., 2015, November. Security evaluation of Saudi Arabia's websites using open source tools. In *2015 First International Conference on Anti-Cybercrime (ICACC)* (pp. 1-5). IEEE.
- Alshehri, M. and Drew, S., 2010. Challenges of e-government services adoption in Saudi Arabia from an e-ready citizen perspective. *World Academy of Science, Engineering and Technology*, *66*, pp.1053-1059.
- Alsmadi, I. and Abu-Shanab, E., 2016. E-government website security concerns and citizens' adoption. *Electronic Government, an International Journal*, *12*(3), pp.243-255.
- Bertot, J.C., Gorham, U., Jaeger, P.T., Sarin, L.C. and Choi, H., 2014. Big data, open government and e-government: Issues, policies and recommendations. *Information polity*, *19*(1, 2), pp.5-16.
- Bissyandé, T.F., Ouoba, J., Ahmat, D., Ouédraogo, F., Béré, C., Bikienga, M., Sere, A., Dandjinou, M. and Sié, O., 2015, December. Vulnerabilities of government websites in a developing country–the case of Burkina Faso. In *International Conference on e-Infrastructure and e-Services for Developing Countries* (pp. 123-135). Springer, Cham.
- Botchwey, G., E-Governance and Cybersecurity: User Perceptions of Data Integrity and Protection in Ghana.
- Choejey, P., Fung, C.C., Wong, K.W., Murray, D. and Xie, H., 2015, November. Cybersecurity practices for e-Government: an assessment in Bhutan. In *The 10th International Conference on e-Business, Bangkok, Thailand*.
- Carter, L. and Ubacht, J., 2018, May. Blockchain applications in government. In *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age* (pp. 1-2).
- Diallo, N., Shi, W., Xu, L., Gao, Z., Chen, L., Lu, Y., Shah, N., Carranco, L., Le, T.C., Surez, A.B. and Turner, G., 2018, April. eGov-DAO: A better government using blockchain based decentralized autonomous organization. In *2018 International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 166-171). IEEE.
- Elisa, N., 2017. Usability, accessibility and web security assessment of e-government websites in tanzania. *International Journal of Computer Applications*, *164*, pp.42-48.
- Elisa, N., Yang, L., Chao, F. and Cao, Y., 2018. A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, pp.1-11.
- Haran, M.H., 2014. Framework Based Approach for the Mitigation of Insider Threats in E-governance IT Infrastructure. *International Journal of Science and Research (IJSR), ISSN (Online)*, pp.2319-7064.
- Hou, H., 2017, July. The application of blockchain technology in E-government in China. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-4). IEEE.
- Murah, M.Z. and Ali, A.A., 2018. Web assessment of libyan government e-government services. *assessment*, *9*(12).
- Osman, I.H., Anouze, A.L., Irani, Z., Al-Ayoubi, B., Lee, H., Balcı, A., Medeni, T.D. and Weerakkody, V., 2014. COBRA framework to evaluate e-government

services: A citizen-centric perspective. *Government information quarterly*, *31*(2), pp.243-256.

- Ølnes, S. and Jansen, A., 2017, September. Blockchain technology as s support infrastructure in e-government. In *International Conference on Electronic Government* (pp. 215-227). Springer, Cham.
- Pandya, D.C. and Patel, N.J., 2017. Study and analysis of E-Governance Information Security (InfoSec) in Indian Context. *IOSR Journal of Computer Engineering*, *19*(1), pp.4-7.
- Rehman, M., Esichaikul, V. and Kamal, M., 2012. Factors influencing e-government adoption in Pakistan. *Transforming Government: People, Process and Policy*.
- Riswan, M.M. and Rajandran, K.V.R., A STUDY ON CYBER SECURITY IN E-GOVERNANCE WITH REFERENCE TO AREAS OF THANJAVUR DISTRICT-TAMIL NADU.
- Rodrigues, G., Sarabdeen, J. and Balasubramanian, S., 2016. Factors that influence consumer adoption of e-government services in the UAE: A UTAUT model perspective. *Journal of Internet Commerce*, *15*(1), pp.18-39.
- Swan, M., 2015. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".
- Yang, L., Elisa, N. and Eliot, N., 2019. Privacy and security aspects of E-government in smart cities. In *Smart cities cybersecurity and privacy* (pp. 89-102). Elsevier.
- Zhao, J.J. and Zhao, S.Y., 2010. Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, *27*(1), pp.49-56.