Secure e-Governance Using Blockchain

Haitham Assiri
School of Electrical and Data Engineering (SEDE)
University of Technology, Sydney
Sydney, Australia
Jazan University
Jazan, Saudi Arabia
Haitham.assiri@student.uts.edu.au

Priyadarsi Nanda
School of Electrical and Data Engineering (SEDE)
University of Technology, Sydney
Sydney, Australia
Priyadarsi.Nanda@uts.edu.au

Manoranjan Mohanty
School of Mathematics and Physical Sciences
University of Technology, Sydney
Sydney, Australia
Manoranjan.Mohanty@uts.edu.au

Abstract— **E-Governance system presents great opportunities for countries around the world offering government services online. Many countries have developed their E-governance systems to facilitate services for their citizen. However, the system suffers from serious challenges like security and privacy issues. These challenges have led to a drastic reduction of public trust in the system. This paper carries out a study on existing studies on securing e-governance frameworks. After a thorough search process and critical quality evaluation, we identify sixteen relevant studies related to the E-governance across various platforms. Our research reveals that use of blockchain technology is a strong option to secure E-government platforms and services. Therefore, a new framework that integrates blockchain into e-governance is proposed with Saudi Arabia selected as a use case. The framework represents a hierarchical model and involves use of blockchain between De Militarized Zone (DMZ) and Secured Intranet zone. We believe our proposed framework would facilitate better and secure management of important functions within the organisation.**

Keywords—Blockchain, E-governance, Security, Privacy

I. 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. Integration of IT into business provide public services available online as well as increase government's efficiency and such a seamless integration is called E-governance.

However, as promising and great as E-governance is, there are privacy and security challenges one should consider while developing such systems. These are some of the big challenges and it is the responsibility of the government to protect their citizen (user data) and strengthen the E-governance system against any form of security threat. Blockchain technology is a good option to secure E-governance. Blockchain technology, the concept behind cryptocurrencies such as Bitcoin, Ethereum etc., is being heavily used in recent years for the benefit in the public sector. It can make government operations and services more secured, 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. This is what creates trust in the network because, once a record or block is created and added to the chain of transactions, it cannot be altered. With this, the distributed ledger is immutable and provides traceability of transactions (Peck, 2017).

Svein and Arild (2017) noted that blockchain technology can be easily mastered and adopted 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. Also, MyungSan (2018) noted that, in less than two years, over hundreds of blockchain projects have already been created to transform government systems in more than thirty nations. For example, Estonia used blockchain technology in the issuance of e-ID for citizens' identity verification. Australia and Ukraine are also using blockchain to build electronic voting systems. Georgia and Honduras (MyungSan, 2018) are working on introducing blockchain technology in the management of land registers. USA is pursuing the use of the technology recording and sharing medical information. China intends to build a blockchain city in near future where works are in progress while, UK is applying blockchain technology to public services (MyungSan, 2018).

Several issues occur in the integration of blockchain into E-governance systems. The objective of this paper is to understand these issues by carrying out an in-depth study. Specifically, we reviewed issues including the level of privacy and security of E-governance, and the effectiveness of blockchain in providing confidentiality, access control and de-centralisation in e-governance system.

The paper is organized as follows: Section II presents the research methods used in carrying out our study. In Section III, a summary of the recent works is presented. Section IV proposes a new framework for use of blockchain in E-governance with Saudi Arabia as the use case. Finally, Section V concludes the paper while setting the stage for further research works.

II. Research Methods

Our research follows guidelines recommended by the PRISMA format (Mohrer, 2009). The steps adopted include Database Search, Exclusion and Inclusion Criteria, Quality Evaluation and Data Analysis.

A. Data Search

This step involves defining the search terms, identifying the data sources and the process of data collection. For this research, four data sources are selected. These search sources include 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/). No paper was obtained from any other source. The search terms entered into the databases include "e-government frameworks", "effectiveness of e-governance", "cyber security of e-governance systems", "blockchain technology" and "blockchain in e-governance". The inclusion and exclusion criteria are provided in the next section.

B. Inclusion and Exclusion Criteria

To review the most relevant papers, our research adopted following criteria.

1. Research work related to e-governance and blockchain or cybersecurity.
2. It is an academic, experimental or commercial project.

1. Publication date is between 2010 and 2019 (both years inclusive)
2. Formal literature review with defined research questions
3. Full text available and written in English.

C. Study Quality Evaluation

The studies selected after applying the inclusion criteria are evaluated using the following quality evaluation questions. Only papers that answer "Yes" to at least two of these questions are ultimately included in this survey.

Q1: Does the paper cover relevant work and explore the research topics comprehensively?
Q2: Does the paper provide clear findings with justifiable results and conclusions?
Q3: Does the paper provide future directions?

D. Research objectives

The specific objectives of our research are as follows:

Research Objective 1: To determine the degree of vulnerability of e-government services to breach of privacy, trust, confidentiality and security.
Research Objective 2: To determine the extent to which blockchain technology contribute to privacy and security of e-government services.
Research Objective 3: To determine the difficulties and challenges involved in applying blockchain technology to e-government services.
Research Objective 4: To propose a new model that leverages blockchain to secure e-governance systems, using Saudi Arabia as a case study.
Based on the above research objectives, our literature review is presented in Section III.

III. 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 left.

A. Privacy, Confidentiality and Security in e-Governance

This section addresses research objective 1 by summarizing the papers that explored the security requirements of e-government systems. These requirements include confidentiality, privacy, trust, and integrity.

Table 1. Summary of Papers on Privacy and Security in 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 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 Drew, S. (2010)	The paper identified the challenges and barriers affecting the adoption of e-government by Saudi citizens.	Online Survey and Data Analysis	Paper did not explore the security	Yes	Yes	No

			requirements of eGovt. in detail.			
Bertot, J., *et al.* (2014)	The paper examined the ways current information policy framework failed to address different policy challenges in e-government. The paper then offered recommendations as 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 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. 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 adoption of e-government services in UAE. Factors identified include confidentiality, users' attitude, and trust.	UTAUT model, Exploratory factor analysis, Regression analysis, 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 filled by 2785 users of Turkey e-govt portal. Utilized structural equation modeling & confirmatory factor analysis.	The security requirements of e-government were not thoroughly explored.	No	Yes	No
AlKalbani, A., Deng, H., and Kam, B. (2015)	This examined how organisational security culture affects information security compliance in public agencies and organisations 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 positive influence on information security compliance.	Yes	No	Yes
Gabriel, B. (2018)	This paper assessed the level of public trust and confidence in the integrity of data and systems exchanged on Ghana's e-governance 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-governance platforms.	Cross sectional survey with respondents drawn from four regions with a high concentration of e-government services.	While the study identified major challenges that need to be addressed like lack of national database to verify information, service exclusion, poor internet etc., it did not provide any solutions.	Yes	Yes	Yes
Mohamed, R. and Rajandran, K. (2017)	The study examined the cause of low participation in e-governance in Thanjavur district and found out the causes include level of awareness, acceptance, attitude towards sustainable development and security of e-governance.	120 respondents selected on the basis of random sampling, regression and correlation analysis	Sample is small; the study noted that e-governance web security needs to be improved but did not state the specific improvements to be made and how.	No	Yes	No

Haran, M. (2016)	The study identified the relevant stakeholders who are insiders as far as e-governance 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 alone	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 cybersecurity program in government agencies in Bhutan. The research showed that several organisations are affected by cybersecurity 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

B. Decentralisation and Access Control in e-Governance

To address research objective 2, this section summarizes the existing literature on how blockchain technology provides security for e-governance services through decentralisation and access control.

The existing e-government services are highly centralised making it vulnerable to outside attacks. Due to its 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 (Choejey et al., 2015). Longzhi *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. The framework proposed by Longzhi et al. (2018) was implemented in four layers. The first layer is the physical layer which has business, employee and citizens known as devices. This first layer implements the basic data capturing functions. The second layer is the communication layer and it connects e-government and users. The third layer is the security layer where the traffic for any suspicious activity is critically analysed. To support record creation, an ethereum platform is also located on the third layer. Finally, the fourth layer has the distributed database of ledger. This database can either be permissioned or permissionless.

In their own research, Weidong *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 analysis of 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 as given in Figure 1. In the figure, G2C means Government to Citizens, G2G means Government to Government, while G2B means Government to Business. The figure typically shows 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 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 government include keeping record of judicial decisions, marital status, digital identity, e-voting, criminal records, tracing money, tax records, passports, business licenses, etc.

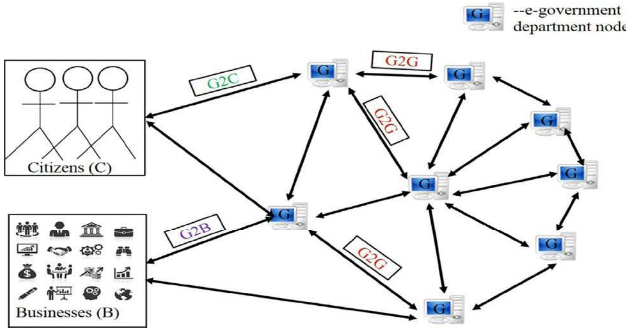

Figure 1. A blockchain-based e-government system (Elisa et al., 2018).

C. *Challenges and Difficulties of applying Blockchain to e-Government Systems.*

To address research objective 3, this section summarises the challenges and difficulties affecting the use of blockchain in securing e-governance services.

Lemuria and Jolien (2018) noted that the challenges facing the adoption of blockchain in e-Government include scalability, flexibility and security. From organisational perspective, the challenges relate to acceptability and the necessity of a new governance model. Meanwhile, from environmental perspective, lack of regulations is the main challenge. Lemuria and Jolien (2018) also opined that the lack of an overall application platform where the scalability, flexibility, security, reliability, and interoperability of blockchain technology for e-governance 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.

Heng (2017) noted that the application of blockchain in 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 (Heng, 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.

IV. PROPOSED NEW E-GOVERNANCE FRAMEWORK

E-Governance systems are vulnerable to external and internal threats and attacks due to various reasons as discussed so far in this review. Watching for such attacks and taking appropriate remedial steps is necessary. Based on this, a newly proposed framework integrates blockchain technology into e-Governance in Saudi Arabia for security and privacy protection of the system and users. This directly addresses research objective 4. The framework is shown in Figure 2 below.

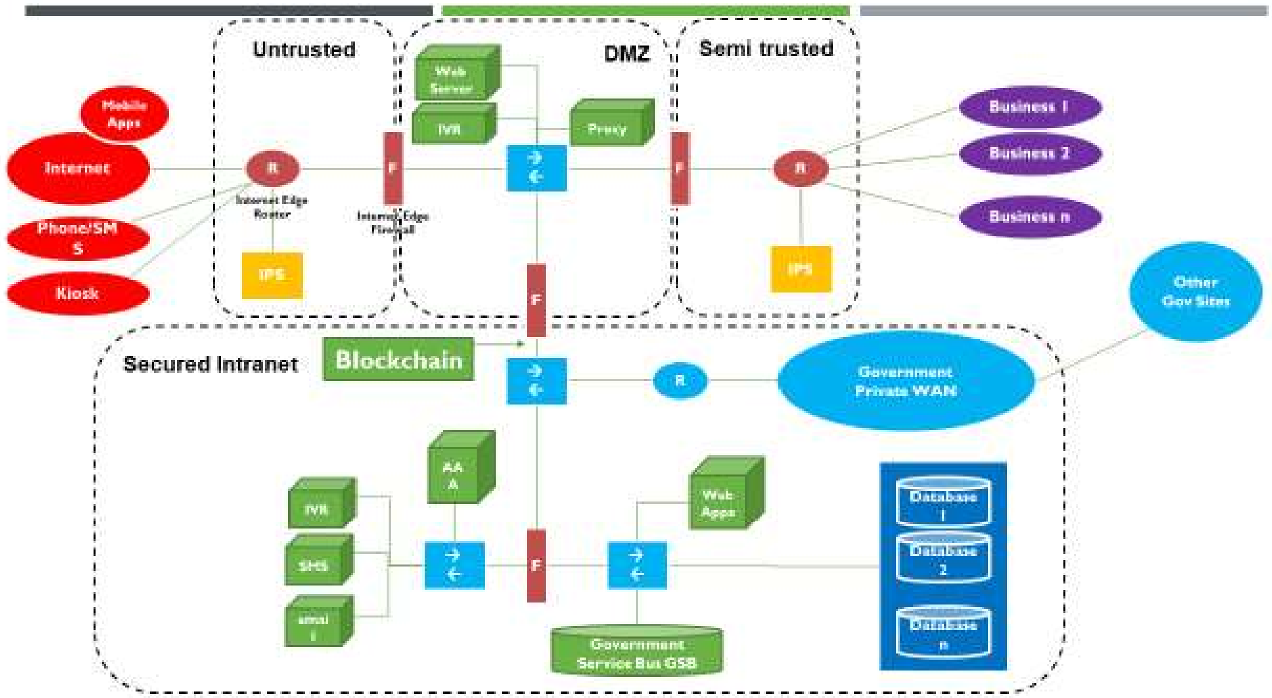

Figure 2. A proposed framework with integration of blockchain for e-governance in Saudi Arabia.

In Figure 2, "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 connection to different businesses which are required to make e-government system meet users' service request. The zone in-between is DMZ (de militarized zone) acting as a connection termination point for both 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 DMZ zone and 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 will protect 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.

The current e-government framework in Saudi Arabia (Yesser) uses a centralised database thereby having low level of confidentiality and trust (Al-Mushayt *et al.,* 2012). The proposed model offers a 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) as shown in figures 3, 4, and 5 respectively.

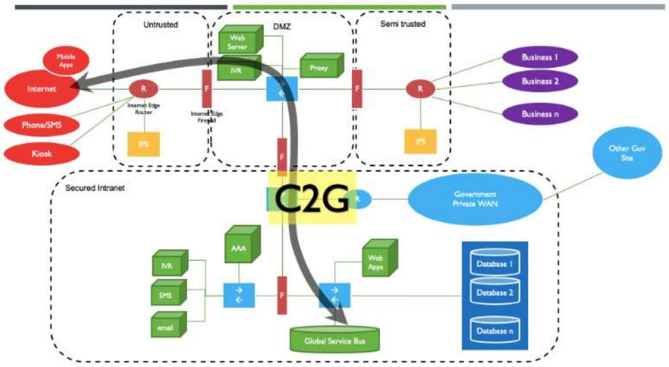

Figure 3. Consumer to Government

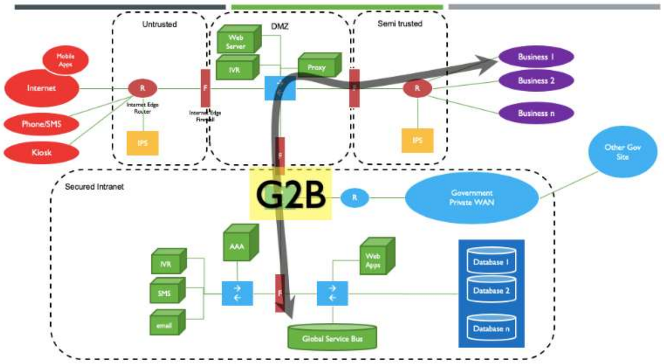

Figure 4. Government to Business

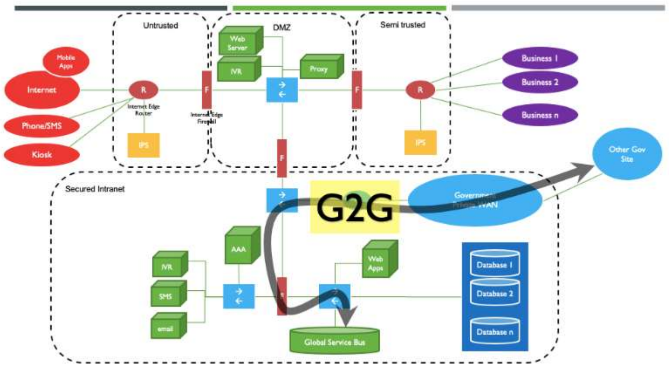

Figure 5. Government to Government

In Figure 3, the government service bus connects directly with internet, mobile apps, kiosk etc. (consumers); in Figure 4, it connects with business providers; and in Figure 5, it connects with a government website (which can be owned by a government agency or ministry). As shown in Figure 2, these three relationships are secured by putting the blockchain technology between DMZ zone and Secured Intranet zone.

V. CONCLUSION AND FUTURE WORK

The study presented in this paper explores most existing literature on securing e-governance systems in different countries. Our study reveals that there are several security and privacy issues 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-Governance system, our 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; have a lack of trust in internet-mediated transactions, and unauthorized access to systems with the help of insiders. To contribute to this growing area of research, this paper proposes a new framework that leverages blockchain to secure e-Governance, using Saudi Arabia as a use case. This proposed model brings decentralisation, access control, confidentiality, and privacy and trust into e-Government service. Also, researchers have not leveraged on blockchain technology to secure Saudi e-Government system in the past.

REFERENCES

AlKalbani, A., Deng, H., & Kam, B. (2015). Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure. *Pacific Asia Conference on Information Systems (PACIS)* (p. 65). AIS Electronic Library (AISeL).

Al-Mushayt, O., Perwej, Y., and Haq, K. (2012). Electronic-government in Saudi Arabia: A positive revolution in thepeninsula.

Alshehri, M., & 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, 42*, 1039-1045.

Bertot, J. C., Gorham, U., Jaeger, P. T., Sarin, L. C., & Choi, H. (2014). Big data, open government and e-government: Issues, policies and recommendations. *Information polity, 19*(1, 2), 5-16.

Choejey, P., Fung, C. C., Wong, K. W., Murray, D., & Xie, H. (2015). Cybersecurity Practices for E-Government: An Assessment in Bhutan. *The 10th International Conference on e-Business (iNCEB2015), November 23rd - 24th 2015* (p. 8 pp). NCEB.

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks* (pp. 1-11). Springer.

Gabriel, B. (2018). E-Governance and Cybersecurity: User Perceptions of Data Integrity and Protection in Ghana, 5th Biennial Social Science Conference of the University of Education, Winneba.

Haran, M. H. (2016). Framework Based Approach for the Mitigation of Insider Threats in Egovernance IT Infrastructure. *International Journal of Science and Research, 3*(4), 5- 10.

Heng, H. (2017). The Application of Blockchain Technology in E-government in China, School of Information Management, Sun Yat-sen University.

Lemuria, C. and Jolien, U. (2018). Blockchain applications in government. Conference Paper. DOI:10.1145/3209281.3209329.

Longzhi, Y., Noe, E., and Neil, E. (2018) Privacy and Security Aspects of E-government in Smart Cities. Department of Computer and Information Sciences, Northumbria University, Newcastle Upon Tyne, NE1 8ST UK.

Mohamed, R. and Rajandran, K. (2017) A Study on Cyber Security in E-Governance With Reference to Areas of Thanjavur District-Tamil Nadu, Asia Pacific Journal of Research.

Moher, D. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. Annals of Internal Medicine, 151, 264.

MyungSan, J. (2018). Blockchain government - a next form of infrastructure for the twenty first century Jun Journal of Open Innovation: Technology, Market, and Complexity.

Osman, I. H., Anouze, A. L., Irani, Z., Al-Ayoubi, B., Lee, H., Balcı, A., .

Weerakkody, V. (2014). COBRA framework to evaluate e-government services: A citizen-centric perspective. *Government information quarterly, 31*(2), 243-256. doi:10.1016/j.giq.2013.10.009

Peck, M. (2017). Blockchains: How They Work and Why They'll Change the World - IEEE Spectrum. *IEEE Spectrum.*

Rehman, M., Esichaikul, V., & Kamal, M. (2012). Factors influencing e-government adoption in Pakistan. *Transforming Government: People, Process and Policy, 6*(3), 258-282.

Rodrigues, G., Sarabdeen, J., & Balasubramanian, S. (2016). Factors that influence consumer adoption of e-government services in the UAE: A UTAUT model perspective. *JIC, 15*(1), 18-39.

Svein, Ø. and Arild, J. (2017). Blockchain Technology as s Support Infrastructure in e-Government, Western Norway Research Institute, Sogndal, Norway.

Swan, M. (2015). Blockchain: Blueprint for a new economy. Newton: O'Reilly Media, Inc.

Weidong, S., Lei, X., Zhimin, G., and Lin, C. (2018). eGov-DAO: a Better Government using Blockchain based Decentralized Autonomous Organization Conference. Avialable at https://www.researchgate.net/publication/325632774

Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly, 27*(1), 49-56.