

Factors Affecting E-Governance Ecosystem for Capital Market in India

Shivkumar Pandey¹, Abhishek Tripathi¹, Davinder Kaur^{1*}

¹Department of Management Studies, CT University Ludhiana, Punjab, 142024

*Corresponding author's email address: drdavinder24220@ctuniversity.in

Article History:

Received: 12-12-2024

Revised: 25-01-2025

Accepted: 05-02-2025

Abstract:

The study investigates factors influencing the e-governance ecosystem in India's capital market, recognizing its critical role in the rapidly expanding Indian stock market. The research aims to create an environment that supports legitimate businesses and investors while deterring unethical practices. The descriptive study was conducted by collecting the primary data through purposive sampling. The sample of 500 capital market employees using a structured questionnaire. The reliability test and exploratory factor analysis are used to examine the data. The findings reveal that the Indian capital market significantly impacts corporate governance by enforcing management procedure regulations. While legal frameworks are essential, the capital market can effectively reward or penalize companies based on their governance practices, provided sufficient accountability and transparency exist. The market's governance function can mitigate agency issues by disciplining management and enhancing overall firm governance. This research contributes to the understanding of e-governance in India's capital market, offering insights into its potential for fostering ethical business practices, investor protection, and overall market integrity. The outcomes of the present study have implications for policymakers, regulators, and market participants in shaping effective e-governance strategies for the evolving Indian capital market landscape.

Keywords: Capital Market, e-Governance, Ecosystem, India, Stock Market.

1. Introduction

E-governance seems vital in the modern era, particularly in the Indian stock market, which has experienced tremendous growth in the last ten years. The main objective should be to foster an environment that is supportive of lawful business owners and investors while regulatory intrusion. Indian capital market is made up of three axes that together form a "golden triangle" for average investors. The first axis is government policy and regulation; major actions taken during the 1990s included the establishment of SEBI, NSE, and NSDL, the removal of the administered pricing regime, the adoption of online trading, and the shift to dematerialization of shares. The second axis is the NSE benchmarking in Indian conditions, which reduced settlement period from 14 days to 5 and now to 3, as well as the cost of transaction drastically dropping from 5% to about 0.15%. The market put pressure on BSE to switch to IT-based trade and procedures as well. These two significant Indian stock exchanges gave international investors a platform to work on, allowing for the quicker interchange of information, the search for new price levels, and market alignment with other countries. This

phenomenon is only observed when information technology is used as a means of transaction facilitation and information sharing. The firms that are listed or anticipated to be listed on stock exchanges and have the ability to issue capital make up the third axis. Their financial strategy, the relative cost of capital in the primary market, and the costs of intermediaries like banks in India and other nations all play a role in this. When making any decision, whether to enter or remain in the capital market, macro and micro aspects pertaining to their turnover and earnings per share (EPS) are crucial. The triangle's surround has made investors more aware of overall risk, particularly on the Indian market where it is in line with worldwide trends. The market, made possible by eGovernment, has reduced reliance even on outside information while also improving efficiency. It is tough for the average investor to maintain

2. Review of Literature

Hassan G Rasha and Khalifa O Othman (2016) communicated their view that e-government sites require further developed and secure e-government organizations to safeguard delicate information from blossoming security dangers and dangers that could incorporate unapproved admittance to assets, pernicious harm, and information capture. These security chances incorporate digital assaults, infections, and crucial data spillages. They have recommended a system to help the most recent arising electronic states and the status of the country. All things considered, particularly in non-industrial nations, offering a completely reliable correspondence between the public authority and the residents of the country.

Fernandes Lynn and Shetty Annapoorna (2016) focused on the significant difficulties in carrying out e-Administration in the nation and the twelfth five-year plan in this circle. These activities help residents as well as different associations in giving vehicle administrations, online installment of bills and expenses, observing of public complaints, land record the board, and administrations in the medical services and training areas. It is a potential instrument that, when utilized proficiently, can lessen debasement to an exceptionally enormous degree. A portion of the central concerns of safety, protection, and absence of coordinated benefits and between operability, security, and absence of incorporated administrations have ended up being significant purposes behind the disappointment of such tasks. Notwithstanding, these issues can undoubtedly be handled with the assistance of computerized instruments that are accessible for observing and monitoring the undertakings, cost administration, quality checks, and booking. The twelfth five-year plan recommends the improvement of this field in both metropolitan and rustic regions by furnishing them with better and bother free administrations.

Harrison S. and JanickeHelge (2016) contrasted customary programming improvement procedures and Lithe philosophy. As per them, security has been seen as a blocker that decelerates an undertaking, at times carrying the venture to a crushing end. This can, and all the more habitually does, have the unfortunate impact of debilitating security and permitting weaknesses to be missed. Accordingly, organizations need to engage with security strategies right all along of the revelation stage and not close to the furthest limit of the advancement cycle on the grounds that any postpone in distinguishing the weaknesses would prompt more work to be exhausted combined with both valuable time and assets that would be expected to determine the security issues.

Chen et al. (2016) utilized a help vector machine to recognize inconsistencies utilizing compressive testing. To distinguish oddities, one needs to manage a lot of information; specifically, the procedures of identifying interruption recognition need to recognize all organization information. Assuming that the information aspect is decreased in the information testing stage and the component information of the organization information are gotten consequently, the productivity of identification can be significantly moved along. A packed examining strategy has been utilized in compacted detecting hypothesis to carry out highlight pressure for stream in network information so that upgraded meager portrayal can be gotten. Then, SVM is utilized to order the pressure results. The proposed procedure has been shown to be proficient in recognizing the way of behaving of organization abnormalities rapidly without decreasing the arrangement exactness. Consequently, the SVM has been shown to be effective in identifying irregularities in the organization. Accepted relationship investigation (CCA) has been utilized for dimensionality decrease and has been shown to be preferable over regular methodologies.

Kumar, D., and Panchanathan, N. (2015) pondered the legitimate prerequisites of network safety and offered a complete e-Administration drive. Activities for getting data and IS would be expected at different degrees of E-administration, which requires a wide scope of regulative changes, including electronic marks, electronic chronicling, information coordinating and opportunity of data, information security, PC wrongdoing, and protected innovation freedoms regulation. As per Kumar and Panchanathan, the onus of getting a properly vigorous regulation that would dissuade and nail down the abuse of the Web and other digital media for any inexcusable exercises' rests with the State. Notwithstanding the activities by the public authority, different partners, for example, network administrations suppliers (ISP), enormous organizations, and little or home clients, are additionally expected to assume their part in expanding the security of the internet inside the country.

A nation's capital market has the power to significantly impact a company by enforcing laws and guidelines pertaining to the company's management procedures. Even while legal and regulatory frameworks are necessary, the capital market has the power to reward or penalise companies based on their governance practices if sufficient accountability and transparency are in place (**Drobotz et al. 2004**). The capital market can use its governance function to punish management and enhance the firm's general governance in order to lessen agency issues. This section of the chapter deals with the elaborations of the different conceptual frameworks given by the researchers in relation to the governance of the capital market in India.

Faizul et al. (2008) presented a Conceptual model on how corporate governance affects a company's ability to obtain financing, its financial performance, and ultimately the growth of the capital market. it demonstrated how a nation's institutional processes, such as its political and economic aspects, legal and regulatory requirements, and markets, have a significant impact on a company's level of corporate governance. Nonetheless, the framework acknowledged that the firm's adherence to the law and its voluntary involvement in corporate governance issues can lower the costs associated with expropriation in the governance process and somewhat offset the inefficiencies of the institutional structures in developing economies. Better firm-level corporate governance, according to the economic approaches to corporate governance, lowers agency costs and raises investors' confidence in the company's future growth and cash flow prospects. This lowers the rate of return that investors were

expecting, which lowers the cost of equity capital for the company. Similarly, better regulated companies should see an increase in their operating and investment performance as a result of lower agency expenses.

Charan Amita (2010) has found that here are four steps that lead to e-governance: transaction, vertical integration, information or cataloguing, and horizontal integration. India has already completed the first, second, and third stages of e-governance and has been successful in putting them into practice. Our nation is currently approaching the hardest fourth stage, which is the one we are most close to reaching. Numerous challenges remain undiscovered, untapped, and untapped. The main obstacles to full-fledged government are social, economic, and geographic divides. Other barriers include illiteracy, a lack of infrastructure, and the security and privacy of financial and personal data. There are eight main components of good governance. Given that India has a mixed economy and public and private organisations engage with one another on a variety of levels, these traits cross over into corporate activities. It guarantees that the presence of corruption is reduced, minority perspectives are considered, and the voices of the most marginalised members of society are heard during the decision-making process. Additionally, it adapts to the demands of society both now and in the future. Reviving effective corporate governance from the bottom up is crucial to maintaining control over the world's largest democracy, India.

3. Objective of the study

- To identify the factors affecting E-governance ecosystem for capital market.

Hypothesis of the study

- **H01:** There are no significant factors affecting E-governance ecosystem for capital market.
- **Ha1:** There are significant factors affecting E-governance ecosystem for capital market.

4. Research Methodology

The existing study is primary and descriptive. The current research chosen purposive sampling for the study. The sample size selected for the study was 500 capital market employees. The responses obtained from structured questionnaire. Reliability test, Exploratory factor analysis was employed for comprehensive data analysis.

5. Results and Discussion

Exploratory Factor Analysis

Principal component analysis was conducted as a means of data reduction, broadly speaking factor analysis provides the tools for analysing the structure of the interrelationship (Correlations) among a large number of variables by defining sets of variables that are highly inter-correlated, are assumed to represent dimensions within the data. Prior to performing PCA, the suitability of data for factor analysis was assessed by following means.

Table 1: Cronbach's Alpha Reliability Statistics (Table: 4.60)

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.912	.912	15

Interpretation: Cronbach's alpha was used to assess the internal consistency of the questionnaire, as it is in the majority of validation studies reported in the literature. Cronbach's alpha was 0.912 in this case, while an alpha value of 0.60 or higher is considered almost acceptable, and values above 0.80 are considered exceptional or good outcomes (Ocak Aktürk et al. 2021). As a result, the findings of the reliability statistics have exceeded the threshold for further factor analysis processing.

Table 2: KMO & Bartlett test results

KMO and Bartlett's Test (Table: 4.61)		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.897
Bartlett's Test of Sphericity	Approx. Chi-Square	13183.730
	df	321
	Sig.	.000

Interpretation: The KMO statistics range from 0 to 1, with values closer to 1 denoting greater adequacy of the factor analysis (KMO \geq 0.6 low adequacy, KMO \geq 0.7 medium adequacy, KMO \geq 0.8 high adequacy, KMO \geq 0.9 very high adequacy). If the result of Bartlett's test is $<$ 0.05, factorial analysis can be used. For the present case the KMO value (.897) is above the acceptable limits & is adequate, while the results of Bartlett's test is $<$ 0.05. Thus, it states that sample is adequate and suitable for the application of factor analysis.

Table 3: SCALE RELIABILITY TEST (using Communalities, Corrected item Correlations, Cronbach's alpha if item deleted, and mean and standard deviations.)

Scale Reliability Test (Table: 3)

Variables	Communalities		Corrected Item total correlation	Cronbach's Alpha if item deleted	Mean	Std Dev.
	Initial	Extraction				
I feel confident that my financial data is secure	1.00	.568	.582	.899	3.19	1.381

when engaging with e-governance systems.						
Organizations in the capital markets are doing enough to protect against cyber attacks.	1.00	.632	.540	.894	3.09	1.302
Adhering to cyber security best practices is important for all users of e-governance systems.	1.00	.719	.542	.894	3.82	1.345
Investing in cyber security ecosystem improves the reliability and stability of e-governance systems.	1.00	.768	.504	.895	3.85	1.398
Adhering to cyber security best practices is important for all users of e-governance systems.	1.00	.613	.430	.897	3.01	1.329
I support increased investment in advanced cyber security technologies for e-governance systems.	1.00	.512	.475	.896	3.62	1.248
I worry that my personal and financial information could be compromised through e-governance systems.	1.00	.663	.482	.896	2.65	1.206
I believe there is a high risk of unauthorized access to my financial accounts through e-governance systems.	1.00	.521	.510	.895	3.25	1.216
A cybersecurity breach could damage my trust in the organizations	1.00	.749	.495	.895	3.04	1.190

providing financial services.						
I am more likely to trust and use online financial services if recommended by friends or colleagues.	1.00	.574	.474	.896	2.24	1.194
I rely on the advice of professionals to guide my decisions regarding the use of online financial services.	1.00	.790	.522	.895	2.14	1.224
The reputation of the organization providing the e-governance service influences my perception of its cyber security.	1.00	.754	.568	.893	2.19	1.204
Accessing e-governance services are easy to use and convenient.	1.00	.686	.544	.894	3.36	1.266
Using e-governance systems allows me to complete my financial tasks efficiently.	1.00	.710	.561	.893	3.99	1.368
Adequate technical support is available when I encounter issues with e-governance systems.	1.00	.745	.594	.892	3.01	1.423
Source: Primary Data						

Extraction Method: Principal Component Analysis

Interpretation: The initial communalities represent the relation between the variables and all other variables (i.e., the squared multiple correlation between the items and all other items) before rotation. The value for communalities using principal component analysis ranged from .568 to .790. here it is admissible to acknowledge that communalities ≥ 0.4 is sufficient for the explanation of construct. All these values show factor analysis has extracted good quantity of variance in the items. Hence all the prerequisites of reliability, validity and one-dimensionality are met.

Table 4: CORRELATION MATRIX OF ITEMS AND VARIABLES OF E-Governance ecosystem

(Table: 4)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1														
2	0.589	1													
3	0.454	0.571	1												
4	0.304	0.219	0.181	1											
5	0.37	0.278	0.118	0.51	1										
6	0.152	0.178	0.284	0.622	0.757	1									
7	0.112	0.2	0.25	0.178	0.154	0.187	1								
8	0.161	0.241	0.202	0.185	0.173	0.203	0.655	1							
9	0.162	0.197	0.253	0.178	0.143	0.121	0.726	0.54	1						
10	0.138	0.265	0.225	0.199	0.16	0.131	0.288	0.296	0.316	1					
11	0.119	0.199	0.259	0.171	0.125	0.192	0.236	0.217	0.142	0.619	1				
12	0.167	0.263	0.251	0.166	0.111	0.182	0.298	0.218	0.181	0.573	0.807	1			
13	0.183	0.249	0.257	0.166	0.074	0.164	0.273	0.277	0.107	0.185	0.119	0.152	1		
14	0.089	0.222	0.169	0.147	0.17	0.239	0.123	0.233	0.118	0.156	0.117	0.171	0.197	1	
15	0.163	0.237	0.236	0.242	0.204	0.238	0.122	0.23	0.1	0.107	0.103	0.189	0.184	0.68	1

Interpretation: This test indicates how each question is associated (Correlated) with each of the other questions. Note that some of the correlations are high and some are low. Relatively high correlations indicate that two items are associated and will probably be grouped together by the factor analysis. Items with low correlations usually will not have high loadings on the same factor. The mean correlation is .389 and it varies from .071 to .807 with a range .736. Thus, there is sufficient correlation to go ahead with the factor analysis. Factor analysis is done using SPSS software with varimax rotated, Principal Component Analysis.

Table 5: FACTOR ANALYSIS (with factor loadings, Eigen values, Parentage of variance and Cronbach’s alpha for each individual factor)

Varimax Rotated Results (Table: 5)

E GOVERNANCE ECOSYSTEM	Factor loadings				
	1	2	3	4	5
F1. ATTITUDE					
I feel confident that my financial data is secure when engaging with e-governance systems.	.858				
Organizations in the capital markets are doing enough to protect against cyber-attacks.	.825				

Adhering to cyber security best practices is important for all users of e-governance systems.	.801				
F2. PERCEIVED USEFULNESS					
Investing in cyber security ecosystem improves the reliability and stability of e-governance systems.		.820			
Adhering to cyber security best practices is important for all users of e-governance systems.		.790			
I support increased investment in advanced cyber security technologies for e-governance systems.		.788			
F3. SOCIAL INFLUENCE (SI)					
I am more likely to trust and use online financial services if recommended by friends or colleagues.			.789		
I rely on the advice of professionals to guide my decisions regarding the use of online financial services.			.765		
The reputation of the organization providing the e-governance service influences my perception of its cyber security.			.655		
F4. PERCEIVED RISK					
I worry that my personal and financial information could be				.840	

compromised through e-governance systems.					
I believe there is a high risk of unauthorized access to my financial accounts through e-governance systems.				.766	
A cybersecurity breach could damage my trust in the organizations providing financial services.				.758	
F5. PERCEIVED EASE OF USE					
Accessing e-governance services are easy to use and convenient.					.837
Using e-governance systems allows me to complete my financial tasks efficiently.					.742
Adequate technical support is available when I encounter issues with e-governance systems.					.722
Eigen values	7.058	3.960	3.283	2.285	1.182
% Of Variance	45.99	15.87	10.27	8.52	5.40
Cronbach's Alpha	.941	.898	.916	.911	.885
<i>Source: Rotated Component Matrix (Primary data)</i>					

Interpretation: The above table shows all the extracted factors with their statements. Factor analysis is used to extract some common factors which describe the entire data set. Principal component analysis with a varimax rotation is applied. Components having eigen value greater than one (1) are retained. These five factors explain 76.136% variance which is considered good. The statements with factor loadings greater than 0.5, are retained. The explanation of various factors emerged from factor solution relating to e-Governance ecosystem in Capital Market is given below.

FACTOR 1. ATTITUDE

The first factor is explaining 45.99% of variance, according to which it can be said that this factor is the most important aspect while deciding about the e-governance acceptance and perception. The factor has an eigen value of 7.01 and Cronbach's alpha value of .941, indicating the results to be valid and relevant. It includes three statements with factor loading ranging from, .858 to .801. the variables included in this factor are: I feel confident that my financial data is secure when engaging with e-governance systems, Organizations in the capital markets are doing enough to protect against cyber-attacks, & adhering to cyber security best practices is important for all users of e-governance. The highest factor loading (.858) was observed for the item, security of the financial data while engaging with e-governance system. Indicating that the attitude toward the secure feeling and the ease of engagement has an impact on the adoption of the e-governance system.

FACTOR 2. PERCEIVED USEFULNESS

This factor accounts for the variance of 15.87, indicating it to be the next relevant and important aspect while considering the e-governance adoption. The eigen value of this factor was 3.96 and Cronbach's alpha of .898, indicated that the results were valid and reliable for further implications. Three statements were there in this factor, which included, Investing in cyber security ecosystem improves the reliability and stability of e-governance systems, Adhering to cyber security best practices is important for all users of e-governance systems & I support increased investment in advanced cyber security technologies for e-governance systems. However, the highest factor loading (.820) was accounted for Investing in cyber security ecosystem improves the reliability and stability of e-governance systems, indicating it to be the most important aspect of the usefulness of the e-governance ecosystem.

FACTOR 3. SOCIAL INFLUENCE

This factor accounted with the variance of 10.27, indicating that this factor can have a more than 10% of the change in the perceptions about e-governance. The Eigen value of 3.28 Cronbach's alpha of .916, highlighted the validity of the results of the factor analysis. Three statements were included in this factor with factor loading ranging from .789 to .655. I am more likely to trust and use online financial services if recommended by friends or colleagues, I rely on the advice of professionals to guide my decisions regarding the use of online financial services, & the reputation of the organization providing the e-governance service influences my perception of its cyber security. However, the highest factor loading of .789 was accounted for the variable, recommendations of the friends and colleagues. Indicating that the adoption of the e-governance is highly dependent on the suggestions of the social environment, in which a person is living.

FACTOR 4. PERCEIVED RISK

This factor accounted with the variance of 8.52, which indicated that this variable has 8.52 % of change power in the overall e-governance system adoption. While the eigen value of 2.285 and Cronbach's alpha value of .911, indicated the results to be relevant and reliable for the further analysis. This factor has three statements with factor loading ranging from .840 to .758. the variables included in this factor are I worry that my personal and financial information could be compromised through e-governance

systems, I believe there is a high risk of unauthorized access to my financial accounts through e-governance systems, & A cybersecurity breach could damage my trust in the organizations providing financial services. However, the highest factor loading was accounted for the variable 'compromise of the personal and financial data through e-governance. Thus, it can be said that although e-governance has many benefits for the public, but the perceived risk about the financial and personal data can limit the access to this system and can result in lack of adoption.

FACTOR 5. PERCEIVED EASE OF USE

This factor accounted for the variance of 5.40, indicating that this factor has the ability of 5% change in the e-governance adoption process. While the results of the eigen value (1.18) and Cronbach's alpha of .885, indicated the results to be valid and reliable for the further analysis. Three statements were included in this factor as Accessing e-governance services are easy to use and convenient, Using e-governance systems allows me to complete my financial tasks efficiently & Adequate technical support is available when I encounter issues with e-governance systems, with factor loading ranging from 837 – 722. However, the highest factor loading was accounted for the variable, accessing e-governance services are easy to use and convenient. Indicating that people prefer the easiness and the convenience while deciding about the adoption of a particular system and operations. Thus, the capital market should look forward to enhancing such ease of use in the system.

Conclusion

For factor analysis of E-governance into the capital market in India, a sample of 500 capital market employees was taken with a total of 15 items. Factor analysis was performed using SPSS software, including a reliability test to find Cronbach's Alpha. Dimension reduction was conducted using Principal Component Analysis as the extraction method. A correlation matrix was created to find similarities among the different items. The analysis concluded with 5 factors accounting for 76.136% of the variance, with the first three factors having variances greater than 10%. These factors have a major impact on the E-governance ecosystem for the capital market in India. The first factors with major impacts are attitude towards ease of use and ease of engagement. The second factor is perceived usefulness, and the third factor is social influence.

References

- [1] Howard, Alexander. "What is a Sybil Attack?" [Online]. Available: <http://www.toptenreviews.com/software/articles/what-is-a-sybil-attack/> [8] M. Dixit. "Future of E-government," *SOCRATES*, vol.4, no.3, 2015
- [2] National Institute for Cyber security Careers and Studies. "Glossary". [Online]. Available: <https://nicscs.us-cert.gov/glossary/>
- [3] Cheriyan, Ruth. Massive Data Breaches and Cyber Threats in India. 2017. [Online]. Available: <http://www.india-briefing.com/news/massivedata-breaches-cyber-threats-india-15405.html/>
- [4] G.N. Thejesh. "Why are Indian Users so Vulnerable to Cyber-attacks?". 2016. [Online]. Available: <https://factordaily.com/why-is-indiavulnerable-to-cyberattacks-bug-bounty-programs-cybersecurity/>

- [5] J. V. Wagenen. Packet Sniffers Threaten Local Government IT. 2018. [Online]. Available: <https://statetechmagazine.com/article/2017/08/packetsniffers-tool-and-threat-local-government-it>
- [6] Techtargt Network. “Denial-of-Service Attack”. 2017. [Online]. Available: <http://searchsecurity.techtargt.com/definition/denial-of-service>
- [7] S. Paliwal and R. Gupta. “Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm”, *International Journal of Computer Applications*, vol. 60, no.19, 2012.
- [8] S. Singh, D.S. Karaulia. “E-Governance: Information Security Issues, International Conference on Computer Science and Information Technology, Pattayya, Dec 2011. [Online]. Available: https://www.researchgate.net/publication/266770761_EGovernance_Information_Security_Issues
- [9] T. Mamatha, Md. Z. Husaain. “Network Security Solutions and Vulnerabilities in E-Government,” *International Journal of Computing and Business Research*, vol. 3, no. 3, 2012. [Online]. Available: <http://www.researchmanuscripts.com/september2012/3.pdf>
- [10] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*. Momentum Press, 2010. Pp-286- 324, ISBN: 978-1-60650-197-9
- [11] R. Sharma. “Gray-hole Attack in Mobile Ad-hoc Networks: A Survey.” *International Journal of Computer Science and Information Technologies*, vol. 7 no. 3, pp-1457-1460, 2016. ISSN: 09759646
- [12] S. Hashemi, K. Monfaredi, and S.Y. Hashemi. “Cloud Computing for Secure Services in E-Government Architecture. *Journal of Information Technology Research*. Vol. 8, No. 1, 2012, pp. 43–61. [Online]. Available: <http://dx.doi.org/10.4018/JITR.2015010104>.
- [13] Celesti, *et. al.* An Approach for the Secure Management of Hybrid Cloud–Edge Environments. *Future Generation Computer Systems*. 2019, pp.1-19.[Online].
- [14] P. Feiler. “Automated Assurance of Security-Policy Enforcement in Critical Systems.” *SEI Insights*. 2018. [Online]. Available: https://insights.sei.cmu.edu/sei_blog/2018/02/automated-assurance-ofsecurity-policy-enforcement-in-critical-systems.html/
- [15] C.H. Malin, *et. al.* Phishing, Watering Holes, and Scareware. In Elsevier: *Deception in the Digital Age*. 2017, pp. 149-166. [Online]. Available: <https://linkinghub.elsevier.com/retrieve/pii/B9780124116306000050>.
- [16] D.C. Pandya and N.J. Patel. “Study and Analysis of E-Governance Information Security (InfoSec) in Indian Context.” *IOSR Journal of Computer Engineering*. Vol.19, no.1 pp-04-07, 2017. [Online]. Available: <http://www.iosrjournals.org/iosr-jce/papers/Vol19-issue1/Version-4/B1901040407.pdf/>
- [17] W. Dormann. “The Consequences of Insecure Software Updates.” *SEI Insights*. 2017. [Online]. Available: <https://insights.sei.cmu.edu/cert/2017/06/the-consequences-of-insecuresoftware-updates>.
- [18] A.D. Householder *et al.* The CERT Guide to Coordinated Vulnerability Disclosure. Software Engineering Institute, Carnegie Mellon University, Rep No. 022, 2017. [Online]. Available: https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_50_3340.pdf/

- [19] Verizon. "The Insider Threats: Protecting the Keys to the Kingdom." 2017. [Online]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breachdigest-2017-insider-threat_xg_en.pdf/
- [20] Verizon. "Data Breach Digest: Perspective in Reality." 2017. [Online]. Available: <http://www.verizonenterprise.com/verizon-insights-lab/databreach-digest/2017/>
- [21] A.C. Tagert. Cybersecurity Challenges in Developing Nations. Ph.D Dissertation. Department of Engineering and Public Policy, Princeton University, Pittsburg, 2010. [Online]. Available: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1021>