International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A Decentralized E-Government Architecture Integrating Blockchain and Artificial Immunity for Enhanced Security

[1]Eman Afroz Munir Ahmad Momin, [2]Sujata. A. Gaikwad
[1,2]TPCT'S College of Engineering, Osmanabad
[1]emanafroz25@gmail.com, [2]sujatagaikwad414@gmail.com

Abstract: With the ever growing tide of e-Government services in the current fast-paced digital government world, there is the need to implement better mechanisms on the protection of data privacy and system security. The old centralized e-Government systems are usually vulnerable and prone to failure which can be exploited by cyberattacks and malicious intrusions. In response to these weaknesses, the paper will introduce a decentralized e-Government model that combines blockchain technology with a threat detection model based on artificial immune system (AIS). The suggested solution can utilize the encryption and immutability features of blockchain and distributed verification to improve the privacy and integrity of government data. At the same time, the integration of AIS provides the framework with the resilience to internal and external threats because malicious activities are dynamically detected and prevented. The framework developed and tested in the Ethereum environment proves that the proposed framework is applicable to mitigating possible security threats without jeopardizing the confidentiality of sensitive data. This study can assist in creating the next generation of secure and privacy-preserving e-Government design, which builds upon the principles of decentralization, intelligent threat detection, and blockchain-based assurance to increase the level of trust and transparency in the delivery of public services.

"Index Terms: e-Government, blockchain, artificial immune system, insider threats, privacy protection".

1. INTRODUCTION

Electronic Government (e-Government) systems have become critical tools in the current governance, through applying digital technologies to provide citizens, businesses and government agencies with the services they need. The implementation of digital transformation programs by e-Government leads to the increase in efficiency, transparency, accountability, and participation of stakeholders, which contributes to greater access to the public services without the constraints of getting physically present. The digital transformation is a significant factor towards inclusivity and responsiveness of government processes, which guarantee that all populations have equal access to services.

Though these are the benefits, e-Government systems still continue to encounter grave threats especially in regard to data privacy and system security. The perpetual weaknesses in terms of data theft, unauthorized disclosures, and advanced cyberattacks against government systems have been demonstrated in various cases around the world. Such problems are normally due to the mismanagement of data, ineffective security measures, or intentional use of vulnerabilities in the system.

Majority of the current e-Government systems are based on centralized architectures in which data storage and processing are all based on central servers.

Even though centralization enables administrative control, it brings about one point of failure making it more vulnerable to cyber attacks such as malware, denial-of-service (DoS), and distributed denial-of-service (DDoS). Besides external intrusions, insider threats, which are caused by authorized users who may have bad intentions, are relatively a challenging issue, since they may quite often escape the classical detection systems.

To address such challenges, the current research suggests a blockchain-based decentralized e-Government design, exploiting the qualities of blockchain technology transparency and immutability and cryptography to ensure security. With this architecture, the information is spread in a peer to peer network where the transactions are encrypted safely and stored in an immutable registry. This type of decentralization removes the presence of single points of failure and greatly enhances the integrity and resilience of data.

In addition, the suggested scheme incorporates an Artificial Immune System (AIS) of smart anomaly detection. AIS is inspired by biological immune system and offers adaptable and decentralized approaches to the detection and response to possible intrusion. Particularly, self-organizing and scalable features of the Dendritic Cell Algorithm (DCA) as a type of AIS are applicable to tracking dynamic network environments (including those within e-Government ecosystems).

In this study, DCA is used in the blockchain model to detect abnormal or malicious traffic such as ransomware, spyware, worms, and spam, and, therefore, avoids storing harmful traffic information on the government blockchain. A combination of security guarantees of blockchain and adaptive defense of AIS lead to a resilient, privacy-abiding e-Government system.

Overall, the paper provides a decentralized e-Government model that is supported by the use of blockchain and AIS. The suggested system will improve information security, citizens trust and guarantee integrity and confidentiality of citizen data-major weaknesses of the conventional centralized e-Government architectures.

2. LITERATURE SURVEY

Electronic Government (e-Government) transformation has been sufficiently explored on different fronts such as adoption, implementation, data privacy, and security. This section discusses the important academic work that has contributed to the vision of secure and privacy-conscious e-Government systems, paying especially close attention to the cultural aspect, cybersecurity issues, and blockchain-based innovations.

Carter and Weerakkody (2008) examined the implementation of e-Government in the cross-cultural perspective, and they have highlighted that cultural perceptions and societal ethics determine the success and adoption of digital governance programs to a large extent [1]. Their results indicate that during the implementation of e-Government solutions, it is important to have culturally adaptive approaches that can make it inclusive and engaging to the user in various regions.

Yang, Elisa, and Eliot (2019) reviewed the privacy and security concern of e-Government systems in the framework of smart cities [2]. Their publication highlights that since urban space is becoming

interconnected with digital services, and infrastructures, the risks to the privacy of citizens and to the security of systems are becoming increasingly imperative, demanding all-encompassing protection and oversight systems.

Palanisamy and Mukerji (2014) also examined the security and privacy concerns that are inherent to the e-Government infrastructures [3]. The focus on their agendas was on the issues of data protection, information sharing between agencies, and the weakness in cyber defense systems. Their work gives a background of how the multi-layered security requirements are to be achieved to ensure that efficient e-Government systems are achieved.

Elisa, Yang, Chao, and Cao (2018) in an influential work proposed a blockchain-based framework that would support the privacy and integrity of the e-Government processes [4]. Their model using the decentralized and immutable properties of blockchain provides a secure platform of storing and verifying transactions of the government, which is a great step towards guaranteeing trust and transparency in government administration.

In organizational and governmental environments, the Verizon Insider Threat Report (2019) has also made an emphasis on the increased number of insider threats [6]. These insider threats are not detected by most cyberattacks; unlike traditional cyberattacks, they are detected by authorized users (though they are legitimate and authorized). This result highlights the need to establish smart threat detection technologies that can counter internal risks.

Continuing with the strengths of blockchain, Elisa, Yang, Li, Chao, and Naik (2019) explored the use of consortium blockchain models in e-Government systems to protect privacy [7]. Their research established the ability of multiple government bodies to work together using a certified blockchain to strike a balance between transparency, trust, and data confidentiality.

Nnko (2020) suggested the decentralized e-Government system that would enhance the privacy and security [8]. The study has highlighted the benefits of decentralization in terms of dependency on central servers, hence lessening the single points of failure and improving the data protection mechanisms.

In another study conducted by Elisa et al. (2019), the importance of consortium blockchain was restated in providing security and privacy in e-Government infrastructures [11]. Their work supported the idea that decentralized trust models may be used to achieve secure inter-departmental collaboration and not violate the integrity or confidentiality of data.

All these studies are significant in driving the point that as promising as e-Government can be in streamlining its administrative operations and involving its citizens, it has its challenges in terms of security and privacy that have continued to resurface. The recent trends in research show that there is an increased interest in implementing blockchain and other decentralized technologies to enhance resilience in the system. These innovations, combined with smart security solutions, are set to make e-Government systems more open, secure and citizen-friendly digital governance systems.

3. METHODOLOGY

a) Proposed Work :

The suggested study presents a decentralized e-Government model, which combines blockchain technology and artificial immune system (AIS) to address the drawbacks of the conventional centralized models. Today the centralized models usually have single points of failure and are not very resilient, thus, they are extremely susceptible to cyber threats, data breaches, and insider attacks.

The framework can provide a strong degree of data protection by using the blockchain technology [7–13], which will guarantee encryption, validation, and unchangeable record maintenance. Any operation of the system is properly recorded on a distributed ledger where unauthorized modifications or changes cannot occur and there are less chances of manipulating information or hacking the system. The decentralized system also increases the continuity and fault tolerance of the services provided so that e-Government functions will not cease in case of localized system failure or cyber attacks [1].

Moreover, individual data of citizens are encrypted and only accepted by authorized organizations, which will not violate the principles of privacy and reduce the possibility of unauthorized access to this information. It is both a way to make the system strong against external pressure and a way to create the model of trust between the citizens and the digital governmental services.

In order to build up the defense mechanism, the system considers Artificial Immune System (AIS) based on the biological immune processes. This security layer is an adaptive type of security layer that keeps track of the activities on the network and identifies anomalies and countermeasures possible threats, including insider-based attacks. The combination of the immutability of blockchain with the self-learning ability of AIS will make the framework dynamically prevent threats and increase the system integrity.

The proposed model therefore offers a robust, smart and privacy protecting e-Government infrastructure that guarantees the confidentiality, authenticity and reliability of transactions of the public services.

b) System Architecture:

The suggested system architecture includes three main elements Government Authorities, Blockchain Infrastructure and Citizens of which each integration will play a part in safe data control, service provision, and openness in the e-Government framework.

1.GovernmentComponent:

This layer is handled by the authorized government officials who verify the information of the citizens. The system enables the authorities to enter, modify, and authenticate data about the citizens using a secure interface. The algorithms of advanced machine learning and artificial intelligence like Decision Tree, Naive Bayes, Support Vector Machine (SVM), Random Forest, Artificial Neural Network (ANN), and the suggested algorithms based on Genetic Features and XGBoost are used to analyze and check the authenticity of the received data. Upon processing, the system carries out a details-matching operation- in case of anomaly, the possible vulnerabilities, or malicious entries are highlighted; otherwise, normal system runs do not interrupt.

2..**Blockchain Layer:**

The blockchain element will ensure that all transactions, data entries, and artificial intelligence products are safe-stored in an unchangeable and transparent registry [9]. It is decentralized, which makes it unalterable and improves accountability and makes all the activities in the system traceable. The data blocks are cryptographically chained together and there is a verifiable and auditable history of operations. This layer is the foundation of the whole framework, which ensures data integrity, fault tolerance, and reliability among the government entities.

3.CitizenInterface:

The citizen element gives the people access to their records and details of the services secured. The citizens are able to check their data presented on the View Details module and monitor the activities they are involved in in relation to services. This facilitates responsibility and gives the citizens the power to keep checks on the use and management of their data.

A combination of these elements is what will allow governmental authorities to handle and analyze the data about citizens efficiently and blockchain-based technology will offer security and transparency. The citizens, in their turn, have the advantage of having a direct, safe access to their information, which further builds trust, efficiency, engagement in online governance.

c) Modules:

The e-Government system proposed is implemented in a number of functional modules that together provide safe data management, effective processing and easy access. Each of the modules will be aimed to provide an increase in the security, usability, and reliability of the framework.

A) Government Authority Login

This module is a secure authentication interface that gives authorized government officials access to the system to manage the information related to citizens in the system. The authentication system allows only the certified staff to carry out administrative functions, which helps to preserve the confidentiality of data and adherence to regulations. With this interface, government officials can effectively control, update and authenticate sensitive data and therefore facilitating smooth governance and accountability.

i) Add Citizen Details

This sub-module will allow the authorized officials to register and keep detailed records of citizens, both personal and verification. All the data records are highly encrypted and stored in the blockchain to be accessed and audited later on. The system will increase accuracy, reduce redundancy, and consistency across departments by consolidating the data of citizens in a secure distributed ledger. Digital governance standards are adhered to in keeping privacy and protection of sensitive data.

ii) View Details

View Details module enables governmental authorities to access and confirm the information of its citizens effectively. To promote informed decision-making and efficient service delivery, the officials can use the updated records to facilitate the need to establish effectiveness and authenticity.

This step improves transparency and accountability of operations, as well as enables the cross-checking of the information stored in the blockchain.

iii) Train Artificial Intelligence Algorithms

This module is used to test machine learning and artificial intelligence (AI) models with the help of related datasets to differentiate between valid and suspicious activities. The trained algorithms include Decision Tree, Naive Bayes, SVM, Random Forest, ANN, and XGBoost (with genetic feature optimization) to be able to detect anomalies and likely intrusion, as well as classify network behaviours. Ongoing learning guarantees that the algorithms are adjusted to new patterns of the threats, which increases the accuracy and resilience of the systems to cyberattacks.

iv) Test AI Algorithm

The Test AI Algorithm module is used to assess the model performance after training and it uses live or simulated data streams. This testing phase exclusively checks that the algorithm is correct in identifying irregular activities, anticipating attacks, and differentiating legitimate requests and the malicious requests. The lessons learned in the process are deployed to make the system more refined, allowing maximum reliability and proactive threat detection of e-Government networks.

B) Citizen Login

The Citizen Login module offers a safe portal of access to citizens by the use of government-issued identification numbers or digital credentials. This process of authentication will provide the assurance of the verified access to e-Government services as well as privacy and integrity of data. With the help of this module, citizens have an opportunity to engage directly with government services, control their data, and engage in digital governance safely and easily.

1) View Your Details

This sub-module enables citizens to check and verify their personal data in the blockchain. It provides the transparency of allowing human beings to confirm whether their information is correct and not altered. The convenient user interface will enhance confidence between the citizens and the government authorities as the user will have the capability to track their data usage and service history with complete privacy protection.

All in all, the combination of these interrelated modules will guarantee a solid, secure, and user-friendly framework of the e-Government activities. Combining blockchain and AI technologies will enhance the efficiency of the system and transparency, as well as the engagement of citizens through enhanced security.

d) Blockchain Integration

The proposed e-Government framework is based on the introduction of the blockchain technology which guarantees the safety of the data, its transparency, and impossibility of any changes in the course of all transactions. The decentralized

architecture of blockchain spreads information across a variety of network nodes that eradicate points of failure and minimize the potential occurrence of unauthorized manipulations or loss of data.

All information, be it about citizen, government, or AI generated is presented as a block on the distributed ledger. Each block has its own cryptographic hash, which is produced with the help of the mechanism of SHA-256 (Secure Hash Algorithm 256-bit). This hashing mechanism means that any change in the content of a block automatically changes the value of a hash, and this will immediately indicate that there is some form of tampering. As such, blockchain makes it possible to confirm data integrity and ensure that all the information stored is authentic and has not been modified.

Since blockchain is based on a peer-to-peer network, with a blockchain all nodes will be involved in the verification of the transactions prior to the addition to the chain. Such a process that is done by consensus is more reliable and ensures that unauthorized or corrupted information is not included. The distributed blockchain nature provides resiliency and availability of the systems even during node failures or server failures.

The encryption and access control capabilities of blockchain provide an additional protection of sensitive citizen and government data. Access to and amendments of certain records is limited to verified and authorized individuals, which guarantees confidentiality and the sharing of data under control.

Secondly, smart contracts are also important in automating e-Government operations. These self-run code scripts are rules that are preset and therefore automatically authenticate and execute transactions without a mediator of such transactions. Citizen identities can be known and authenticated via smart contracts, making sure that there is accuracy, consistency, and trust in digital public services.

Integration of blockchain, in this model, provides a reliable and secure digital ecosystem that cannot be tampered with by the e-Government application, as it is immutable, transparent, and is verified automatically. Not only does it ensure confidential information, but it also improves efficiency, responsibility and citizen trust in government administration.

4. EXPERIMENTAL RESULTS

In order to prove the usefulness of the decentralized e-Government model, a prototype has been created and deployed with the help of blockchain and artificial intelligence (AI) technologies. The experimental system exhibits the functionality of the system, user interaction interfaces and general performance of the system in different modules.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Fig 2 Home Page

Figure 2 represents the Home Page, as the main portal of both the citizens and the government entities. It offers safe navigation to the different portals of the logins making sure that only the authenticated users have access to the system.

Fig 3 Government Authority Login Screen

Figure 3 shows the Government authority login screen wherein authorized personnel can safely log in to manage and authenticate citizens information. With the successful authentication access, the user is able to access several administrative functions of the system.

Fig 4 Add Citizen Details

Figure 4 represents the Add Citizen Details screen, through which the government officials can add new citizen records and store them. After data entry and verification are done successfully, a confirmation message will be displayed (as in Figure).

Fig 5 Citizen Details are Added Successfully

Figure 5) signifies that the citizen record is safely stored in the blockchain.

Fig 6 View Details

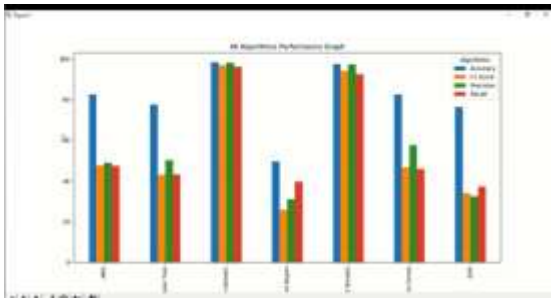

Figure 6 introduces View Details module where authorized officials are able to access and confirm stored data of citizens. This is an aspect that guarantees transparency and easy keeping of records.

Fig7 Train Artificial Intelligence Algorithms Graphs

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

Figure 7 illustrated the Train Artificial Intelligence Algorithms phase, showing the graphical results that were obtained following the training of different AI algorithms, such as Decision Tree, Random Forest, and ANN algorithms. These models are tested according to their ability to identify anomaly and the ability to identify legitimate and malicious requests.

Fig8 Performance Evaluation Table

The **Performance Evaluation Table in Figure 8,** shows the performance and efficiency of the tested algorithms in predicting performance. The review outcomes validate that there is an improvement in the general accuracy and detection rate of models when genetic features optimization is integrated.

Fig9 Test AI Algorithm

Figure 9 Figure 9 presents the Test AI Algorithm module, according to which trained models are tested with the help of test datasets to evaluate their possibilities to detect possible attacks and to protect blockchain integrity.

Fig10 Citizen Login

Fig11 View Your Details

Figures 10 and 11 represent the Citizen Login and View Your Details interfaces on the citizen side. These characteristics enable citizens to safely log in, access their personal records as well as ensure that information in the blockchain network is accurate.

On the whole, the results of the experiment confirm that the framework under consideration is efficient in all modules. The blockchain integration provides the

safety and impossibility of data modification, whereas the application of the AI-driven anomaly detection helps to enhance the resilience to insider and external attacks even more. These findings affirm that the system has been able to create a balance between security, privacy and accessibility in provision of digital public services.

5. CONCLUSION

This study offers a safe and privacy-saving e-Government model that unites blockchain technologies with artificial intelligence (AI) to overcome the drawbacks of traditional centralized systems. The suggested model contributes to improvement of data integrity, confidentiality, and resilience of systems significantly by decentralizing data storage as well as the use of immutable ledger mechanisms.

The framework complies with cryptography, smart contracts, and distributed consensus solutions to ensure that the work of the government services is transparent and secure. The system is further reinforced by the usage of AI algorithms, especially in detecting anomalies and pattern recognition with the ability to detect and contain possible security risks such as insider and external attacks.

Experimental testing of the system revealed that the joint application of blockchain and AI, in addition to enhancing the security system, also elevated the efficiency and reliability of the government digital services. The secure citizen login and verification module will provide greater comfort to the users facilitating safe and convenient access to the necessary services.

All in all, this article demonstrates the potential of blockchain and AI-based defense mechanisms integration as a way to transform the e-Government infrastructures. The offered strategy helps to create a credible, open, and robust digital governmental infrastructure and opens the way to the future of safe citizen services markets.

6. FUTURE SCOPE

The implementation of new technologies such as AI and Internet of Things (IoT) and distributed ledger technology (DLT) can contribute greatly to e-Government systems. In the future, the research might explore applications to the blockchain and these technologies to create synergies that allow new applications including smart governance, predictive analytics, and autonomous decision-making. With the help of AI to analyze data and IoT to monitor events in real-time and DLT to perform safe and open transactions, it becomes possible to reach even greater efficiency, transparency, and responsiveness with e-Government systems. Such integration of technologies can bring a breakthrough to the governance process, creating more proactive, data-oriented, and citizen-centered ways of managing the state.

REFERENCES

[1] L. Carter and V. Weerakkody, ‘‘E-government adoption: A cultural comparison,’’ Inf. Syst. Frontiers, vol. 10, no. 4, pp. 473–482, Sep. 2008.

[2] L. Yang, N. Elisa, and N. Eliot, ‘‘Privacy and security aspects of E-government in smart cities,’’ in Smart Cities Cybersecurity and Privacy. Amsterdam, The Netherlands: Elsevier, 2019, pp. 89–102.

[3] R. Palanisamy and B. Mukerji, ‘‘Security and privacy issues in E-government,’’ in Cyber Behavior: Concepts, Methodologies, Tools, and Applications. Pennsylvania, PA, USA: IGI Global, pp. 880–892, 2014.

[4] N. Elisa, L. Yang, F. Chao, and Y. Cao, ‘‘A framework of blockchain-based secure and privacy-preserving E-government system,’’ Wireless Netw., vol. 24, pp. 1–11, Dec. 2018.

[5] J. Glasser and B. Lindauer, ‘‘Bridging the gap: A pragmatic approach to generating insider threat data,’’ in Proc. IEEE Secur. Privacy Workshops, May 2013, pp. 98–104.

[6] (2019). Verizon Insider Threat Report. Accessed: Mar. 22, 2020. [Online]. Available: https://www.verizon.com/about/news/verizon-refocuses-cyberinvestigations-spotlight-world-insider-threats/

[7] N. Elisa, L. Yang, H. Li, F. Chao, and N. Naik, ‘‘Consortium blockchain for security and privacy-preserving in E-government systems,’’ 2020, arXiv:2006.14234.

[8] N. E. Nnko, A Decentralised Secure and Privacy-Preserving E-Government System. Tyne, U.K.: University of Northumbria at Newcastle, 2020.

[9] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, ‘‘Consortium blockchain for secure energy trading in industrial Internet of Things,’’ IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3690–3700, Aug. 2017.

[10] S. Underwood, ‘‘Blockchain beyond bitcoin,’’ Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.

[11] N. Elisa, L. Yang, H. Li, F. Chao, and N. Naik, ‘‘Consortium blockchain for security and privacy-preserving in E-government systems,’’ in Proc. ICEB, 2019, pp. 99–107.

[12] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, ‘‘Consortium blockchains: Overview, applications and challenges,’’ Int. J. Adv. Telecommun., vol. 11, nos. 1–2, pp. 1–14, 2018.

[13] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Decentralized Bus. Rev., Manubot, Tech. Rep. 21260, 2008.

[14] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Sebastopol, CA, USA: O’Reilly Media, 2014.

[15] J. Greensmith, U. Aickelin, and S. Cayzer, ‘‘Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection,’’ in Proc. Int. Conf. Artif. Immune Syst. Springer, 2005, pp. 153–167.

[16] Z. Chelly and Z. Elouedi, ‘‘A survey of the dendritic cell algorithm,’’ Knowl. Inf. Syst., vol. 48, no. 3, pp. 505–535, Sep. 2016.

[17] N. Elisa, L. Yang, X. Fu, and N. Naik, ‘‘Dendritic cell algorithm enhancement using fuzzy inference system for network intrusion detection,’’ in Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE), Jun. 2019, pp. 1–6.

[18] A. Deshpande, P. Nasirifard, and H.-A. Jacobsen, ‘‘EVIBES: Configurable and interactive ethereum blockchain simulation framework,’’ in Proc. 19th Int. Middleware Conf. (Posters), Dec. 2018, pp. 11–12.

[19] N. Moustafa and J. Slay, ‘‘UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),’’ in Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), Nov. 2015, pp. 1–6.

[20] J. R. Gil-Garcia, S. S. Dawes, and T. A. Pardo, ‘‘Digital government and public management research: Finding the crossroads,’’ Public Manage. Rev., vol. 20, no. 5, pp. 633–646, May 2018.

[21] E-Government in Support of Sustainable Development/UN Department of Economic and Social Affairs, United Nations E-Government Survey 2014, New York, NY, USA, 2016.

[22] M. Stefanova, S. Stefanov, and O. Asenov, ‘‘Identity protection accessing E-government through the biometric authentication methods,’’ in Proc. 6th IEEE Int. Conf. Intell. Syst., Sep. 2012, pp. 403–408.

[23] V. Ndou, ‘‘E–government for developing countries: Opportunities and challenges,’’ Electron. J. Inf. Syst. Developing Countries, vol. 18, no. 1, pp. 1–24, 2004.

[24] V. Buterin, ‘‘A next-generation smart contract and decentralized application platform,’’ White Paper, vol. 3, no. 37, pp. 1–2, 2014.

[25] C. Cachin, ‘‘Architecture of the hyperledger blockchain fabric,’’ in Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers, vol. 310, 2016, pp. 1–4.

[26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ‘‘An overview of blockchain technology: Architecture, consensus, and future trends,’’ in Proc. IEEE Int. Congr. Big Data (BigData Congress), Jun. 2017, pp. 557–564.

[27] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, ‘‘Blockchain for industry 4.0: A comprehensive review,’’ IEEE Access, vol. 8, pp. 79764–79800, 2020.

[28] D. Di Francesco Maesa and P. Mori, ‘‘Blockchain 3.0 applications survey,’’ J. Parallel Distrib. Comput., vol. 138, pp. 99–114, Apr. 2020.

[29] A. A. Monrat, O. Schelén, and K. Andersson, ‘‘A survey of blockchain from the perspectives of applications, challenges, and opportunities,’’ IEEE Access, vol. 7, pp. 117134–117151, 2019.

[30] M. Jun, ‘‘Blockchain government—A next form of infrastructure for the twenty-first century,’’ J. Open Innov., Technol., Market, Complex., vol. 4, no. 1, p. 7, Dec. 2018.

[31] M. Kuperberg, S. Kemper, and C. Durak, ‘‘Blockchain usage for government-issued electronic IDS: A survey,’’ in Proc. Int. Conf. Adv. Inf. Syst. Eng. Springer, pp. 155–167, 2019.

[32] C. Sullivan and E. Burger, ‘‘E-residency and blockchain,’’ Comput. Law Secur. Rev., vol. 33, no. 4, pp. 470–481, 2017.

[33] Dubai Blockchain Strategy, Smart Dubai, Dubai Government, Dubai, United Arab Emirates, Dec. 2016.

[34] (2016). Blockchain Project in USA. Accessed: May 27, 2020. [Online]. Available: https://consensys.net/blog/enterprise-

blockchain/which -governments-are-using-blockchain-right-now//

[35] (2018). Blockchain Project in Canada. Accessed: Mar. 22, 2020. [Online]. Available: https://bitaccess.ca/blog/government-of-canada-ipfs///

[36] (2017). Blockchain Project in Mexico. Accessed: May 22, 2020. [Online]. Available: https://www.gob.mx/cidge/acciones-y-programas/blockchainhackmx/

[37] (2019). Blockchain Project in Argentina. Accessed: May 22, 2020. [Online]. Available: https://www.bloomberg.com/press-releases/2019-08-26/nec-idb-lab-and-ngo-bitcoin-argentina-to-deploy-a-blockchain-ba/

[38] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, ‘‘Intrusion detection system: A comprehensive review,’’ J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013.