



A Decentralized E-Voting System.

¹Ritik Chauhan, ²Usha K, ³Rishabh Srivastava, ⁴Pratham Jaiswal, ⁵Rajat Manwal

¹U.G Student, ²Assistant Professor, ³U.G Student, ⁴U.G Student, ⁵U.G Student

¹Computer Science and Engineering,

¹JSS Academy Of Technical Education, Noida, India

Abstract: As a citizen, casting a ballot is both a right and an obligation. Every person has the chance to vote for the representatives who will speak for them when it comes to the requirements and recommendations of the populace. Elections are the method used to choose these MPs. The way of giving of vote with existing system OLD (Paper based) and traditional (Electronic Voting Machine) is not much secure. The problem with existing system is that centralized architecture, attack prone and not trustable. The need of Decentralized voting system is to increasing security, quickness, protection. This paper explores the way to recognize voting problem and provides solution of that security problem through Blockchain Technology.

Index Terms - blockchain, e-voting, electronic voting, Ethereum

I. INTRODUCTION

Every democracy is built on the foundation of voting. Everyone in the nation has an equal say in who leads them in this decision-making process. As a result, picking the correct national leader is crucial. For citizens to choose their representatives, a country must have an impartial election process.

OLD (Paper Based) elections were conducted using a ballot paper where People marked the candidates and submitted the ballot papers at the voting stations. These ballot papers were counted and managed manually which resulted in a huge delay in the election process. Although this method of conducting elections was very simple, it did not much more secure. Numerous problems are being faced by voters, including booth capture, a long line in front of the voting booths, fraudulent voting, and time-consuming procedures. Thus, replacing the pen-paper based voting system by using a new electron system had to the potential to limit fraud and make the voting process verifiable[1].

This Problem was solved by the Election Commission of India by introducing Electronic Voting Machines (EVMs) in the year 1990. This device was cheap, easy to use and had a simple design. EVMs were consequently extensively used across the nation. EVM recently increased frauds in the 2009 parliamentary elections because it doesn't address any security issues and has issues with universal approval. This has raised various concerns in the minds of the citizens regarding the election process in the country. Anyone with the basic knowledge of electronics can disturb the mechanism of the EVM which in turn could disrupt the entire election process. As a result of this, the authorities have been forced to look for other reliable Voting Procedure. I-voting and e-voting are the two varieties of automatic voting. I-voting involves using an internet browser to cast a ballot, while e-voting involves using a voting machine. Although, concept of i voting solve various problem faced by the traditional system, but not provide security for the voters [1][2].

Blockchain is immutable, robust and trustable technology that includes blocks of data linked using cryptography. Blockchain was developed by Satoshi Nakamoto [3] as a medium to secure online transactions. Blockchain provides as a highly secure method of storing data by providing proof of work and decentralized using peer-to-peer networks. If someone wants to tamper with the data, the hash value gets changed and the link is broken. To make the attempt successful, the attackers needs to change and recalculate the hashes of

subsequence blocks. Each block, when created, is curated by the users and based on their consensus and the block may be added or rejected. Hence the blockchain provides Security, Immutability and Transparency.

1.1 Related Work

Satoshi Nakamoto [3] first used blockchain, a reliable, unchangeable, and trustworthy technology, in 2008 to establish the idea of cryptocurrencies, or bitcoins, as a safe way to exchange money. Numerous studies have demonstrated the wide range of uses, including Bitcoin, banking, healthcare, and cyber security. Electronic voting systems are one example of how blockchain technology is being used. A trustworthy and decentralised blockchain based electronic voting system suggested the trustless blockchain-based e-voting method[4]. Users can cast their vote at the comfort of their house view the results, and confirm that the votes are correct. In a similar vein, With the help of blockchain technology, Suyel Namasudra, Pratima Sharma, and his colleagues [5] were able to create a decentralised and secure cab sharing system that offers drivers and passengers a safe platform for shared trip services without the need for outside providers. Blockchain dependent Auto-Tallying Voting Protocols in Decentralised Internet of Thing provides a solution for government in another study by testing the algorithm.

II. ARCHITECTURE OF OUR SYSTEM

Our strategy is predicated on creating a more practical decentralized electronic voting system with blockchain technology. As follows, we describe the steps for our proposed approach in more details. The system is developed using Html/CSS & JavaScript front-end and Blockchain, MongoDB database back-end which contains the voter's personal details already stored such as- Aadhar database. A biometric device is used for validation purpose. If the voter/ user is a valid voter/user then he/she is handed a hash code/address that is used as a credential purpose for login into the voting machine. The voter name with symbol of voter is mentioned in the smart contract. It is the actual logic peace of entire election process. In this project we have used Ganache-CLI and Ethereum. The user can access the application after registering, and their identity is verified by their license and OTP. The total number of votes cast is measured via a web application. A single vote may be cast from a single account, and the account information is removed from the current election process when the vote is cast.

Major components of this approach are:

- EVM-Ethereum Virtual machine
- OTP Verification

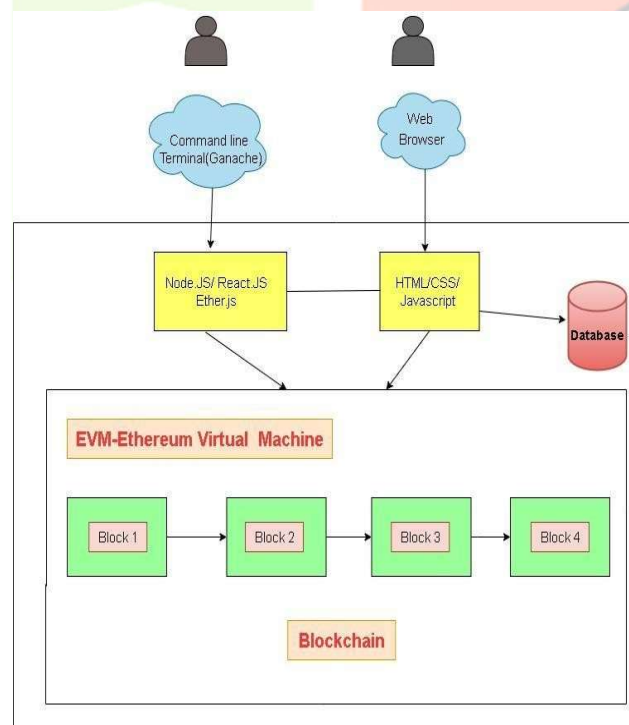


Fig.1. Decentralized e-Voting Architecture.

III. METHODOLOGY

The well-known secure electronic voting system described in Ryan (2008) is treated as the core for the decentralized voting system model that we present in this research. The system was created to facilitate an election-based application in a practical setting, by fulfilling the requirement of existing voting system such as privacy, verifiability, eligibility and enhanced security. The goal of the suggested approach is to establish a safe online voting process [7].

3.1 Blockchain

3.1.1 Blockchain Definition?

As the name implies, a blockchain is a network of blocks. Each block of blockchain data contains a hash value of all the data from the block that came before it. A distributed, decentralised, immutable ledger system called blockchain facilitates asset tracking and transaction recording inside a business network. You may take Google Doc as an example to understand blockchain technology easily. When we create a document or file and shared with many people, this document will get distributed instead of copying and transferring. This makes a decentralized distributed chain that can provide access to everyone at the same time duration. Although blockchain is more complex than a Google Doc but the concept is same [8].

In blockchain when we encrypt any message then the original data cannot be retrieved via decryption which makes it more secure and prevent fraudulent transactions as it is tough task to crack. The structure of blockchain is given below in figure 2:

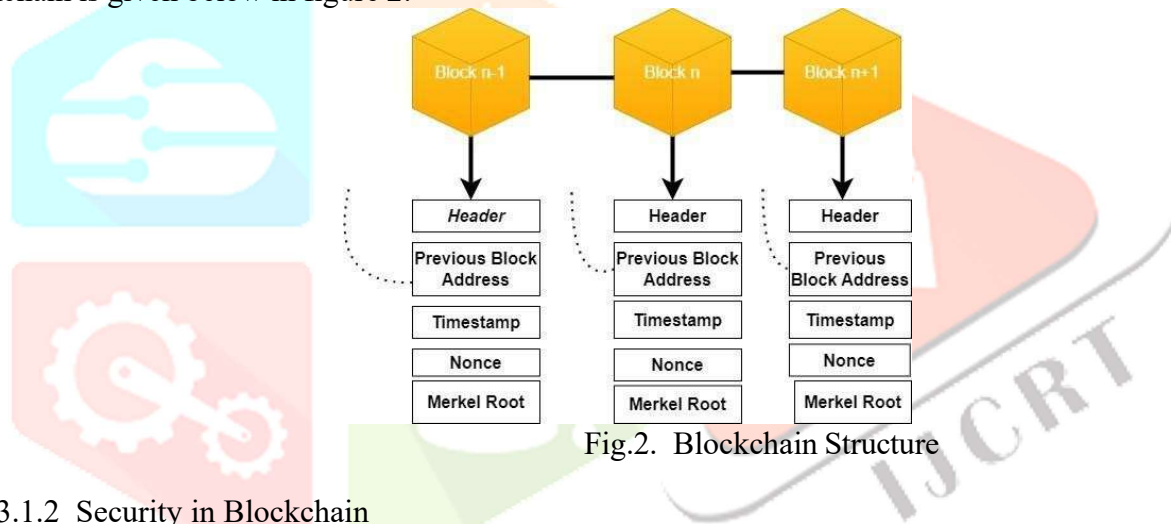


Fig.2. Blockchain Structure

3.1.2 Security in Blockchain

To ensure system security in this blockchain based system, we have employed Elliptic Curve Cryptography or ECC. It has two types of keys: 1.Public key and 2.Private key. These keys are used to provide security in the encryption and decryption process. Everyone has access to the public key, which allows anyone to view all of the networks' public information. To ensure account security, the private key is not shared with anyone on the network and is not publicly accessible to everyone. Only the account holder is aware of the private key, which is kept confidential. It is employed to give accounts security. In contrast to a regular account, in order to offer security to an account using this technique, everyone must use the receiver end's private key, which is known only to the receiver, in order to access and know the account details or to take any significant action.

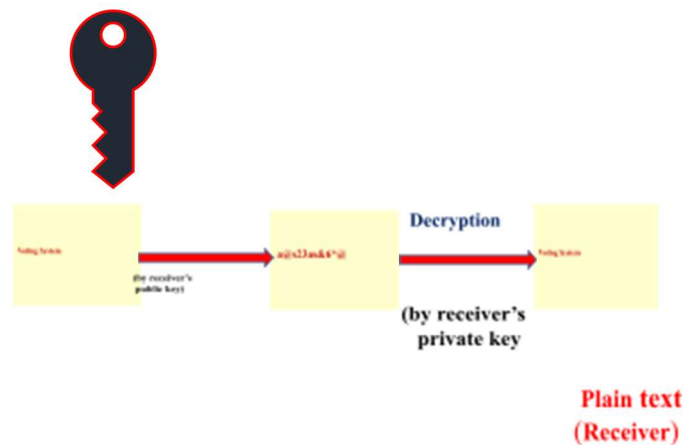


Fig.3. Encryption and Decryption process using Public and Private Keys

3.2 Ethereum

Ethereum is the most prominent phrase in blockchain technology at the moment. Vitalik Buterin published this powerful, open-source, decentralised blockchain-based programmable platform in 2015, enabling developers to design decentralised applications. Ethereum is an open platform that can be used to create and implement smart contracts. The cryptocurrency with the second-highest value right now is Ethereum. The market capitalization and is intended to surpass Bitcoin as the most popular cryptocurrency globally as well as a valuable investment. Its own cryptocurrency, Ether (ETH), is used to reimburse minors for validating transactions on the network and to pay transaction fees [10].

3.3 Metamask

A software wallet for cryptocurrencies is called Metamask. It is employed to communicate with the Ethereum network. In the present situation, it is one of the most popular applications. It enables users to interact with decentralised apps by connecting to their Ethereum wallet via a mobile app or browser extension.

3.4 React.js

An open-source JavaScript framework for making interactive user interfaces is called React.js. It is among the most used front-end JavaScript libraries worldwide.

3.5 Node.js

Although it is also a JavaScript framework, Node.js is primarily used to create an application's backend. Simply put, React.js and Node.js are both JavaScript frameworks; the only distinction is that Node.js is used for the back-end while React.js is used for the front-end.

IV. RESULT AND DISCUSSION

As previously mentioned, in order to protect the voting system from external threats by adding IP attackers to the blacklist, we need to identify a number of attacks, especially the Denial Of Service attack on the data centre that houses the citizen record and other attacks within the Electronic-voting station's network. These attacks have the ability to weaken democracy's foundation by compromising the voting process. The identification of such assaults is demonstrated using the machine learning paradigm. The Machine Learning Classifier predicts attacks by analysing network data. The data collection was used to train our machine learning model. The data set contains numerous instances of both typical traffic and traffic attacks. Zero-day attacks are easier to detect when there is regular traffic.

The location of the Intrusion Detection System is critical to the defence of the Electronic-voting network. The right site must be found in order for the IDS to produce accurate forecasts. Both the Datacenter (from which each E-voting station can access the data) and the Electronic-voting station itself should have their maximum number of infiltration attempts discussed. We placed the IDS in the middle of the voting station network for the Electronic-voting station such that it can monitor more traffic and more accurately defend the system, and we placed it at the edge of our data centre to more specifically detect distributed denial of service attacks at

given link mentioned below as: <https://docs.google.com/document/d/13F1uk64pgj0VMP0MnT8DEK41v0twsXOKCXhVZkziXXs/edit>.

The Fig.4 represents the overall structure of our project-

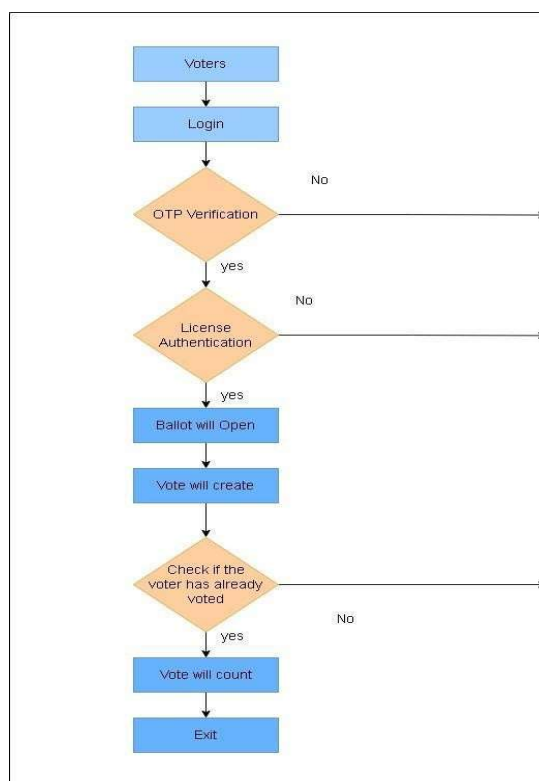
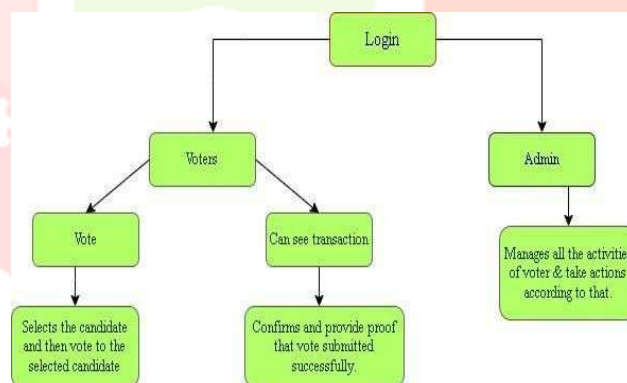
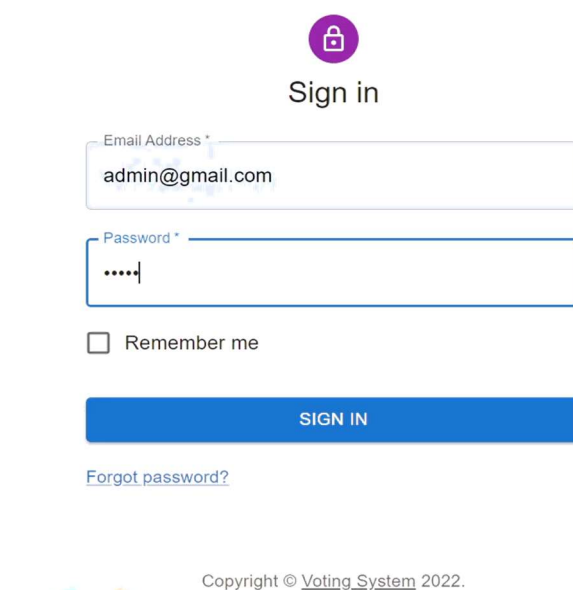


Fig.4. Overall Process of This Project

The Fig.5. Shows the data flow diagram of decentralized e-voting system which explains all the activities of Voters and Admin.



The below figure-6 represents the dashboard of our project where the admin will login into the system-



The image shows a web form for signing in. At the top center is a purple circular icon with a white padlock. Below it is the text "Sign in". The form consists of two input fields: "Email Address *" with the value "admin@gmail.com" and "Password *" with masked characters ".....". Below these fields is a checkbox labeled "Remember me". A blue button with the text "SIGN IN" is positioned below the checkbox. At the bottom left of the form is a link that says "Forgot password?". At the very bottom of the page, centered, is the copyright notice "Copyright © Voting_System 2022."

Fig.6. Admin Page

The below figure-7 Shows the election between Candidates-

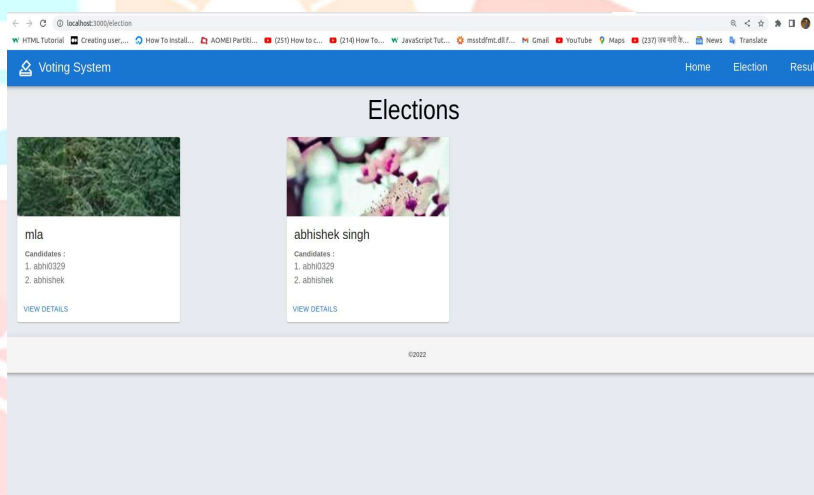


Fig.7. Election Page

A software wallet called Metamask is used to communicate with the Ethereum network.

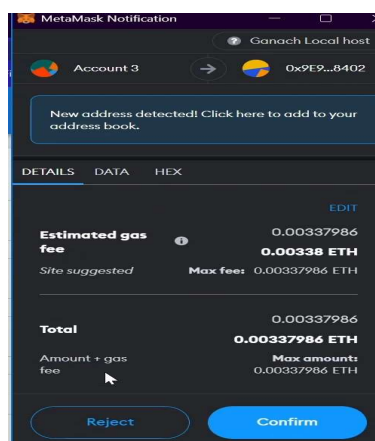


Fig.8 Notification by Metamask

A Survey of various algorithm to establish decentralized e-voting system has been done. Below we have mentioned the different algorithms to develop a secure e-voting system along with their accuracy.

The Table II shows the publication year distribution of the e-voting articles. These results show that e-voting with blockchain is the most commonly used articles in this new era.

TABLE II SHOWS NO. OF PUBLICATION ARTICLES IN PREVIOUS YEAR

Year	No. of Articles
2015	1
2016	0
2017	7
2018	25
2019	30
2020	32
2021	36
2022	39
2023	42

Our analysis of the blockchain-based electronic voting system by year of publication revealed that there was one paper in 2015, seven in 2017, twenty-five in 2018, and thirty in 2019. Thus, this outcome demonstrates that the use of blockchain-based electronic voting systems has grown annually.

V. CONCLUSION

When properly implemented, the aforementioned suggested method would offer a mechanism that might increase the security of the voting process. This project is essentially an effort to lessen the issues with the current voting system, which has a centralised design, is vulnerable to assaults, and is unreliable due to the fact that it is either highly difficult to maintain or hackable. As your vote cannot be traced back. With blockchain, however, everything is stored as a transaction, so you receive a receipt for your vote (in the form of a transaction ID), which you can use to safely confirm that your vote was tallied. Using Ethereum, A token id will be generated and will be goes on Platform of Ethereum network, it will be secured and cannot be altered & deleted by anyone. By using blockchain technology we are developing this project which will give guaranteed to the people that their valuable vote will be secured and will not fraud at any cost.

VI. REFERENCES

- [1] Sahare, Ashay, et al. "Blockchain Based Decentralized Voting System." (2020).
- [2] Alvi, Syada Tasmia, et al. "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system." *Journal of King Saud University-Computer and Information Sciences* 34.9 (2022): 6855-6871.
- [3] Satoshi Nakamoto, "Bitcoin: a peer-to-peer electronic cash system." Available at: <http://bitcoin.org/bitcoin.pdf>
- [4] Golnarian, Daria, Kimia Saedi, and Behnam Bahrak. "A decentralized and trustless e-voting system based on blockchain technology." *2022 27th International Computer Conference, Computer Society of Iran (CSICC)*. IEEE, 2022.
- [5] Namasudra, Suyel, and Pratima Sharma. "Achieving a decentralized and secure cab sharing system using blockchain technology." *IEEE Transactions on Intelligent Transportation Systems* (2022).
- [6] Li, Yannan, et al. "A blockchain-based self-tallying voting protocol in decentralized IoT." *IEEE Transactions on Dependable and Secure Computing* 19.1 (2020): 119-130.

- [7] Khan, Kashif Mehboob, Junaid Arshad, and Muhammad Mubashir Khan. "Secure digital voting system based on blockchain technology." *International Journal of Electronic Government Research (IJEGR)* 14.1 (2018): 53-62.
- [8] Indapwar, Aishwarya, Manoj Chandak, and Amit Jain. "E-voting system using Blockchain technology." *Int. J. of Advanced Trends in Computer Science and Engineering* 9.3 (2020).
- [9] Shah, Akhil, et al. "Blockchain enabled online-voting system." *ITM Web of Conferences*. Vol. 32. EDP Sciences, 2020. [10]. Ahad, S. A., Sangra, S., Saini, J., & Deepa, R. (2023). Decentralized E-Voting System Using Ethereum Blockchain Technology. In *Advances in Science and Technology* (Vol. 124, pp. 619-627). Trans Tech Publications Ltd.
- [12] Lalitha, V., Samundeswari, S., Roobinee, R., & Swetha, L. S. (2022, May). Decentralized online voting system using blockchain. In *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 1387-1391). IEEE.
- [13] Bhardwaj, S., Poongodi, T., Dixit, A., & Sharma, S. (2022, February). A Decentralized Digital Voting System Based on Block chain Architecture. In *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)* (Vol. 2, pp. 756-760). IEEE.
- [14] Saeed, S. H., Hadi, S. M., & Hamad, A. H. (2022). Iraqi Paradigm E-Voting System Based on Hyperledger Fabric Blockchain Platform. *Ingénierie des Systèmes d'Information*, 27(5) .
- [15] Garg, H., Singh, M., Sharma, V., & Agarwal, M. (2022, September). Decentralized Application (DAPP) to enable E-voting system using Blockchain Technology. In *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)* (pp. 1-6). IEEE.
- [16] Hyrynsalmi, S., Hyrynsalmi, S. M., & Kimppa, K. K. (2020). Blockchain ethics: A systematic literature review of blockchain research. In *Well-Being in the Information Society. Fruits of Respect: 8th International Conference, WIS 2020, Turku, Finland, August 26–27, 2020, Proceedings 8* (pp. 145-155). Springer International Publishing.
- [17] Ojo, A., & Adebayo, S. (2017). Blockchain as a next generation government information infrastructure: A review of initiatives in D5 countries. *Government 3.0–Next Generation Government Technology Infrastructure and Services: Roadmaps, Enabling Technologies & Challenges*, 283-298.
- [18] Andrian, H. R., & Kurniawan, N. B. (2018, October). Blockchain technology and implementation: a systematic literature review. In *2018 international conference on information technology systems and innovation (ICITSI)* (pp.370-374). IEEE.