DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

A Review: E-voting Security in Mobile Fog computing

Asma Ibrahim Hussein[1], Abeer Tariq MaoLood[2], Ekhlas Khalaf Gbash[3]
[1]*Ministry of Higher Education and Scientific Research, Bagdad, Iraq*
[2.3]*Computer Science Department, University of Technology, Baghdad, Iraq*
[1]*Cs.20.10@grad.uotechnology.edu.iq*, [2]Abeer.t.maolood@uotechnology.edu.iq,
[3]*110026@uotechnology.edu.iq*

Abstract— *Conventional voting activities are often replaced by electronic voting (EV) in light of the quick expansion of the Internet. For a variety of reasons, various nations have lately switched to EV rather than conventional voting. Different EV systems were presented up to this point. In both practical and theoretical fields, on the other hand, there is no perfect solution. To meet such objectives, the researchers strive for preserving cryptographic primitives when developing high-efficiency e-voting schemes. The concept of fog computing was developed to improve network infrastructure to satisfy the demands of large amounts of data the same time as also increasing the efficiency of the processing power. Also, it has been created as well to address concerns with Cloud computing, like the distribution environment complexity, real-time response, mobility, and IoT application location awareness. The concentration of this study was on a complete review regarding the systems of EVs through various scholars as a platform to detect flaws or problems in the deployment of extremely secure EV systems. In addition, nations having a history of EV system adoption were examined. A concept for future work on establishing a safe EV system depends on problems discovered in numerous works.*

Index Terms— *fog computing, security, E-voting, cryptographic, cloud computing.*

I. INTRODUCTION

The EV system can be defined as a new voting paradigm. EV has become one of the significant technologies worldwide in place of conventional paper voting. Developments in communication technology may make geographically distant locations more convenient and accessible. E-voting systems come in a variety of types [1]. The fingerprint voting system requires the user to submit her or his fingerprint as proof of identity. The fingerprint technology scans the data from the fingerprint and validates data that has already been saved in the database in addional the finger vein recognition scheme is considered more robust, secure, and emerging biometric traits[2].

Due to its unique characteristics such as live detection, anti-counterfeit, and need small portable capturing devices. In the case where the provided information matches the database data, the system permits the person to vote. As a result, the heart of the computerized EV system, where election data is stored, recorded, and processed as digital information in the modern day, was confidentiality, security, accuracy, and reliability. At the time of voting, fingerprint sensing could be used to authenticate online voting. Since National identity is considered one of the system's keys, it will make the system more secure by utilizing the National identity card number, distinctive for every individual, ensuring that there is no duplicate voting [3]

Face recognition plays an important role in many powerful types of research. With the current world security status, governments, as well as the private sector, demand dependable methods to recognize individuals precisely without contradicting with rights or privacy.[4] Face recognition systems have

Received 13/June/2022; Accepted 05/July/2022
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

become far more efficient. Yet, the accuracy of the face recognition method could be improved. The effects of such approaches are influenced by changes in the surroundings, like expression disparity, illumination deviations, and pose variations [5].

E-voting with the use of biometric has provided a more secure way of voting in a democratic country compared to the traditional voting where papers are used, and voting is insecure . Biometric is a physical and biological quality of an individual which is different for every person .There are different types of biometric traits among which are facial recognition, Fingerprint, iris recognition, and palm print.[6]

Fog computing can be defined as a method for bringing centralized cloud operations closer to end users by moving computing applications, services, and data to the network edge[7]. It's a distributed model that delivers the cloud as a service for network edge devices. Rather than controlling network devices like the switches and getaways, it creates control, configurations, and administration over the Internet [8]

II. RELATED WORK

Different researches on using the voting systems are still underway in the literature. The properties of such technology enable the creation of decentralized and automatic voting systems in theory. Also, indeed, scientific research is still a long way from finding a definitive solution for creating an EV system that can replace conventional voting methods, as evidenced by recent studies in the Table I below.

TABLE I. RELATED WORK

No	Authors and name of a paper	Method	Results and features	Limitation
[9]	Zinah J. Ameen, "Application Voting System of Web based in Iraq" (2017)	Web-based system.	This study introduced a computer-assisted voting and counting mechanism. Election-related data is stored and managed digitally in an EV system. A web-based EV program with the use of ASP.net and SQL server was proposed. This application implements the voting procedure in the voting station and displays the results of the election.	The dataset very small where This system was tested on ten persons six were recognized and able to vote.
[10]	A. Ben Ayed "Aconceptual secure Blockchain based electronic voting system" (2017)	Hash Algorithm (SHA-256)	Depending on Blockchain technology, the research presented an EV mechanism. It's a decentralized system that doesn't depend upon trust. Any registered voter will be capable of voting via any device with an Internet connection. No one will be capable of manipulating Blockchain because it will be distributed and verifiable publicly.	The centralization of the I-Voting system makes it vulnerable to DDOS attacks what could make the elections inaccessible to voters.

Received 13/June/2022; Accepted 05/July/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

[11]	M. Pawlak, Towards the intelligent agents for blockchain e-voting system" (2018)	intelligent agents + Blockchain	The goal of this study's agent-based solution for the ABVS EV system is to improve voting security by decreasing the application's role in polling stations to that of an intermediary between agents and voters, who will handle all of the tasks that are associated with vote processing and transmission. Furthermore, the agents could be distributed via nodes, making any attempts for breaking into the EV system and steal sensitive data easier to identify.	the voters would receive unique electronic voting cards. These cards would not be sent directly, but as voting agents this make misuse or attacks can be get to this card this make the system weakness.
[12]	SH. GAO and el., "An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function" (2019)	combining with traceable ring signature algorithm + Blockchain	This study suggests a blockchain based EV protocol that ensures the transparency of the voting process. By using certificate-less and code-based cryptography, this approach may audit voters acting wrongly and quantum attacks.	This study is suitable for the small-scale election and has some advantages in security and efficiency when the number of voters is small.
[13]	S. Aruna, M.Maheswari el., "Highly Secured Block-chain Based Electronic Voting System Using SHA-3 and Merkle Root" (2020)	Blockchain + SHA3 + RSA	Based upon the block-chain block generation and sealing, research created an efficient approach to create a block for each vote. Each candidate's votes could be counted using the sealed blocks. This suggested system overcomes the drawback that votes are cast by EVMs, and there isn't any method to ensure that votes are not cast in any form of electoral fraud and that just a voter has access to her/his data and who voted for them. All information regarding the EV system is very secure on a blockchain with the use of RSA, SHA3, and Merkel root algorithms.	the main problem occurs when the clients don't safeguard their private credentials. This implies there is consistently a danger of private keys being taken. As an undertaking or business, you have to teach clients on the best way to protect their private keys.
[14]	A. Santha Sheela et., "E-Voting System Using homomorphic Encryption Method (2020)	Homomorphic	This voting mechanism makes it simple for everyone to cast their votes. Online voting increases the number of votes cast, and manual tallying will be unnecessary. Therefore, we will get a very quick and clear result. We can solve numerous problems with the present system by employing this newly built system. This system is more effective than the one currently in use.	Using the Aadhaar card number of the particular voter and then check whether the given number is correct or not from the Aadhaar card detail database this card able to wasted and database to vulnerable to attacks

Received 13/June/2022; Accepted 05/July/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

[15]	E.Vetrimani and et., "Real Time Face Recognition in Electronic Voting System using RFID and Open CV (2020)	Haar feature-based cascade classifiers	This research proposes a more efficient method of voting. In the voting process, we have two levels of security. The first level is RFID number verification, and the second level is face recognition. The implementation of a new approach for each voter has greatly increased our system's security. Face recognition in the application improves user authentication in the system, allowing the application to determine if the user is authenticated or not.	voting system is not secure and time consuming as well. The people who are not eligible to vote can also cast their votes by unwanted means, which may cause various problems
[16]	Onu, Fergus Uche (Ph.D.) Ibe, Walter EyongEneji, "Analysis of Strengths and Weaknesses of Online Voting Systems: the Way Forward" (2021)	Blockchain	Online voting systems in their design for accommodating good security characteristics which will shield them from the fraud, and enable harvesting plenty of benefits that are related to systems.	observed that the DEF CON method of sending ballots over email like the military does, is incredibly insecure
[17]	R. Tas and O. Tanrı¨ "A Manipulation Prevention Model for Blockchain-Based E-Voting Systems" (2021)	Blockchain & Homomorphic	The counting and voting phases of the suggested system operated as expected, according to simulation data. Ballots are encrypted using homomorphic encryption and after that distributed to system nodes. Only valid voter ballots will be recorded as transactions that will then be mined into blocks. It has been verified as well that the system continues to function even in the case where a node fails. All stakeholders would be informed of the election results without any data loss.	most important limitation has been the difficulty of simulations with as many nodes as a real election system needs.
[18]	M. Goyal and et., "Sustainable E-Infrastructure for Block-chain-Based Voting System"(2021)	Ethereum Virtual Machine	The key aspect of this system is that voters might vote from anywhere in the world because the voting process has gone online and digital. Because voters from outside the country might vote from any place where they are, the total percentages of voting can be greatly increased. Because this EV is based on Blockchain technology, it's entirely secure and authorizes the system. The most essential features of this system are that it is transparent, portable, simple, and reliable.	Need to make it simple and easy so that anyone can use it without any professional knowledge of Computers.

Received 13/June/2022; Accepted 05/July/2022

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

III. E-VOTING SYSTEM AND SECURITY REQUIREMENTS

Electronic voting constitutes an important part of democratic governance in an ICT-enabled environment. This is aimed at increasing the participation of citizens in the nation`s electoral process while at the same time improving the outcome of an election as compared to traditional voting systems.[19] Electronic voting supports a critical electoral process including verification of eligibility, registration stage, voting stage and finally counting of votes electronically. *Fig. 1* depicts the conventional voting system. The following EV requirements must be met by adequate EV systems[20]:

1**. Anonymity** The voting turnout should be protected from external interpretation during the polling procedure. There will be no correlations between the registered votes and voter IDs within an electoral structure.

2**. Accuracy and Auditability**

Accuracy, also known as correctness, requires that declared results match election results exactly. This indicates that no one can influence other citizens' votes, that the final tally includes all of the valid votes, and that no conclusive tally of the invalid ballots exists.

3. Democracy/Singularity

A "democratic" system is one in which only eligible voters might vote and each registered voter could just cast one vote. Another feature is that the vote must not be duplicated by anybody else.

4. **Vote Privacy**

After a vote has been cast, nobody must be able to link a voter's identity to their vote. Computer secrecy represents a delicate confidentiality form, implying that voting relations will remain concealed for a long time as computer power and new approaches change the present rate.

5**. Integrity and Robustness**

This requirement ensures that a sizable group of voters or representatives will not be able to sabotage the elections. It assures that registered voters will be able to abstain with no difficulty or encourage others to exercise their right to vote. Officials and citizens who are corrupt are banned from contesting election results by claiming that another member did not fulfill their part appropriately.

6. **Lack of Evidence**

While anonymous privacy protects against electoral fraud, no system can guarantee that the votes are not influenced by bribes or election rigging. From the beginning, this question has been rooted.

7. **Fairness and Transparency**

It means that no one can learn the details before the count is made public. It prevents acts such as prediction publishing to affect the decisions of the late voters or presenting a large, however, an unfair advantage to particular groups or individuals in return for being the first to know.

8. **Mobility and Availability**

The systems of voting must be available at all times throughout the voting period. Voting systems must not restrict where people can vote.

9. **Verifiable Participation/Authenticity**

The desirability criterion allows you to determine whether a single voter participated in the elections or not. This criterion should be met when voting by voters is made mandatory through the constitution (as it is in some nations like Germany, Australia, and Greece) or when abstention is considered a disrespectful act in a social setting (like the medium and small-sized elections for the delegated corporate board).

Received 13/June/2022; Accepted 05/July/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

10. **Reassurance and Accessibility**

To ensure that everyone who wishes to vote has the chance to do so at the appropriate polling station, which should be open and accessible to voters. Only qualified voters must be permitted to vote, and all of the ballots have to be counted precisely to ensure that the elections are genuine [20]

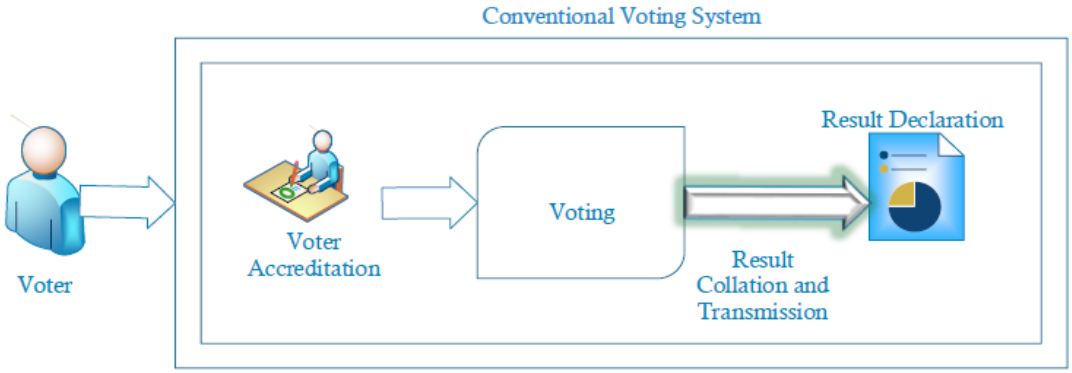

FIG. 1 CONVENTIONAL VOTING SYSTEM[21].

IV. ON-LINE VOTING SYSTEM PROBLEMS AND SOLUTIONS

Many conditions must be met for traditional paper-based voting, voting via digital voting machines, or voting through an internet voting system: the solutions and problems for achieving such criteria in online voting systems are summarized in Table II below [20]

TABLE II. SOLUTIONS AND PROBLEMS OF VOTING SYSTEMS

no	properties	Problem	Solutions
1	Eligibility	There are threats: To begin, any changes to the voter list must be double-checked to ensure that no illegal voters are added, and the mechanism of identification has to be both secure and trusted to ensure that a voter's account can't be stolen or exploited by intruders.	The solution to the eligibility problem is simple. To vote online, voters must use a recognized identification system to verify their identity. All of the legitimate voters' identities must be added to the participants' list.
2	Unreusability	It's difficult to achieve both voter anonymity and un reusability. Furthermore, allowing the voter to re-vote could be important, making the task much more difficult.	glance, implementing un reusability could appear straightforward in the case where a voter casts their vote, all that is required to be done is placing a mark in the list of participants and not allowing them to vote another time.
3	Privacy	Privacy in an online voting context means that nobody but the voter knows the way a participant has voted	Homomorphic encryption, blind signatures, and mix-networks are merely a few of the ways that are utilized to achieve this attribute. A blind signature represents a data signature type where the signer does not have an idea of what they are signing. It is accomplished by employing a blinding function, which combines signing and blinding.

Received 13/June/2022; Accepted 05/July/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

4	Fairness	Voters encrypt their selections before sending them, and these choices are decoded at the end of the process of voting, ensuring that no one gets intermediate outcomes. The important point to understand here is that in the case where somebody has a key to decryption and access to the encrypted decisions.	The solution to this issue is through the distribution of the key amongst many key-holders.
5	Soundness and completeness	Although the soundness and completeness characteristics appear to be simple, implementing them could be difficult based on the protocol. In the case when ballots are decrypted one at a time, it's simple to differentiate between invalid and valid ones, yet in the case where the hemimorphic encryption is used, things become more problematic.	Zero-knowledge proof is used to tackle this problem. This represents a cryptographic way to prove a statement regarding the value without releasing the actual value, according to the definition. Range proofs, in the instance, show that a given value belongs to a specified group in these cases.[22]

V. LIMITATION AND BENEFITS OF E-VOTING SYSTEM

The use of electronic means or information technologies for conducting voting operations is known as EV. In addition, EV is a broad phrase that encompasses a wide range of technologies, methods, and applications. EV systems have several drawbacks and advantages illustrate in Table III [23] : -

TABLE III. DRAWBACKS AND ADVANTAGES

Limitation	• Legislature: The current government's unwillingness to pass legislation supporting the development of mobile voting electoral systems. It could be a fear of not being able to manipulate the system for personal gain, a lack of basic ICT understanding, or something else. • Lack of trust in the technology used to enable mobile voting in terms of security and reliability; Mobile voting represents a relatively new technology that has yet to acquire widespread adoption in electrical procedures. • Complete control by the governmental authorities: The purpose of the electoral system is to fulfill the people's mandate. This is majorly essential to limit the activities of political office holders while still reaping the benefits of governance[16] • when that voter will utilize a secure device for casting their votes. Even when the system is secure, the hackers are capable of casting or altering a vote with the use of malicious software that has been installed already on the device of the voter. [22]
Benefits	• Fraud prevention, through decreasing human involvement. • accelerating results processing. • Decrease the spoilt ballots through automatic validation and enhanced presentation of the ballots. • Increasing the involvement in the democratic process because of easier availability (i.e. remote voting). • Decrease of costs because of the reduction in voting overhead. • possibility for more direct democracy[11]

Received 13/June/2022; Accepted 05/July/2022
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

VI. RISK AND CHALLENEGES OF E-VOTING SYSTEM

It is vital to know and prevent financial, technological, and management-related risks and problems for electronic technologies to be deployed efficiently in the long run the existing challenges can be divided into two categories: first, those related to the inherent weaknesses of the e-voting system, which are generally related to issues of data validation and security; and second, those related to the condition of voters and the completeness of supporting facilities and infrastructure[24]:

1. Lack of transparency: Dissimilar to all other ICT technologies, electoral technologies have a distinctive feature: they maintain the ballot's secrecy.

2. Security: The transmission of the summary data from polling stations to districts or the upper level must be protected by security measures. When the transfer is done over the Internet (by modem or satellite equipment), the risk increases.

3. Foreign interference: A hacking attack/cyber-attack on electron infrastructure is one of the most common forms of interference. The voting process is subject to hacking attacks and cyber-attacks in electronic elections through DoS [5]to describe the difficulty of the voting system: -

- The system is only useful for remote voters. Not the voters who are residing in the area in which voting is held.
- A huge initial investment is required to set up units in different locations.
- The biometric authentication process may consume a little more time as it involves several processes.
- Biometric authentication sometimes fails to identify even genuine voters and denies them the right to vote.
- It is functioning largely depends on the sophisticated network infrastructure as most of the operations are cloud-based.
- As almost all the processes are happening using cloud infrastructure, there may be cause to worry about the security and safety of data [22].

VII. FACTORS THAT EFFECT ON SECURITY

Threats are the entities or activities that jeopardize the safety and accuracy of an e-voting system. Based on the source, they can be categorized into internal and external :

1. The internal threats come from those who have authorized access to the e-voting infrastructure and components, including authorized users or even internet service providers.

2. The second threat source comes from the people that have no authorization to access the equipment or infrastructure. Voters may access the e-voting system through personal computers, public computers, or kiosks, and try to use different identities (fake or real) to cast multiple votes.

3. using personal or public computers may impose the voters on the danger of malware vote modification – changing votes, collecting their information, or even attacking the evoting system . Election officials access the e-voting system through the consoles. They are authorized users for manipulating evoting system properties such as adding/removing eligible voters' groups, defining vote structure, time, and date of casting votes .

4. External threats – the second source – are from individuals or organizations that do not play any supportive role in elections, like hostile individuals, criminal organizations, protest groups, foreign intelligence services, and terrorist organizations . Relying on their technical capabilities, these individuals may try to ban votes to be cast, monitor the voting process, hurt the e-voting system, and change election results. Since these attackers are supported by organizations or groups like other countries or rival political parties, the damages can be significant or even change election results[25]

Received 13/June/2022; Accepted 05/July/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

VIII. COMPARISON OF CASE STUDIES OF THE EXPERIENCE OF ELECTRONIC VOTING FOR DIFFERENT COUNTRIES

E-voting has lately been reported as the unavoidable future of electioneering in various nations worldwide. Some nations have legally approved the use of EV methods for electing their leaders, whereas governments in other nations are hesitant. Technical questions about the rejection and adoption of EV methods were undoubtedly raised. As a result, Table IV show overview of using EV methods in some nations. [26]

TABLE IV. EV METHODS IN SOME NATIONS

no	country	Technologies used	problems
1	Netherlands	direct-recording electronic (DRE) voting machine	When a voter has turned away due to an invalid ID card, the Netherlands faced a security-based authentication challenge. Imposters might also fake an actual voter's ID card. The Neap ES3B's Erasable Programmable Read Only Memory (EPROM) might be removed and substituted with tampered memory to favor one candidate over another.
2	United States of America (USA)	Those technologies are DRE, Machines of Hybrid Voting, and Optical Scan.	In 2016, the US accused Russia's government of interfering with the US election's cyber security.
3	India	Adhere card and finger-print are the main authentication credentials	The costs of creating Adhere cards for authentication are higher compared to non-biometrics-based cards.
4	Switzerland	the voting system that is referred to as Unisys Internet voting system which has been launched in 2002	The SMS channel has been discontinued in 2007. Voters' votes were secured using encryption methods.
5	Estonia, a country in Northern Europe	National ID cards and mobile IDs on the website for the authentication	Because decryption and encryption methods create suspicion of the sensitive results, rigging is feasible.
6	Nigeria	introduced Permanent Voters Card (PVC) and card readers for the accreditations	election malpractices like rigging, false voting, and false declarations of the winner have been characterized in the 2019 general elections
7	Bangladesh	Automatic fingerprint identification system (AFIS)	BVR encountered major logistical, legal, political, administrative, social, and environmental problems during its development and execution. In particular, (a) there was no legal framework for collecting AFIS data or producing and distributing NIDs; (b) time was limited because the election had been postponed and there was pressure to hold it as soon as possible, and (c) the EC required a considerable amount of money, logistics, and technical expertise for the BVR process.
8	Uganda	A digital camera was used to take a photo of the voter, and biographical data was collected with the use of a paper-based registration form.	Multiple voting was not detected in some circumstances by the facial recognition system. The poor image quality influenced the FRS results, and by 2010, images taken in 2001 had aged and were no longer easily examined. Since the images on the floppy drives used for storing the images were corrupted, certain voters did not have a photo. [27]

Received 13/June/2022; Accepted 05/July/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

IX. FOG TO ENHANCE SECURITY AND PRIVACY

Fog computing, dissimilar to cloud computing, has its own set of properties, including resource constraints, distributed nature, and distant operation. Those properties have created a distinctive environment in the area of image transfer security and privacy. Despite fog computing being a featuresrich platform, it is dogged by its susceptibility to several security, privacy and safety concerns, which stem from the nature of its widely distributed and open architecture[28], [29]it also used to work with sensitive information which is generated from several sources. For securing these types of sensitive information, privacy is one of the most significant concerns in Fog computing. There are lots of privacy issues that arise in the Fog environment[30]

That is, because it presents specific local privacy and security services like threat detection and local monitoring, it might improve the overall security regarding the IoT layer. However, the bulk of research has found that Fog reduces the privacy and security of IoT applications.

In this architecture, three layers can be identified; device layer, Fog layer, and Cloud layer. These three layers can be connected directly or indirectly with public authorities such as key generation center and certificate authorityas depicted in *Fig. 2* [31],[32]

Device layer: In general, the devices in this layer are geographically distributed and have low computation capabilities and limited storage resources. These devices collect and send raw data to the upper layer (Fog layer) for processing and storage. **Fog layer**: It is located close to the device layer and it is composed of a large distributed number of Fog nodes. The Fog nodes consist of network equipment (mobile or static) with higher storage and computation resources than the device layer capabilities such as gateways, routers, access points, switches, access points, and so on. **Cloud layer**: The Cloud layer consists of multiple high-performance servers and permanent storage of an enormous amount of data. It provides many applications and services such as smart power distribution and smart transportation. These services are accessible at any time and from anywhere through the internet connection[28]

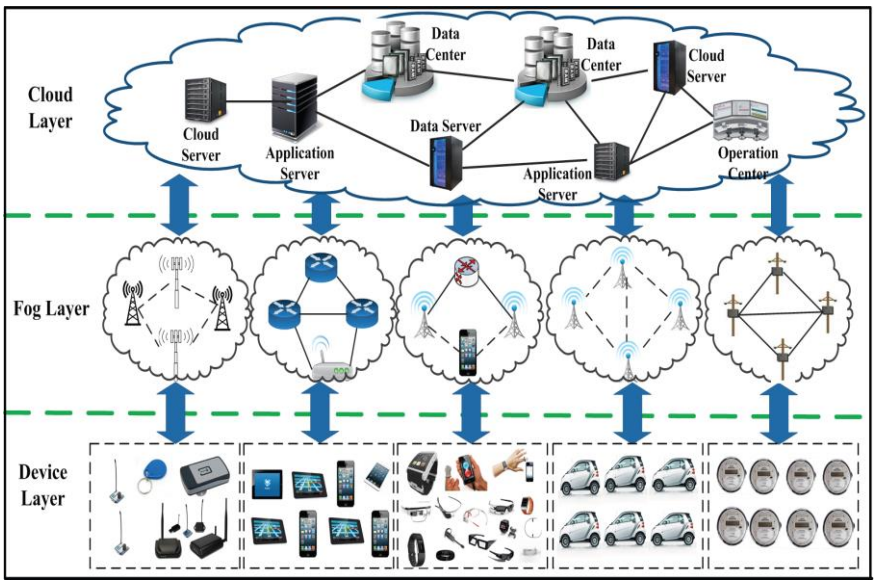

FIG. 2 ARCHITECTURE OF FOG COMPUTING[33].

Received 13/June/2022; Accepted 05/July/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

X. CONCLUSIONS

The purpose of the present work is to review and assess the present study based on the EV systems. The latest EV research with the use of various technologies is discussed in this article. First, the concept and its applications are discussed, followed by present EV systems. After that, a list of problems in present EV systems is identified, as well as the potential of the addressee to improve EV, present solutions for based EV, and future research directions on based EV systems. A decentralized EV system, according to several experts, could be a good fit. Through research and review of research on electronic voting, were found some limitations in achieving security for voter data and achieving transparency in the electoral process, some researchers used fingerprints to conduct voting, but this requires voters to attend voting centers to cast their votes, and some of them used the fact that the face is exposed to external circumstances, including age Beard, hat, and lenses, and some of them used the voter's identity to achieve a kind of security. Suggesting new encryption techniques and building a hybrid system to achieve system security and invulnerability from any attacks.

XI. A FUTURE WORK

The following are the findings and recommendations for developing a secure EV system:

1. Using fingerprint biometric and face identification, in addition to using techniques recently found for encryption in transferring voter data to the main center in a way that achieves a kind of security.

2. The possibility for the election to take place without the presence of voters through the use of smart devices to conduct the poll safely, and will reduce the time and effort.

3. It will send the data via the Fog computing environment, and it will employ this technology to address all of the issues raised in this work, as well as to meet the functional and security criteria of EV to achieve credible elections at all levels.

REFERENCES

[1] H. H. Ali, “Secure E-voting system based on iris authentication,” Ph.D. dissertation, U Iraqi Commission for Computers and Informatics, Iraq, 2010.

[2] K. Shaheed *et al.*, "A Systematic Review on Physiological-Based Biometric Recognition Systems: Current and Future Trends," *springer*, *Archives of Computational Methods in Engineering*, vol. 28, no. 7. 2021. doi: 10.1007/s11831-021-09560-3.

[3] A. Piratheepan *et al.*, “Fingerprint Voting System Using Arduino College of Technology Jaffna , Sri Lanka,” *Middle-East J. Sci. Res.*, vol. 25, no. 8, pp. 1793–1802, 2017.

[4] Q. Meng, S. Zhao, Z. Huang, and F. Zhou, “MagFace: A universal representation for face recognition and quality assessment,” *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, pp. 14220–14229, 2021, doi: 10.1109/CVPR46437.2021.01400.

[5] Z. J.Ameen , “Face Recognition Integrated with Chaotic Encryption for Secure Electronic Election Application,” *Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications*, no. 23, pp. 1–19, 2019.

[6] K. Okokpujie, J. Abubakar, S. John, E. Noma-Osaghae, C. Ndujiuba, and I. P. Okokpujie, “A secured automated bimodal biometric electronic voting system,” *Intrnational Journal of Atitifical Intellegent*, vol. 10, no. 1, pp. 1–8, 2021, doi: 10.11591/ijai.v10.i1.pp1-8.

[7] A. A. Laghari, A. K. Jumani, and R. A. Laghari, “Review and State of Art of Fog Computing,” *Arch. Comput. Methods Eng.*, vol. 28, no. 5, pp. 3631–3643, 2021, doi: 10.1007/s11831-020-09517-y.

[8] S. F. Hassan, “Task Scheduling for Video Streaming using Fog Computing,” M.S. dissertation, University of Technology, Iraq, 2019.

[9] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," *Nature Communications*, vol. 9, no. 1, pp. 1–11, 2018.

[10] A. Ben Ayed, “A Conceptual Secure Blockchain Based Electronic Voting System,” *Int. J. Netw. Secur. Its Appl.*, vol. 9, no. 3, pp. 01–09, 2017, doi: 10.5121/ijnsa.2017.9301.

Received 13/June/2022; Accepted 05/July/2022

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.23.1.5

[11] M. Pawlak, A. Poniszewska-Maránda, and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," *Procedia Comput. Sci.*, vol. 141, pp. 239–246, 2018, doi: 10.1016/j.procs.2018.10.177.

[12] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum e-voting protocol in blockchain with audit function," *IEEE Access*, vol. 7, pp. 115304–115316, 2019, doi: 10.1109/ACCESS.2019.2935895.

[13] S. Aruna, M. Maheswari, and A. Saranya, "Highly secured blockchain based electronic voting system using SHA3 and merkle root," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 993, no. 1, 2020, doi: 10.1088/1757-899X/993/1/012103.

[14] A. C. S. Sheela and G. F. Ramya, "E-voting system using homomorphic encryption technique," *J. Phys. Conf. Ser.*, vol. 1770, no. 1, 2021, doi: 10.1088/1742-6596/1770/1/012011.

[15] E. Vetrimani, J. Akash, C. Rishi, and P. Raveena, "Real Time Face Recognition in Electronic Voting System using RFID and OpenCV," *Int. Res. J. Eng. Technol.*, pp. 3995–3998, 2020, [Online]. Available: www.irjet.net

[16] F. U. Onu and W. E. Uche, "Analysis of the Strengths and Weaknesses of Online Voting Systems: the Way Forward," *IOSR J. Comput. Eng.*, vol. 22, no. 2, pp. 53–57, 2020, doi: 10.9790/0661-2202015357.

[17] R. Taş and Ö. Ö. Tanriöver, "A Manipulation Prevention Model for Blockchain-Based E-Voting Systems," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/6673691.

[18] M. Goyal and A. Kumar, "Sustainable E-Infrastructure for Blockchain-Based Voting System," *Digital Cities Roadmap*, 9 April 2021.

[19] S. Choi, J. Kang, and K. S. Chung, "Design of Blockchain based e-Voting System for Vote Requirements," *J. Phys. Conf. Ser.*, vol. 1944, no. 1, p. 012002, 2021, doi: 10.1088/1742-6596/1944/1/012002.

[20] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors*, vol. 21, no. 17, 2021, doi: 10.3390/s21175874.

[21] M. A. Musa, B. S. Maina, and A. M. Bade, "Fog comuting based elecronic voting system:a solution to denial of servic," vol. 8, no. 1, pp. 1–9, 2021.

[22] V. chandra, G. P. K., R. M., and K. P. K., "A Conceptual Framework for the Integrated, Smart and Secure Remote Public Voting System (SSRPVS)," *Int. J. Manag. Technol. Soc. Sci.*, vol. 5, no. 1, pp. 318–334, 2020, doi: 10.47992/ijmts.2581.6012.0097.

[23] C. Science and S. Bhat," Android Based Online Voting System ," *Electronics ,Software and mechinical* , no. 06, pp. 2934–2937, 2022.

[24] F. Bachmid and H. Djanggaih, "The Future of E-voting Implementation in Indonesian General Election Process : Constitutionality , Benefits and Challenges," *Varia Justicia*, vol. 18, no. 1, pp. 34–51, 2022.

[25] S. S. Chaeikar, A. Jolfaei, N. Mohammad, and P. Ostovari, "Security Principles and Challenges in Electronic Voting," *Proc. - IEEE Int. Enterp. Distrib. Object Comput. Work. EDOCW*, no. December, pp. 38–45, 2021, doi: 10.1109/EDOCW52865.2021.00030.

[26] M. Chikhladze, "E-voting in georgia," Council of Europe, E-voting handbook - Key steps in the implementation of e-enabled elections, 2021.

[27] P. Wolf," Introducing Biometric Technology in Elections," 2017. [Online]. Available: https://www.booktype.pro

[28] Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al- Ahmad, "Fog computing security and privacy for the Internet of Thing applications: State- of- the- art," *Secur. Priv.*, vol. 4, no. 2, 2021, doi: 10.1002/spy2.145.

[29] R. Neware and U. Shrawankar, "Fog Computing Architecture, Applications and Security Issues," *Int. J. Fog Comput.*, vol. 3, no. 1, pp. 75–105, 2019, doi: 10.4018/ijfc.2020010105.

[30] A. Rahman, M. Uddin, H. Riaz, N. Nath, and A. Q. M. S. Pathan, "A Fog Based Encryption Algorithm for IoT Network," *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)*, vol. 17, no. 4, pp. 199–204, 2019.

[31] A. A. Patwary, R. K. Naha, S. Garg, S. K. Battula, and M. Gong, "Towards Secure Fog Computing : A Survey on Trust," pp. 1–52, 2021.

[32] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, 2017, doi: 10.1186/s13677-017-0090-3.

[33] H. Sabireen and V. Neelanarayanan, "A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges," *ICT Express*, vol. 7, no. 2, pp. 162–176, 2021, doi: 10.1016/j.icte.2021.05.004.

Received 13/June/2022; Accepted 05/July/2022

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*