International Journal of Informatics, Information System and Computer Engineering

Preventing Man in The Middle Attack on E-Voting System using Multi-Layer Security Protocol

*Uzoma Sunday**

National Open University of Nigeria, Nigeria
*Corresponding Email: Sundayuzoma007@gmail.com

ABSTRACTS

Intelligent technologies, most notably the growth of the World Wide Web, are used to improve human life. In comparison to prior eras, an increasing number of jobs may now be accomplished swiftly and efficiently thanks to the Internet's spectacular development. One relatively new field that has been identified is e-voting. There are several ways to vote, including online, using a mobile application, and in person at a polling station. The internet's rapid expansion means that application security cannot be ignored. I developed an Android application with a 5-step security process—user authentication, fingerprint authentication, captcha, OTP verification, and cryptography—before voting in order to thwart phishing attempts. With a mobile device, voters may now cast their ballots online at any time and from any place. The application is created and deployed using Android Studio. The software development life cycle is followed in this research when developing the voting application. The outcome of this study is the development of a voter-friendly mobile application that functions as a useful tool to enable voters to cast ballots with five security levels.

ARTICLE INFO

Article History:
Received 26 Mar 2024
Revised 01 May 2024
Accepted 14 Aug 2024
Available online 21 Dec 2024
Publication date 01 Dec 2025

Keywords:
Technology, Cybersecurity, Computer Engineering, Information System

DOI: https://doi.org/10.34010/injiiscom.v6i2.12595
p-ISSN 2810-0670 e-ISSN 2775-5584

1. INTRODUCTION

Voting is among the best things an individual can do for the community they live in and for oneself. People generally think that their vote is unaffected by the vote of another individual. However, many fail to recognize the importance of each and every vote. People may select the sort of life they desire for themselves and future generations by using their right to vote (Basit, et.al, 2020). It's a chance to talk about things that people care about, including the sort of leader they want. In elections, the choices are made by the voters. If you don't vote, someone else will make the decision. Even though elections are held every year, not many people in this day and age understand how important they are (Bishop, et.al, 2017).

One of the reasons is that many are reluctant to go to voting stations in person. E-voting is the process of utilizing a phone or other electronic device to cast a ballot online. It's commonly called an electronic voting system. With the rapid advancement of technology, voting through a variety of channels—including the phone, the internet, and private computer networks—has grown more influential. These voting techniques provide several benefits, such as reduced expenses, ease of use for voters with disabilities, prompt installation, and simplicity of use (Ali, et.al, 2015).

Nonetheless, there are security holes in online voting platforms that leave the voting procedure vulnerable to serious attack. If the security is weak and the control system is ineffective, attackers may launch a variety of dangerous operations, such as using phishing attacks to rig the online vote and alter the result (Basit, et.al, 2020). A sort of social engineering attack known as "phishing" involves administrators or end users being tricked into divulging personal information over the phone, through emails, texts, or phone calls. With the use of this technology, organizations will be able to cast votes on significant, confidential internal business decisions (Arafin, et.al, 2018).

Being safe is essential to an electronic voting procedure. Security concerns in the context of electronic voting are highly delicate. This is a result of some characteristics that conflict with one another. Ensuring anonymity, for instance, makes it more difficult to detect election fraud. Furthermore, a major factor influencing e-voting security is the kind of technology utilized (Basit, et.al, 2020). There are two primary types of electronic voting: remote and in-person. The former is conducted in a designated station, overseen by the election administration, and using an ad hoc machine. With distance e-voting, the voter uses his or her personal computer to cast a ballot, sending it over the internet to a central server. The latter is vulnerable to several types of assaults due to its electronic and network-based structure (Bishop, et.al, 2017).

Man-in-the-middle attacks (MITMAs) are one of the most significant and possibly harmful types of attacks that should be considered while developing and deploying secure electronic voting systems (Bojjagani, et.al, 2017). An intermediary party is positioned between the client and server sides in a typical MITMA, eavesdropping their conversations and retransmitting messages as he pleases. Neither party is aware that the private conversation is being unlawfully monitored during the

DOI: https://doi.org/10.34010/injiiscom.v6i2.12595
p-ISSN 2810-0670 e-ISSN 2775-5584

attack. MITMAs can seriously harm both parties to a transaction, from taking control of a session cookie to changing an online payment (Chen, et.al, 2016).

1.1. Types of man in the middle attack

The image below shows the different type of man in the middle attack on an online voting environment.

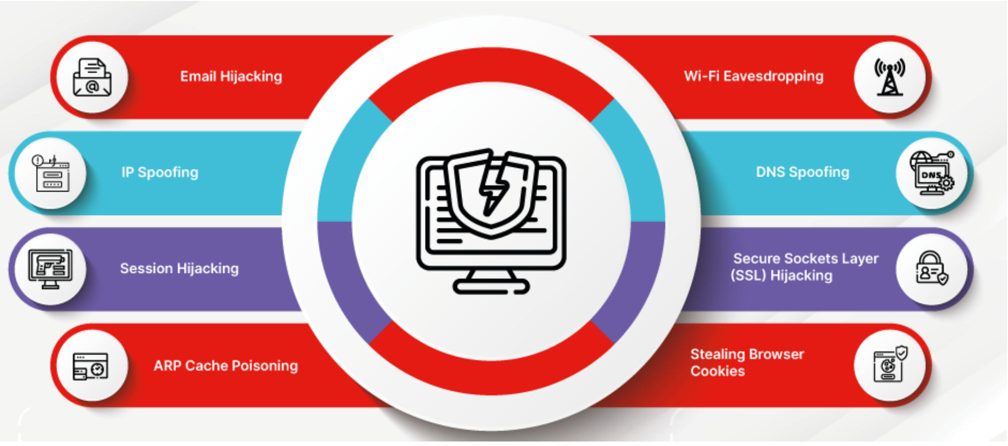


Fig. 1. Man in the middle attack
(Source: Evans et.al,2014)

1. Email Hijacking

As the name implies, fraudsters utilize this type of attack to gain access to the email accounts of trustworthy companies, voters, or castes, which contain important data. Once inside, the attackers can monitor the votes cast and control the polling station's voting process.
Social engineering, or winning the victims' trust, is the key to success in this type of MITM attack (Chen, et.al, 2016).

2. Wi-Fi Eavesdropping

Wi-Fi eavesdropping is a tactic used by cybercriminals to fool users into joining a nearby wireless network that appears legitimate. In reality, though, the network is set up to do malicious tasks. The user might come across the wireless network as being part of a nearby business that they frequently visit, or it might have a name that sounds harmless, like "Free Public Wi-Fi Network." In certain cases, the user may join without even providing a password.

According to Evans et al. (2014), the attacker may monitor the victims' online activities or use the compromised Wi-Fi to obtain login credentials and other private information. Users that are constantly aware of the network they are connected to are the strongest defense against this attack. People who use mobile phones should disable the Wi-Fi auto-connect feature when they are traveling locally to prevent their devices from automatically connecting to a rogue network.

3. DNS Spoofing

DNS cache poisoning, sometimes referred to as DNS spoofing, is the technique of employing altered DNS records to reroute legitimate internet traffic to a fake website that mimics and feels like a website that people are likely to recognize and trust. Like with all

DOI: https://doi.org/10.34010/injiiscom.v6i2.12595
p-ISSN 2810-0670 e-ISSN 2775-5584

spoofing techniques, attackers deceive visitors into inadvertently visiting the fraudulent website by convincing them to take specific actions, such as casting their votes for the candidates they want to support. The attackers gather as much data as they can from the victims during this procedure (Frith, 2022).

4. Session Hijacking

One type of MITM attack called "session hijacking" happens when a hacker waits for the victim to log into an application, like email or electronic voting, before stealing the session cookie. Next, using the cookie from their browser, the attacker accesses the victim's account.

A session is a piece of data that indicates a quick information exchange between two devices or between a computer and a user. Attackers exploit sessions since they are used to determine who has logged in to a website. However, attacks have to move quickly because sessions terminate after a set amount of time, which could be as short as a few minutes (Khusial et al., 2015).

5. Secure Socket Layer (SSL) Hijacking

Nowadays, the majority of webpages indicate that they use a secure server. The initial part of the Uniform Resource Locator (URL) that shows in the browser's address bar is not "HTTP" or Hypertext Transfer Protocol; rather, it is "HTTPS," short for Hypertext Transfer Protocol Secure. The HTTPS, or secure version, will display in the browser window even if users enter in HTTP or none at all. All information communicated with that secure server is safeguarded by this common security protocol (Oppliger, et.al, 2018).

6. ARP Cache Poisoning

Using the Address Resolution Protocol (ARP), a communication protocol, an internet layer address can be linked to a link layer address, like a media access control (MAC) address. An important function of the ARP is to translate the link layer address into the Internet Protocol (IP) address of the local network.

The cybercriminal deceives the victim's computer into thinking that the fraudster's computer is the network gateway by using false information. Instead than using the real network gateway, the victim's computer essentially sends all of its network traffic through the malicious actor once it is online. Using this rerouted traffic, the attacker then examines and obtains all required data, including personal identification (Serpano et al., 2021).

7. IP Spoofing

Redirecting internet traffic meant for a reliable website to a fraudulent one is known as IP spoofing, which is comparable to DNS spoofing (Oppliger et al., 2018). Rather of using a DNS record spoof, the attacker modifies the IP address of the malicious website to appear as if it is the IP address of the legitimate website visitors are intended to visit.

8. Stealing Browser Cookies

Computers store small amounts of data called cookies. Sometimes known as an HTTP cookie, a browser cookie is information collected by a web browser and stored locally on a user's computer. Browser cookies allow websites to remember information, which may enhance the user experience. According to Husial et al. (2015), a user may be able to avoid typing the same information on a form, such as their username, password, and first and last names, if cookies are enabled.

Browser cookie stealing requires another MITM attack technique, such Wi-Fi eavesdropping or session hijacking, in order to be effective. Cybercriminals can gain access to a user's device and use one of the other MITM techniques to do everything an MITM attack can, including stealing browser cookies. Gaining access to browser cookies allows attackers to steal passwords and other confidential data that users regularly store in their browsers.

1.2. Statement of the Problem

The study was birthed due to the constant man in the middle attack that has crippled the online voting system and has led to a major scare in the online Voting Environment.

1.3. Purpose of the Study

The main purpose of this study is to develop an online voting system with multi-layer security that can prevent man in the middle attack. Other specific objectives include:

- Develop a mobile app for an online voting system
- Develop an online voting system that uses, OTP, Captcha, Finger Print Authentication, Cryptography and User Authentication.

2. METHOD

2.1. Parameters required for the proposes system

The created system is an online voting system designed to eradicate man in the middle attack in an online voting environment.

- **User authentication**: In this process admin registers polling officers, contestants and voters
- **Finger Print Authentication**: this process contestant captures their fingerprints, in other to verify if they are the same person in the system
- **Text cryptography**: this encrypts all votes casts, and all contestant's information, so only those with the decryption key than decipher and upload results.
- **Captcha**: secure online transactions and prevent all Denial-of-Service attacks
- **OTP**: this enables the system to send OTP to voters in other to verify they are the ones who want to login to the system.

2.2. Analysis of the existing system

Due to the vulnerabilities in the present system, there are issues with the online voting environment to man-in-the-middle assaults. These assaults often have an effect on the effectiveness and efficiency of the voting procedure as a whole. Other conclusions about the existing setup are as follows:

- anyone with the login details and password can vote.

- votes castes are not secured, as anyone can hack into the system and manipulate the results.
- The system in prone to denial-of-service attack.

2.3. Limitation of the existing system

The existing electronic voting system is limited by:

1. Impersonation
2. Security breach
3. Phishing attack
4. Man in the middle attacks

2.4. Justification of the proposed system

The developed system intends to: -

I. capture face of voters in other to eradicate impersonation

II. II. implement captcha in other to prevent denial of service attack

III. III. Encrypts Vote Cast in other to secure votes in case of any successful attack

2.5. System architecture design of the proposed system

The image below depicts the architecture of the proposed system, that can eradicate or help eradicate man in the middle attack in an online voting environment.

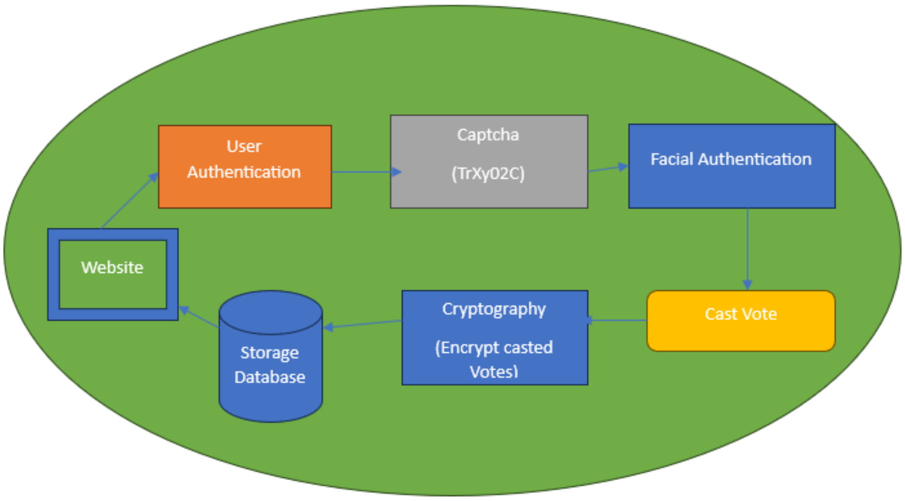


Fig. 2. System Architecture

DOI: https://doi.org/10.34010/injiiscom.v6i2.12595
p-ISSN 2810-0670 e-ISSN 2775-5584

2.6. Flow chart of the proposed system

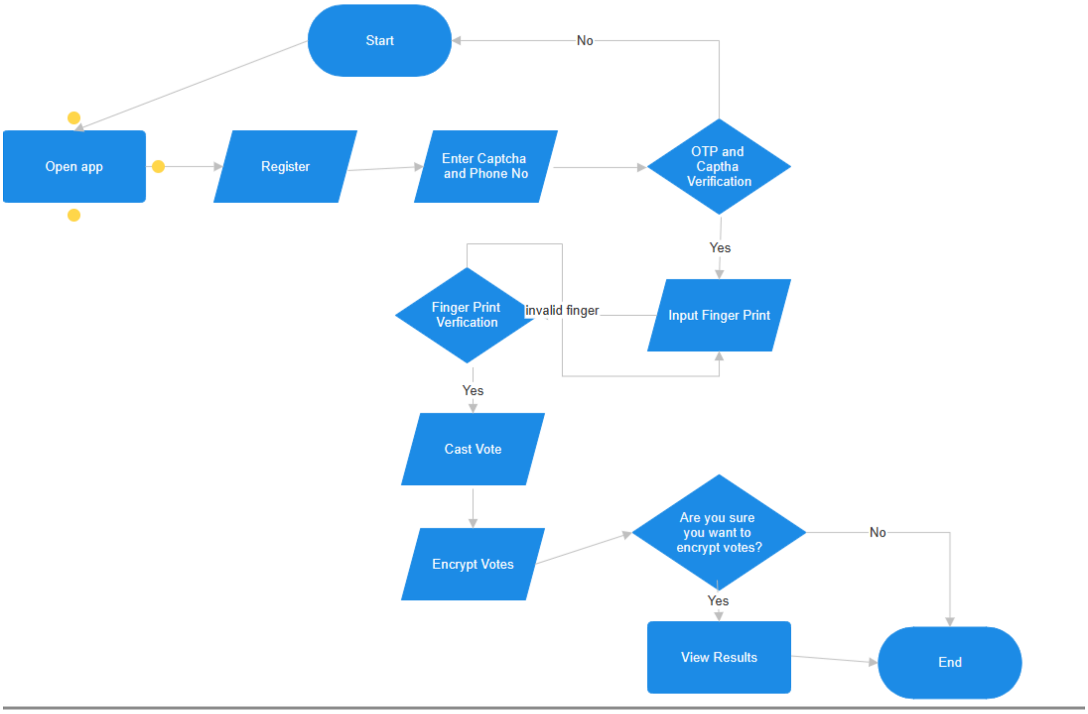


Fig. 3. Flow chart of the proposed system

3. RESULTS AND DISCUSSION

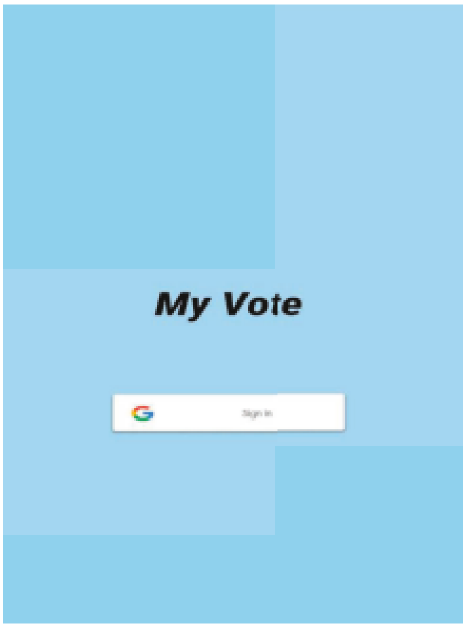
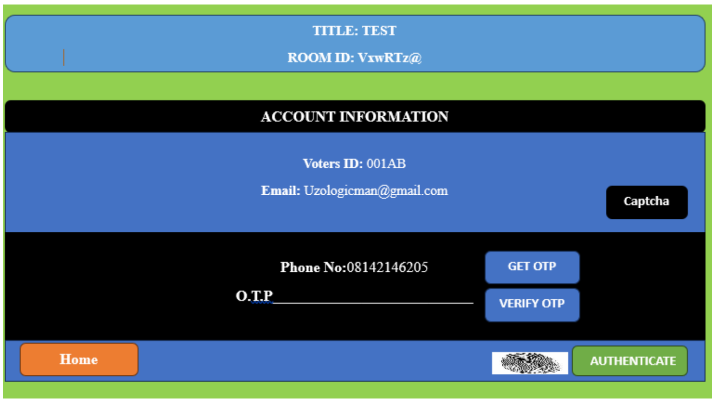


Fig. 4. Registration Page

DOI: https://doi.org/10.34010/injiiscom.v6i2.12595
p-ISSN 2810-0670 e-ISSN 2775-5584



TITLE: TEST
ROOM ID: VxwRTz@

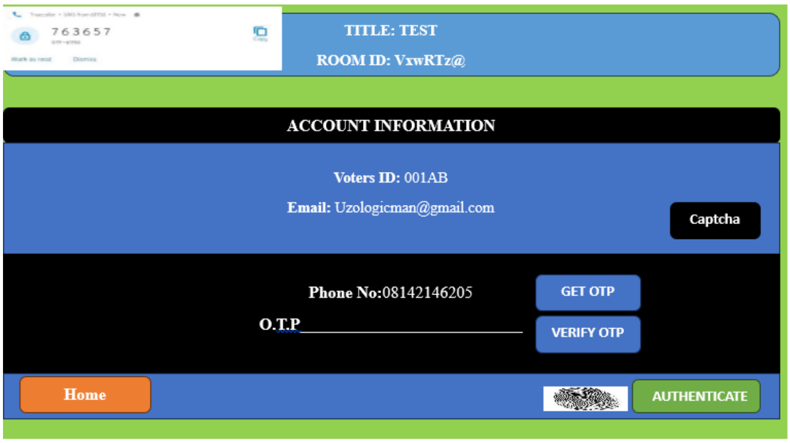
ACCOUNT INFORMATION

Voters ID: 001AB
Email: Uzologicman@gmail.com

Phone No:08142146205
O.T.P

Fig. 5. Account Verification page

This page enables the voters to verify their identity, using Captcha, OTP and finger print attached to their mobile phones



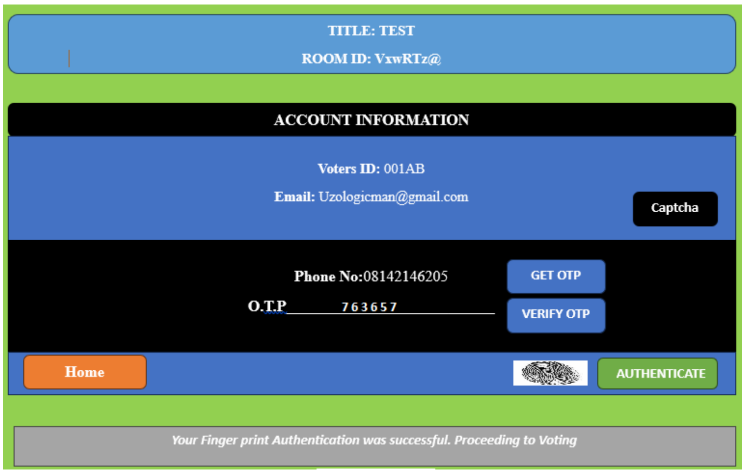
TITLE: TEST
ROOM ID: VxwRTz@

ACCOUNT INFORMATION

Voters ID: 001AB
Email: Uzologicman@gmail.com

Phone No:08142146205
O.T.P

Fig. 6. OTP verification



TITLE: TEST
ROOM ID: VxwRTz@

ACCOUNT INFORMATION

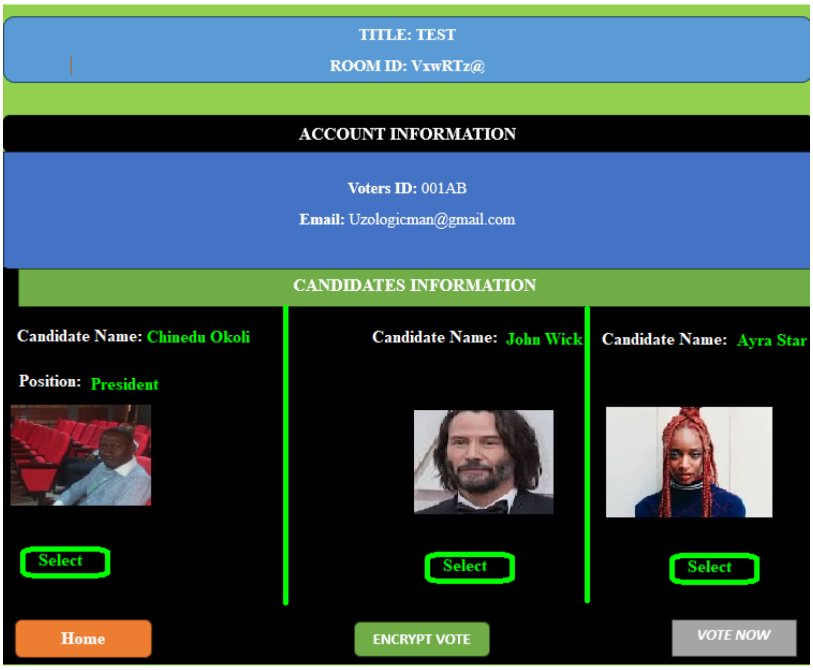
Voters ID: 001AB
Email: Uzologicman@gmail.com

Phone No:08142146205
O.T.P 763657

Your Finger print Authentication was successful. Proceeding to Voting

Fig. 7. Finger print authentication

DOI: https://doi.org/10.34010/injiiscom.v6i2.12595
p-ISSN 2810-0670 e-ISSN 2775-5584



TITLE: TEST
ROOM ID: VxwRTz@

ACCOUNT INFORMATION

Voters ID: 001AB
Email: Uzologicman@gmail.com

CANDIDATES INFORMATION

Candidate Name: Chinedu Okoli
Position: President

Candidate Name: John Wick

Candidate Name: Ayra Star

Fig. 8. Voting Dashboard Firebase

3.1. Programming languages used

1. ((C++ II.) Kotlin III. Java Script iv.) Java

2. Firebase

A. Software Specifications:

1. Android Studio

2. Fire Base

B. Hardware Specifications:

I. Dell inspiron Laptop system

II. 16 GB RAM

III. 500GB Hard disk

IV. 3.0 Ghz Intel Processor (Core i7)

4. CONCLUSION

In conclusion, there are certain hazards associated with the computerized voting method despite its numerous benefits. First and foremost, the system's justice and safety are the most crucial. There are some network hazards associated with the system's necessity to operate over the network, and vote fairness cannot be ensured. Hackers will also be the subsystem's greatest adversary. Voting systems and other technologically complex items are a result of people's dependency on technology in today's world. This is only one issue. Young people thus have little interest in the conventional paper voting mechanism. Conclusively, in order to combat man-in-the-middle attacks and other potential security risks in online voting environments, a multi-level security online voting system with security features was created.

ACKNOWLEDGMENTS

The authors sincerely appreciate the various authors whose work was cited in the course of this study.

Conflict of Interest

DOI: https://doi.org/10.34010/injiiscom.v6i2.12595
p-ISSN 2810-0670 e-ISSN 2775-5584

The authors have no conflict of interest.

Data Availability Statement

All of the data used in this were obtained from online sources.

Funding Information

The authors have no funding to disclose.

REFERENCES

Ali, M. M., Siddiqui, O. A., Nayeemuddin, M., & Rajamani, L. (2015, January). An approach for deceptive phishing detection and prevention in social networking sites using data mining and wordnet ontology. In *Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on* (pp. 1-6).

Arafin, M. T., & Qu, G. (2018). Memristors for secret sharing-based lightweight authentication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *26*(12), 2671-2683.

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*, 139-154.

Bishop, M., & Wagner, D. (2007). Risks of e-voting. *Communications of the ACM*, *50*(11), 120-120.

Bojjagani, S., & Sastry, V. N. (2017). A secure end-to-end SMS-based mobile banking protocol. *International journal of communication systems*, *30*(15), e3302.

Chen, J., & Guo, C. (2006, October). Online detection and prevention of phishing attacks. In *2006 First International Conference on Communications and Networking in China* (pp. 1-7). IEEE.

Evans, D., & Paul, N. (2004). Election security: Perception and reality. *IEEE Security & Privacy*, *2*(1), 24-31.

Khusial, D., & McKegney, R. (2005). e-Commerce security: Attacks and preventive strategies. *IBM Toronto, Canada, Tech. Rep*.

Oppliger, R., Hauser, R., & Basin, D. (2008). SSL/TLS session-aware user authentication. *Computer*, *41*(3), 59-65.

Serpanos, D. N., & Lipton, R. J. (2003). Defense against man-in-the-middle attack in client-server systems with secure servers. *IEICE Transactions on Communications*, *86*(10), 2966-2970.