Computing, Information Systems & Development Informatics Journal
Vol. 13 No. 3, September, 2022 - www.isteams.net/cisdijournal

Towards An Enhanced Smartphone Security Using Distributed Ledger Technology (Blockchain)

Esther S. Alu., Muhammad U. Ogah & Awal J. Yakubu.
[1,2,3]Department of Computer Science
[1,2,3]Nasarawa State University, Keffi, Nigeria
E-mails: estheralu@nsuk.edu.ng; mohammedogah@gmail.com and yawal7363@gmail.com

ABSTRACT

Smartphones have now become an important tool in our daily lives, even to the level of addiction for some individuals. Due to the increase in the usage of cell phones, security issue has become a major challenge in mobile transactions. In this paper, smartphone security/vulnerabilities, and awareness on data security challenges were discussed. Due to big data and massive usage of online data, security implementation in cellphones cannot be under-estimated. However, diverse data protective measures such as fingerprint sensors, Face ID, iris scanner for cellphones and biometric security features, smartphones have existed but could not provide adequate mitigate against any security breach. As a result, smartphone producers encourage their users to safeguard their devices with strong passwords. However, with all of this security counter measures, loopholes still plague the mobile phones such that antivirus software are inadequate in protecting phone users against cyber-attacks. Blockchain is an alternative that evolve to boost the security of transactions using smartphones to clamp down on any possibility of external breach. This paper also expound the use of visual sim technology other than the existing physical Sim cards in providing more security enhancement in smartphones.

Keywords: Blockchain, Smartphones, Threats, Security, Visual Sim technology.

CISDI Journal Reference Format
Esther S. Alu., Muhammad U. Ogah & Awal J. Yakubu. (2022): Towards An Enhanced Smartphone Security Using Distributed Ledger Technology (Blockchain) . Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 13 No 3, Pp 1-.10. Available online at www.isteams.net/cisdijournal

1. INTRODUCTION

Recently, the digital world has experienced transformation of information from one devices to another though cloud services without having to send any information from a remote location. Smartphones are smart technologies that have made this to be possible especially in optimal completion of daily routines and office tasks with access restrictions to sensitive data. However, access to critical information was very porous which crave demand for securing these organizational information from unauthorized users. Therefore, the onset of smartphone technologies paved way for securing critical information by adopting such technologies boosting the aspect of information security as a fundamental task for security professionals. Although, smartphones usage with social media has created huge security challenges in ensuring security of mobile transactions. Various researchers have proposed different studies on smartphone and cloud computing services authentication and security techniques.

Similarly, [Siddiqui, 2018] carried out a comprehensive review and security analysis of various authentication frameworks in cloud computing and smartphones usage. [Siddiqui, 2018] in addition presented the security challenges using different graphs and identified existing authentication presumptions, threats, and other issues necessary to make future suggestions in smartphone authentication domain.

Similarly, the world's population uses android smartphones for online activities such as storing all the sensitive information including pictures, social media account details, emails etc. As per experts' analysis, sadly, android devices lack up-to-date built-in security features, making them a potential target for sniffers, attackers, eavesdroppers and unauthorized users. In the field of cyber-security, consequently, protecting users' android smartphone becomes very crucial. Researchers and cyber experts are researching on efficient and elaborate ways to secure android smartphones from cyber-attacks. Blockchain technology evolves as a modern-day secured technology in developing mobile app, enabling clients to get the best, convenient, and secure mobile transactions. However, security in transactional data is dependent on how data is encrypted into a secured mesh.

Today numerous companies have adopted blockchain technology in their management systems with an increase usage in health care services, governance and supply chain. Blockchain is a distributed network of computers or digital ledger for information storage. Data is synchronized and collaboratively distributed using these computers. When the data within the block is modified, it must reflect in all the computers holding the ledger. The decentralized network can decide to keep or neglect the changes depending on the nature of the change. The distributed network of computers is utilized as servers for mobile apps [2]. The entire system becomes better when developers get more storage and enhanced data streaming.

Initially, the distributed ledger technology started with Bitcoin cryptocurrency and other altcoins such as Litecoin and Ethereum which consequently constitute a claiming giant stride in the crypto-market. With diverse applications of distributed technologies, Blockchain technology becomes the ultimate to combat the increasing cyber-attacks. The prevalence of cyber-attack adequate and prompt attention as it jeopardizes mobile security, privacy and confidential data by hacking into the device. The risks is more with smartphones in certain areas such as hotels, coffee shops, airports, cars, trains, etc. However, home Wi-Fi connections can be potential risk areas without adequate protection against any attacker in accessing confidential personally identifiable information (PII) and data [5]. Nonetheless, this study expound the importance of blockchain technology in smartphones application for mobile transactional security enhancement and effectiveness.

1.1 Benefits Of Mobile Applications In Blockchain Management.

The distributed mobile applications offers the following benefits to their clients. Thus;

(a) Enhanced Security

Blockchain technology provides security enhancement in mobile application utilizing its advanced cryptographic techniques, making it safe and secure when handling transactions using smartphones. Basically, blockchain consists of interconnected blocks of transactions and the blocks provide timestamps to other blocks. Blockchain uses cryptographic has to encode and save all data which makes it extremely difficult to alter any block of transactions. Developers can now spend less time on security and more time building apps as security in mobile application increases using high-level encryption and cryptography, benefiting both the mobile developer and the client seeking mobile development.

(b). High Reliability
Apart from the fact that blockchain enhances the security of smartphones, it also increases the reliability of mobile applications making them very safe for transactional purposes. Globally, data are replicated across multiple devices in different locations as a result of blockchain nodes distributed worldwide. As a result, the mystical belief that blockchain crashing are minimal due to its decentralization stands out to be through except for more enhanced computer systems that could break and penetrate the cryptographic power of the distributed ledger making it easy for cyber-attacks.

(c) Highly Transparent.
The decentralized and distributed record of transactions in blockchain makes it easy for anyone to track transactions globally. Blockchain transparency gives users relaxed mind as they do not need to worry about fraudulent transactions and scams which are almost impossible on the network. The whole distributed platform unmodifiable, incorruptible and scalable. Consequently, mobile apps that use digital technology can easily increase the number of users to meet their requirements.

(d) Enterprise-Level Mobile Apps
Since the resources used to build distributed ledgers are available, developers can easily access them and start developing apps quickly. Also, the technology is open source, therefore developers can contribute to making blockchain even better for improved implementation. Besides, enterprises can benefit from this by giving directives on how their enterprise apps can be developed to suit their needs. However, in the future, government institutions and enterprises will utilize blockchain technology to store data that can't be manipulated. Since this data is viewable by anyone, anywhere and anytime, the information will be transparent and reliable.

2. LITERATURE REVIEW.

2.1 Mobile Phones
In 1983, the first mobile phone (Motorola DynaTAC 800x) with a height of 13 inches and weight of 1.75 pounds, taking about 10 hours to recharge was launched. At the initial launch of mobile phones, hackers find it very easy to clone phone's identity and run any charges on users' account, but as advancement in the phone industry progresses, mobile phones has metamorphosed from the "brick" of the 1980s to the compact and well featured smartphone of today. However, mobile phones is king in connecting users' across the globe for communication, reading news, get directions, stream music, check bank accounts, store assets and so much more. Although, as users and companies increasingly depends on our mobile devices, new measures of attack keeps striving. So much of our sensitive personal information and digital assets such as corporate data and bank account and credit card numbers, are accessible via our mobile devices. They have become treasure troves for attackers.

2.2 Blockchain-based Mobile Phones
Different telecommunication companies have been investing in integrating blockchain technology with smartphones in order to create decentralized devices. Finney from Sirin Labs is one of the first blockchain mobile devices which came to market towards the end of year 2020. Notably, the Finney is comparable price to high-end phones such as iPhone and Samsung models [3]. The Finney phone is a one-stop shop," declared Sirin Labs' co-founder and co-CEO Moshe Hogeg during the launch event. "Before the Finney, you needed a ledger, you needed a computer, you needed wallet software, and then you needed to go to an exchange, and then you could convert. The Finney does all of this in one phone."

Finney is not the only blockchain smartphone currently on the market. HTC offers a blockchain technology on its phone, Exodus 1. The company recently announced a partnership with Bitcoin.com that will see that the Bitcoin Cash (BCH) wallet app is pre-installed on all new Exodus 1 phones. While these initial devices only leverage blockchain technology in order to make cryptocurrency more accessible, people are already considering future possibilities. Phil Chen, HTC's chief decentralized officer, envisions the blockchain smartphone evolving into as a way for people to secure and control their personal data.

2.3 The Future of Blockchain in Smartphones.

With blockchain technology users have control over their online activities and data. In addition, its security and anti-theft capabilities could allow phone owners to use techniques such as social recovery to access their data if their device is lost. They could also blacklist the International Mobile station Equipment Identity number (IMEI) for their lost device. This process allows carriers and smartphone suppliers to quickly identify and disable blacklisted devices in order to protect personal information stored on the phone. However, the advent of De-Web (decentralized web), called "Web 3.0" blockchain and other distributed technologies will provide support to decentralized applications (dapps) on public, peer-to-peer networks instead of private corporate servers.

Blockchain in smartphones provides another benefit such as decreasing the amount of plastic in smartphones. For instance, the United States Patent and Trademark Office granted Verizon a patent for a system that uses blockchain in making V-SIM (Visual Sim) cards. Consequently, the system's blockchain would associate a virtual SIM card (vSIM) with a unique user account, activate the SIM card and then the device will send feedback via blockchain to confirm activation. Although, v-SIM cards aren't new technology as WorldSIM offerred localized v-SIM cards in order to enhance the ability to make local calls. However, visual sim will stop the usage of physical and plastic sim cards as blockchain would help to encrypt user data, making each V-Sim to be unique to a device, the process could become fully digital.

2.4 Smartphones Security Threats.

Smartphones security threats refers to a single and all-encompassing threat. Majorly, four different types of mobile security threats that organizations need to take steps to protect themselves from include [4]:

a) Mobile Application

This happens when smartphone users download apps that look legitimate but actually skim data from their device. Examples are spyware and malware that steal personal and business information without the users knowledge of its occurrence. Social engineering attacks occur when cyber-attackers send fake emails (phishing attacks), text messages (smishing attacks) or voice calls (Vishing attacks) to employees in an effort to trick them into handing over private information like their passwords or downloading malware onto their devices. In the year 2020, reports by cybersecurity firms (Lookout and Verizon) revealed over 37% increase in enterprise mobile phishing attacks, making such attacks the top cause of data breaches globally.

Figure 1: An Example of a phishing scenario.

b) Web-Based Threats

This type of threats are subtle and unnoticeable. It occur when users visit phishing websites that look legitimate on the front-end but in reality, it automatically download malicious content onto the devices. An example of this threat type is Spyware. Spyware is utilized to survey or collect data and is most commonly installed on a mobile device when users click on a malicious advertisement (malvertisement) or through scams that trick users into downloading it unintentionally. Whether the employees have an iOS or Android device, their devices are targets ripe for data mining with spyware, which could include users' private corporate data if that device is connected to the organization's systems.

c) Mobile Network Threats

The usage of public WiFi can led to Network-based threats. This threats are prominent and very risky as cybercriminals can steal unprotected data using WiFi networks. For instance, an encryption gap is like a water pipe with a hole in it. While the point where the water enters (users' mobile devices) and the point where the water exits the pipe (systems) might be secure, the hole in the middle lets bad actors access the water flow in between (figure 2).

Unencrypted public WiFi networks are one of the most common examples of an encryption gap that poses huge risk to organizations. The unsecured network creates an opening in the connection for cybercriminals to gain access to the organization's information between employee's devices and the systems. However, WiFi networks and unencrypted mobile messaging apps poses a threat for cybercriminals with access to sensitive company information.

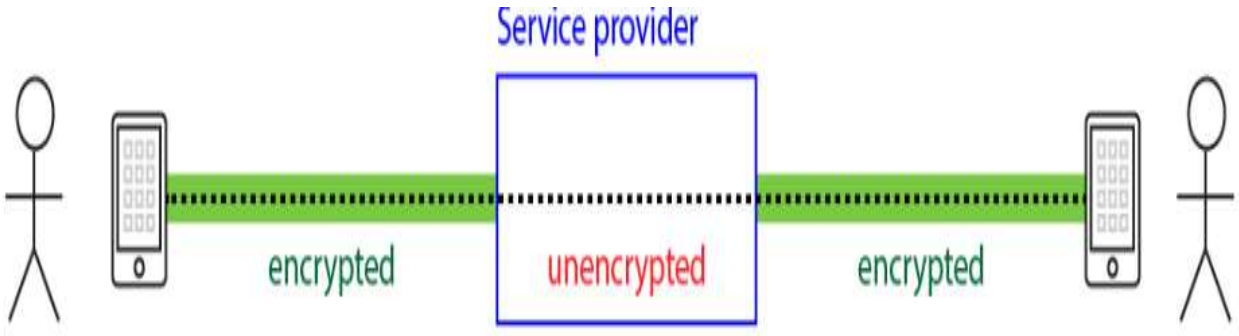

Figure 2: An Encryption Gap.

d) Mobile Device Threats.
These are physical threats to mobile devices due to loss or theft of a device. Since hackers have direct access to the hardware where private data is stored, this threat is especially dangerous to business enterprises. The types of mobile devices that access organization's systems are mainly from mobile phones and tablets to include wearable tech (Apple Watch) and physical devices (Google Home or Alexa). As a result, many of the latest IoT mobile devices have IP addresses which bad actors can utilize to gain access to organizations' network over the internet if those devices are connected to the systems.

2.5 Related Works.
Chin et al [10] presented an analysis of smartphone security practices among undergraduate business students at a Regional Public University. The study revealed that in 2019, the number of smartphone users in the United States was estimated to be over 266 million or 81% of the population. Stating also that smartphones combined with a plethora of apps that are readily available, have become wholly integrated into our daily lives posing a multitude of risks for consumers. The authors further assessed smartphone security practices among undergraduate business students at a regional public university, focusing on security-related practices administered to students in multiple business classes at the university. The results of the survey showed that students exhibit a high degree of care on some measures of security, but lax in other areas. From the result of the survey, males exhibit evidence of some more risky behaviors than their female counterparts. Those who have lost their phones in the past are more likely to be familiar with some disaster preparedness phone features to insure their smartphones. Rassan and AlShaher [11] proposed and implemented a new user authentication mechanism of mobile cloud computing using fingerprint recognition system to enhance mobile cloud computing resources. This study provided a generalized overview, but could not present details of the authentication computations.
Absence of a secure mechanism has made this study vulnerable to parallel processing attacks

Mohini et al [8] stated that android has the biggest market share among all Smartphone operating system and security becomes one of the main concerns for today's smartphone users. As the power and features of Smartphone's increase, so has their vulnerability for attacks by viruses etc. Perhaps android is more secured operating system than any other Smartphone operating system today. Android has very few restrictions for developer, increases the security risk for end users. The authors also reviewed android security model, application level security and security issues in the android based Smartphone. Shahzad et al [9] proposed a survey on smartphones data security, challenges and awareness. The study utilized a user-centric approach to the data protection challenge on cellphones, and examined the needs for data protection systems from the perspective of users' viewpoints. The authors also the types of data that users want to keep private, investigated current users' data-protection habits and demonstrated how the security requirements for various data kinds varies.

3. BLOCKCHAIN SOLUTION FOR SMARTPHONES SECURITY.

The finance domain is constantly been revolutionized and propelled towards convenience and widespread accessibility. Due to this, digital transactions through mobile apps are already becoming a pervasive reality. In a recent survey, banking reveals that over 89% of the respondents utilizes mobile banking for convenience undermining the thought factor of 'safety'. The figures increased to about 97% using smartphones for financial activities. However, as financial transactions move towards mobile applications, security still persists as a major concern for users and organizations alike. The sensitive nature of financial transactions and the threat of possible negative ramifications has resulted in some users remaining skeptical of implementing emerging technology in the financial domain [6].

Similarly, smartphones are easily lost, stolen and susceptible to cyberattacks because of their technological vulnerabilities [5]. Smartphone antivirus protection applications can provide a false sense of security because their effectiveness varies greatly. Thus, users have to take responsibility in ensuring the safety of their professional and personal smartphones and possibly organization supplies to its employees. Although various counter measures (encrypting mobile devices, regularly updating mobile devices' applications and operating systems, setting strong passwords etc.) have being employed to help reduce the risks associated with mobile devices but the introduction of the distributed ledger technologies in an emerging area which promises to totally eliminate smartphones security threats. Blockchain cryptography provides a major security for smartphones due to its unique features of cryptographic encryption, transparency, unmodifiable data structure and security enhancement using digital signature. Employees in organizations uses mobile phones that are connected to the systems, at such security of such devices must be beefed in order to secure data and sensitive information from data breach.

Blockchain technology has the potential to drive significant advancement in the world of mobile finance. The technology is equipped to address the fundamental issues regarding financial inclusion, costs and security. Blockchain has the potential to take mobile apps to the next level of security and accountability, which is of crucial importance in industries like finance technology (fintech) and healthcare. It is a technology that has the power to disrupt institutions ranging from banks to insurance providers and credit unions. Adopting blockchain would not only help businesses retain the competitive advantage, but would also give them an upper hand by adding a layer of security to their mobile apps.

Security leaders can bolster their mobile app security with the technology due to these cybersecurity advantages:

Data Transparency
In the case of blockchain, data is recorded in a manner that can be easily tracked by its users. This makes it impossible to falsify information or create fake transactions, aiding security leaders in their loss and fraud prevention efforts. This renders the system completely impervious to any kind of tampering, which is of crucial importance, especially in the case of mobile banking. In a blockchain ledger, categorization and storage of information can be tracked, verified and secured all at once. As more entries are made, the blockchain expands and more information is automatically added to the system. With complete user authority, blockchain presents a very strong check and balance system.

Blockchain encryption
Complexity in blockchain encryption makes it impossible for unauthorized access for any user without its equivalent decryption key. This lends itself to any system that requires giving access to multiple users but also needs verification of information that is adjusted.

Decentralization
The decentralized architecture of blockchain presents several advantages for mobile apps. It doesn’t have a single point of failure in the system, so any malfunction occurring at the top of the hierarchy poses no negative ramifications to the system itself. The client-server model in decentralized apps is completely distributed. Information and protocols stored on blockchain are encrypted. The apps are usually open-source, with tokens issued for the network users as rewards. The overall network governance is undertaken by an algorithm. Mobile apps use a conventional user and server-side system where the phone and mobile app act as the user and the central server distributes data upon request. With multiple users trying to access the data wirelessly, some of the information is prone to be lost. With decentralization as a result of blockchain adoption, advanced storage and data streaming capacities flow into mobile applications, which presents more opportunities for security leaders.

3.1 Proposed System Architecture

In this study, we analyzed the security features provided by blockchain technology when integrated in mobile applications. Several researches have greatly stressed on security measures in mobile phones for safe activities but advancement in internet, technology and cyber activities tends to describe those previous mobile apps security as inefficient and ineffective for smartphone safety of usage in carrying out any transactions. The proposed system consists of a user's mobile phone IMEI registered on a distributed ledger of transactions. Once a user purchases a mobile phone, the user registers it on the blockchain and its unique IMEI. Every smartphone has a unique identifier attached to its IMEI. Every transactions on the mobile phone is saved on the distributed ledger. In the case of any theft, the mobile phone owner reports same using his private key to sign in to the distributed network and report the fraudulent case. The IMEI is tracked and said to be declared invalid henceforth. Also, the replacement of physical sim with virtual sim is an enhanced way of increasing the security of smartphones safety.

The Virtual sim is linked with other blocks on the nodes, all transactions are tracked and recorded on the ledger. See figure 3 for the proposed architecture of integrating blockchain in smartphones. With a blockchain-enabled vSIM, the private key is automatically generated in the vSIM card and the phone can be easily used for blockchain-enabled authentication and transactions. The SIM (Subscriber Identity Module) is a small chip of varying form factors that has a phone number & carrier associated with it. In order to change carriers or phone numbers, users have to swap between different SIM cards, which can be a nuisance for people and a limiting factor for systems using multiple IoT devices. The emerging vSIM standard embeds all the features of the traditional SIM on a very small programmable chip. This allows phones and devices to seamlessly switch between service providers or even use multiple phone numbers simultaneously, without swapping a card. The programmable memory area in an vSIM will be preloaded with blockchain functionality that allows users and devices to authenticate against blockchain.

With a blockchain-enabled vSIM, the private key is automatically generated in the vSIM card and the phone can be easily used for blockchain-enabled authentication and transactions. The same features will be usable also by IoT devices, whose security is also of high importance, and who will also benefit from the reduced form size and power consumption of the vSIM.

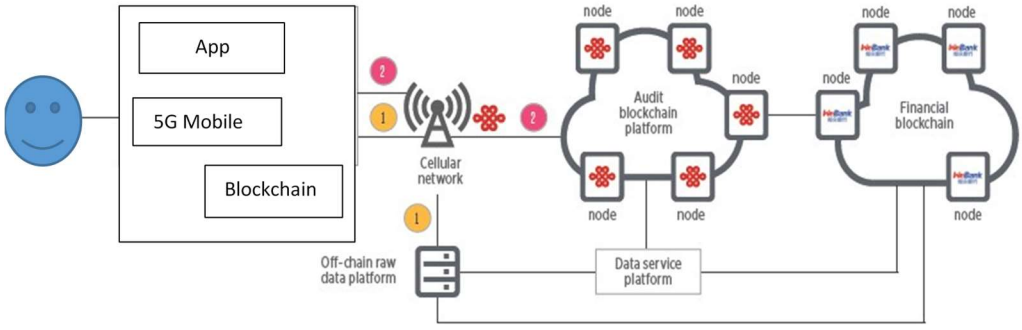

Figure 3: Integrating mobile apps with blockchain technology.

3.2 Challenges In Blockchain Adoption.

The integration of blockchain in the mobile app industry has the potential to transform industries such as banking, finance, insurance and healthcare. However, the following challenges impair successful implementation of the distributed ledger.

i) **Network limitations**: Since blockchain is a network-based technology, assumptions are made based on the network size, which makes the computation of its return on investment a challenge for the businesses.
ii) **Cost**: The blockchain network is dependent on high computing power and thus needs a huge amount of electricity consumption in verifying and validating transactions by the miners.
iii) **Speed**: Transaction processing in blockchain is slow compared to the conventional transaction processing systems that has the ability to process tens of thousands of transactions per second. This poses a challenge in large scale applications.
iv) **Interoperability**: Despite the numerous and unique features on blockchain, it is also said that the distributed networks work in siloes and fail to communicate with other peer-to-peer networks. Besides, lack of standardization hinders interaction between the various networks. The variation in protocols, programming languages and consensus mechanisms make interoperability a major challenge in blockchain. However, efforts are ongoing to provide counter measures to these challenges in the development of blockchain applications. Although, despite the challenges of this technology, the decentralization, encryption and transparency provided by blockchain can serve as an asset to cybersecurity professionals working to secure mobile applications and transactions from fraud and other cyber-crimes.

4. CONCLUSION

As blockchain technology continues to evolve, it has increasing opportunities to help advance autonomous vehicles, healthcare, supply chain, and the Internet of Things (IoT) with its secure network. Companies and businesses are looking to do ways to improve their transactions in terms of security, convenience, and reliability. That has prompted them to seek blockchain solutions because it provides all these features. The technology has substantially improved and is now incorporated into mobile app development. There are numerous companies using blockchain in their apps, including Facebook, Coinbase, and Blockone. This is meant to make transactions fast and secure for both clients and these companies. The beauty of using blockchain is that anyone can access information anytime, anywhere, using any device, making mobile apps built-in blockchain technology convenient. The integration of vSIM and blockchain is however still in its early stages, as is blockchain technology itself. So there is plenty of time for blockchain SIMs to mature and offer connected people & devices with increased security & versatility while reducing device size, making them ready for the next massive technological leap.

REFERENCES.

1. Seker, E. Is More Secure and Stable Communication Possible by Using Blockchain Technology For eSIM? 2021.https://ensarseker1.medium.com/is-more-secure-and-stable-communication-possible-by-using-blockchain-technology-for-esim-b99225ec4675
2. https://www.mobileappdaily.com/how-blockchain-impacting-mobile-app-security.
3. https://innovationatwork.ieee.org/blockchain-smartphones-going mobile/#:~:text=Blockchain%20technology%20can%20give%20users,if%20their%20device%20is%20lost.
4. Gontovnikas, M. The 9 most common security threats to mobile devices in 2021. https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/
5. Blagojevic, N. Smartphone Security:Tips for protecting your PII on mobile devices. 2016. Fraud. Magazine. https://www.fraud-magazine.com/article.aspx?id=4294992799.
6. Varshneya, R. Securing mobile applications with blockchain technology. Security Webinar. 2022. https://www.securitymagazine.com/articles/97078-securing-mobile-applications-with-blockchain-technology.
7. Siddiqui1, Z, O. Tayan And M.K Khan.Security Analysis Of Smartphone And Cloud Computing Authentication Frameworks And Protocols Special Section On Security Analytics And Intelligence For Cyber Physical Systems. 6(2018). 34527-34542. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8374417
8. Mohini, T., S.A Kumar and G. Nitesh. Review on Android and Smartphone Security. Research Journal of Computer and Information Technology Sciences. ISSN 2320 – 6527. 1(6). 12-19. November (2013). Res. J. Computer and IT Sci.
9. Shahzad, L; E. Ahmad; T. Sadiq and F.Sohail. A Survey Paper on Smartphones Data Security, Challenges and Awareness. 2022. 2022 International Conference on Decision Aid Sciences and Applications (DASA).
10. Chin, Amita G.; Little, Philip; Jones, Beth H. An Analysis of Smartphone Security Practices among Undergraduate Business Students at a Regional Public University. International Journal of Education and Development using Information and Communication Technology. 2020. 16(1). 44-61.