International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

NFC – Blockchain as a Secure Solution

Mahesh V

Abstract: ***Near Field Communication (NFC) has remained as attractive from many years for customers as trendy for portable devices. Its utilization is growing day by way of day by fast pace as expand in the accessibility of the NFC enabled devices in the marketplace. It is developed for the integration with handy mo-biles, which could communicate with each other mobiles or read information on tags and cards. NFC device can also be used in card emulation mode, to provide flexibility with contactless smart card devices. This is very affective in allowing NFC enabled smart-phones to exchange typical contactless plastic playing cards used in public transport, get entry to control, ATMs and different comparable applications. The most pertinent concern would be that how a good deal inclined the new technological know-how is and it is evaluated to many susceptible types of out-breaks. This research provides solution to this hassle using blockchain technology.***

Keywords: Blockchain (BC), Secure element (SE), Data Ex-change Format (NDEF), Near Field Communication (NFC), Radio frequency identification (RFID), Internet of things (IOT).

I. INTRODUCTION

Near Field Communication functions at restrained vary by Wi-Fi exchange machinery. It practices the simple communication arrangements of Radio Frequency Identification (RFID). It functions on 13.56 MHz frequency with information fee of 424 kilobits per second with a distance of 10 centimeters. NFC enabled systems could communicated with other devices when they are touched in the working range. NFC technology is the main source of numerous applications in a variety of corporations like property documentation verification and tracing in chain administration, public ticketing in transportation coordination, get right of entry to regulate systems and verification of folks via practice of identification cards and also passports.

NFC consists of three usual machine running methods: (1) Card Emulation mode, (2) Reader/Writer mode, and (3) Peer-To- Peer mode [2]. NFC emulation includes two mobiles for the communication purpose with one initiator and target device. Initiator begins the communication and it is classically an energetic NFC system.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Mahesh V*, Assistant Professor, Department School of Computer Science and IT, Jain (Deemed-to-be-University), Bangalore, Karnataka, India, E-mail: v.mahesh@jainuniversity.ac.in.

Initiator is the one who is accountable for stimulating the goal in situation the target system is a inactive system as it holds an power element which could produce dynamism for the target device also. The target gadget can be an RFID tag, this is primarily works on the principle of NFC device.

The objective of this device is to reply to the requests created by the initiator with related to responses [1]. NFC based totally cell strategies classically smart mobile are generally used in both reader and tag styles concurrently by using smoothly using the interface handy on the mo-bile screens. Applications established for smart phones consist of a range of make use of NFC technologies.

Blockchain technological know-how is most clearly described as a decentralized, distributed ledger that data the provenance of a digital asset. Blockchain technological know-how is a new technology integrates reorganization, dispersed calculation, potholed encryption, timestamp, agreement process. It affords a disbursed ledger that streamlines the account settlement technique over encryption strategies and dispensed message broadcast etiquette, and preserves a huge volume of information thru decentralization. Hence, it is capable for the enhancement of records processing competence, and presents information sharing characteristic whilst nevertheless making convinced data security. So, evaluating to normal skills, blockchain technology is outfitted with the assets of sustainability, compatibility, statistics allocation, and interconnectivity [2]. As the science matures, it anticipated to see greater and extra real-world applications using blockchain. Many blockchian developers foresee that there will be extra NFC gadgets in the future and subsequently there is an exigent need for a native NFC mechanism built without delay on the blockchain network in the spirits of decentralization and disintermediation of the community itself in greater tightly closed way.

II. NFC OPERATIONAL MODES

A. Emulation of card mode

Primarily all Smart mobile devices act identical to a contactless smart card when we practiced in emulation of mode method. The same method is also practiced in NFC and primarily based on fee and ticketing constructions on smart mobiles. Smart mobiles use the applications of libraries of present groundwork of smart cards. An ISO-14443 smart-card behavior is replicated via the NFC controller of the mobile phone executing device. These cellular units can also be used in normal smart cards for repayment transactions or physical entry regulations etc. Here, the NFC controller works as a gateway to channel the secure information and instructions from the card software on the cellular machine to the getting bare hardware. In this method NFC regulator itself does no longer rise out any calculation.

The above operation is also called as Host-based card emulation in present day and has been bundled by Google with the Android 4.4, Kitkat. Operating system creates reply to the NFC traffic flow predictable from outside readers.

B. Writer/Reader mode

It approves the smart-mobiles to read data from NFC devices or smart cards comprising RFID labels. The identical smart mobile could be used in writer mode where it can be used to write ticket info on the absolute and un-initialized labels. Then NFC enabled smart device can read NFC labels, like NFC enabled smart poster labels.
A person can recover label facts stored in the label for in addition movements afterwards.

C. Peer-To-Peer mode

For any communication two devices needed to works as dispatcher and receiver and it is an inactive device. Two way communications happen among two NFC enabled devices to interchange data. The channel for messages among two devices happen using the indistinguishable channel in half duplex mode. NFC Data Exchange For-mat or NDEF is a uniform design which is used to accumulate data on labels. It also requires the requirements for transport of information amongst two NFC gadgets in device to device mode method.

D. Wireless Charging mode

In this mode Small IOT gadgets such as a Bluetooth headset, health tracker or smart watch can be charged with the contact-less switch of up to1 W of power.

III. RELATED WORK

NFC conversation happens in wireless manner which is very inclined to the possibilities of snooping. It is a key to danger in wireless communiqué which includes extra properties to quit such events. Communication amongst two devices with NFC frequency can be intercepted or acquired with the aid of an invader in the neighborhood of the NFC enabled devices. The invader can use better and operative antennas compared to cellular gadgets to receive the communication. This allows the invader to snoop an NFC communication with longer distances. The information conveyed completed through NFC interface can be reformed via an invader if he can capture it. The information exploitation can be regarded as denial of service if the invader deviates the information in an un-known format. The discussion among the sender and receiver could be disturbed. This disruption can be temporary if the invader has centered on the broadcast medium among the NFC devices. If the facts deposited on the labels or in the storage of the mobile devices is despoiled than it marks that particular label to be unusable and the mobile system would be mandatory to get back the information once more [2].There is another way to fraudulent the records can be by means of transmission of the identical frequencies at the stretch when genuine units strive to connect with each other device. This kind of exploitation could be carried out by using malevolent software executing on the similar smartphone in background. This kind of assault does no longer fraudulent the authentic facts but the data received at the receiver give up is tarnished. It develops a Denial of Service attack. To go onward from information corruption to information alteration, invader vicissitudes the genuine information with the valid, however it is improper information. The target device receiver receives records deployed by way of the attacker in the course of its broadcast. The occurrence requires know-how of the invader in the area of wireless and radio communication where attacker can play and take care of the plenty of inflections of the broadcast. Reprobate and undesirable records can be introduced in the form of communications via an invader into the records whilst being exchanged among two NFC devices. The achievement of invader in this operation depends on the period of conversation and the reply of time of the getting devices. For a NFC system, sensitive data and codes ought to be saved on a Secure Element (SE) platform as an alternative of visiting untrusted software program aspects [5]. Some different applications such as malicious ones will disturb except an impenetrable execution environment. SE has the same excessive security standards as the common smart card, which presents impenetrable storage, invulnerable execution surroundings and encryption algorithm primarily based on the hardware to withstand a range of assaults when the facts storage is study and operated. But distinct manufacturers execute unique modes and solutions, protection vulnerabilities nonetheless exist such as whether or not SE is locked and Application Programming Interface (API) is lack of coding signature [5]. Block chain innovation offers with the human provider administrations to supply invulnerable records sharing amongst exclusive partners, records interoperability, adaptable and fast charging. In Today's world, the technology has a fast increase in its upcoming future with a considerable digital transformation by way of making a higher substitute each day. Internet of things, detecting advancements, and 5G are the quickest creating innovation offers a markable dedication to human provider administrations [6]. In NFC label offerings like smart poster, smart coupon services, smart ordering, etc., NFC Data Exchange Format (NDEF) memorandums are transported from label to mobile for change the data. However, there is no correct way to recognize the consumer whether the NDEF communication comprise the spyware or malwares. Furthermore, the invader might overwrite the NDEF communications or change the label for transmission of the malware into target's device for identical cause with smashing assaults [7]. Blockchain has obtained more and extra interest because of its attainable to decentralize, two disinter mediate, and enable `trustless' interactions [11].

IV. PRESENT SECURITY IN NFC

When NFC card emulation is excellently furnished the use of a secure element, the card to be emulated is provisioned into the secure element on the system via an Android application. Then, when the user holds the gadget over an NFC terminal, the NFC controller in the gadget direct all records from the reader at once to the secure element as proven in the following discern [4].

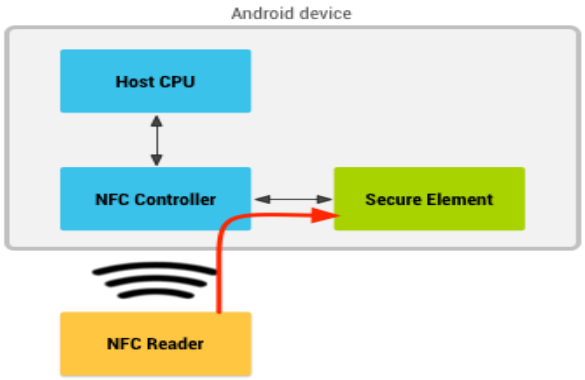

Figure 1: NFC card emulation with a secure element.

V. METHODOLOGY USING BLOCKCHAIN MODEL

The nice strategy to defend towards most attacks is to use a impervious blockchain technology is the answer between the communicating devices. Owing from the controlled hardware useful source of NFC devices, the application of the NFC for any transaction withdrawal process can also a reason for system lost time or some other difficulties. Therefore, this research proposes a peer-to-peer recording machine. With this machinery, each NFC device can be located to another system in the blockchain community through the individuality registration procedure, and then take part in the confirmation and conservation of the whole NFC enabled device blockchain.

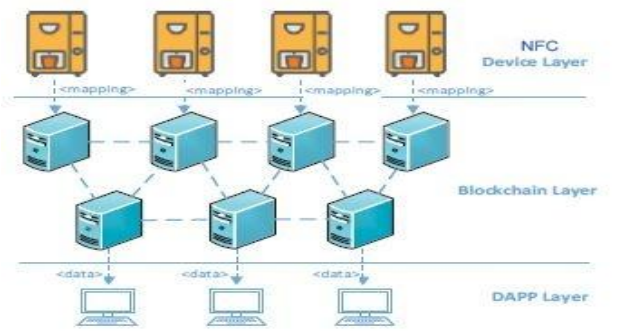

Figure 2: NFC devices with blockchain model

The above devices can be either a lightweight or a Block creator system. Smart NFC gadgets can share user usage information in the blockchain set-up with the help of this system and acquire rewards afterward the information is used up and it can be reused with other users.

VI. COST OF THE MODEL

NFC enabled systems must pay a definite quantity of tokens to add customers transaction information, so that we can prevent the machine from nastily importing a illegal records and inflicting network crowding. At that peak time, saving node generates a block, it will acquire a positive wide variety of tokens as remuneration, this process encourage greater devices to contest for block chain, and jointly hold the consistency of the blockchain ledger. DAPP inventors, who improve customized so-licitations for NFC enabaled devices, must pay a definite quantitiy of tokens for installing DAPP to the blockchain, and the same tokens should be earned from DAPP users as a facility burden. To attain the consistent info resources, the information customer has to pay certain amount of tokens to the information creator earlier than the usage of the data. Normal users of NFC enabled units might attain positive token rewards after the usage of NFC gadgets and use these tokens to change items or offerings from a range of NFC gadget operators.

VII. RESULTS

In this research we have explained the introduction of NFC technological knowledge with different styles of procedures. The utmost common and viable dangers to the NFC communications which has been registered and accompanied by using the proposed answer with the powerful blockchain technology in protection of opposition to them with more secure way.

VIII. CONCLUSION

NFC does no longer challenge the concept of security in entireness and it needs the inclusion of trendy cryptographic performs to shield its communication frequency and the records while being at rest in transportation. Blockchain applications in NFC can shield contrary to most outbreaks. With blockchain conversation through NFC frequency is covered in opposition to Man-in-Middle outbreak outstanding to the small distance of conversation time. NFC has big opportunities and it is being used in our day to day applications where it can deliver comfort in numerous activity tasks like mobile payment methods, ticketing machine in transport and get admission to manipulate many approaches.

REFERENCES

1. N. A. Chattha, "NFC — Vulnerabilities and defense," 2014 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, 2014, pp. 35-38.
2. S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou and B. Zhang, "A High Performance Blockchain Platform for Intelligent Devices," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, 2018, pp. 260-261.
3. https://nfc-forum.org/resources/what-are-the-operating-modes-of-nfc-devices on March 2020
4. https://developer.android.com/guide/topics/connectivity/nfc/hce on March 4, 2020.
5. W. Fan, W. Huang, Z. Zhang, Y. Wang and D. Sun, "A Near Field Communication(NFC) Security Model Based on OSI Reference Model," 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, 2015, pp. 1324-1328.
6. M. S. Christo, A. M. A., P. S. G., P. C. and R. K. M., "An Efficient Data Security in Medical Report using Block Chain Technology," 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2019, pp. 0606-0610.
7. J. Baek and H. Y. Youm, "Secure and Lightweight Authentication Protocol for NFC Tag Based Services," 2015 10th Asia Joint Conference on Information Security, Kaohsiung, 2015, pp. 63-68.
8. A. Al-Haj and M. A. Al-Tameemi, "Providing security for NFC-based payment systems using a management authentication server," 2018 4th International Conference on Information Management (ICIM), Oxford, 2018, pp. 184-187.
9. A. Al-Haj and M. A. Al-Tameemi, "Providing security for NFC-based payment systems using a management authentication server," 2018 4th International Conference on Information Management (ICIM), Oxford, 2018, pp. 184-187.

10. R. Wang, J. He, C. Liu, Q. Li, W. Tsai and E. Deng, "A Privacy-Aware PKI System Based on Permissioned Blockchains," 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2018, pp. 928-931.
11. S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 184-193.
12. Homoliak, S. Venugopalan, Q. Hum and P. Szalachowski, "A Security Reference Architecture for Blockchains," 2019 IEEE
13. International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 390-397.

AUTHORS PROFILE

Mahesh V working as assistant professor in school of computer science and IT, Jain(Deemed-to-be-University), Bengaluru-560 069, Karnataka, India, E-mail: v.mahesh@jainuniversity.ac.in. Eight years of teaching experience and currently perusing Ph.D. in spyware using data mining techniques. An area of interests includes machine learning and blockchain, cyber security and data science.