DNS Security - Prevent DNS Cache Poisoning Attack using Blockchain

Mukesh Kumar Bansal, M. Sethumadhavan

Abstract*: The block chain is attaining popularity day to day as it is acting as distributed ledger for Cryptocurrency such as Bitcoin and ripple. This research paper has focused on the Blockchain and its working pattern with technical implementation of block creation. This technical paper is considering the prevention of DNS Cache poisoning attack in Blockchain which is known as larger class of name-based attacks. DNS Packet interceptions may be made using various attacks like Cache poisoning attack, man-in-the-middle attacks etc. As there are numerous security mechanisms to secure the Blockchain but in order to make Blockchain immune from cache poisoning attack, there is need to update the block creation module. Therefore, this research work is proposed to make reduction in probability of data corruption that can be created from different attacks. It resolves the issue of cache poisoning attacks using user defined port instead of predefined port. However, the initialization of transmission is performed here using predefined port number. In second step, the encrypted port number is decrypted to initiate communication using user defined port number. The use of port with IP address would restrict attacks during data transmission. The paper has presented the comparative analysis of existing DNS attacking prevention mechanism to proposed work.

***Keywords*: Block Chain, Cache poisoning, DNS Attack, PORT.**

I. INTRODUCTION

A. The Blockchain approach

Blockchain is a distributed ledger technology. It was developed as an object related to intense interest in tech business as well as beyond to it. Blockchain technology is a way to maintain the record of transactions or digital interaction. This technology is designed to secure and make transparency in the transactions. It is highly resistant to outages withaudit ability as well as the efficiency. It decreases the chances to disrupt the industries and allow the innovative models. This technology is innovative and being updated continuously. In order to avoid the disruptive surprises as well as to get the better opportunities, strategists, planners are required to pay attention now. They should investigate innovative models of Blockchain. Blockchain technology is known as a distributed database which has been used to record a rapidly increasing the set of data records securely.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author

Mukesh Kumar Bansal*, Center of Cyber Security, Amrita University, Coimbatore, India. Email: b_mukeshkumar@cb.students.amrita.edu

Dr. M. Sethumadhavan, Head of Centre for Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore, India. Email: m_sethu@cb.amrita.edu

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

It is shared naturally, means to say that no master computer is required to hold the whole chain, instead there are copies of chain for included nodes. It is ever-growing and data records are added to chain.

Two types of elements are there in a blockchain:

- **Transactions**: Transactions have been known as the actions. These are generated by the nodes in a block chain system.
- **Blocks:** Blocks are able to maintain the record of transactions. These ensure the correct sequence of transactions.

B. Advantages of Blockchain

There are several benefits of this technology. The main advantage of Block chain is that it is publicly able *to use*. Every user has the authority to see the blocks as well as the transactions which are stored. The records of transactions are secured using private key. It also can be configured to be used as private Blockchain where nodes are added in chain after authorization.

The technology of Blockchain is not *centralized*. Therefore, no single authority is there who provide the approval for the transactions. No any single entity can set specific rules related to acceptance of transactions. Mean to say that it is a secure system because the approval of a set of (selected based on defined algorithm, called smart contract) the participants is necessary to accept transactions.

It is very important thing that it is *secure*. One can extend the database but not can make changes in previous records.

C. Working of Block Chain

When a new transaction is added to chain, a minimum set of participants provide the validation to this transaction. Apply an algorithm (smart contract) to verify the transaction. The exact number of participants to validate the transaction can be defined using the Blockchain system. It can vary as per the systems. It is required that the majority of the participants must be agreed on the validation of a transaction. After that, a set of verified transactions is put in a block which is transferred to all nodes in a network. The participants verify the additional block. Every successive block includes a hash which is specific fingerprint, of existing block.

Systems of Block chains are secured with shared computing system that provides the high Byzantine fault tolerance.

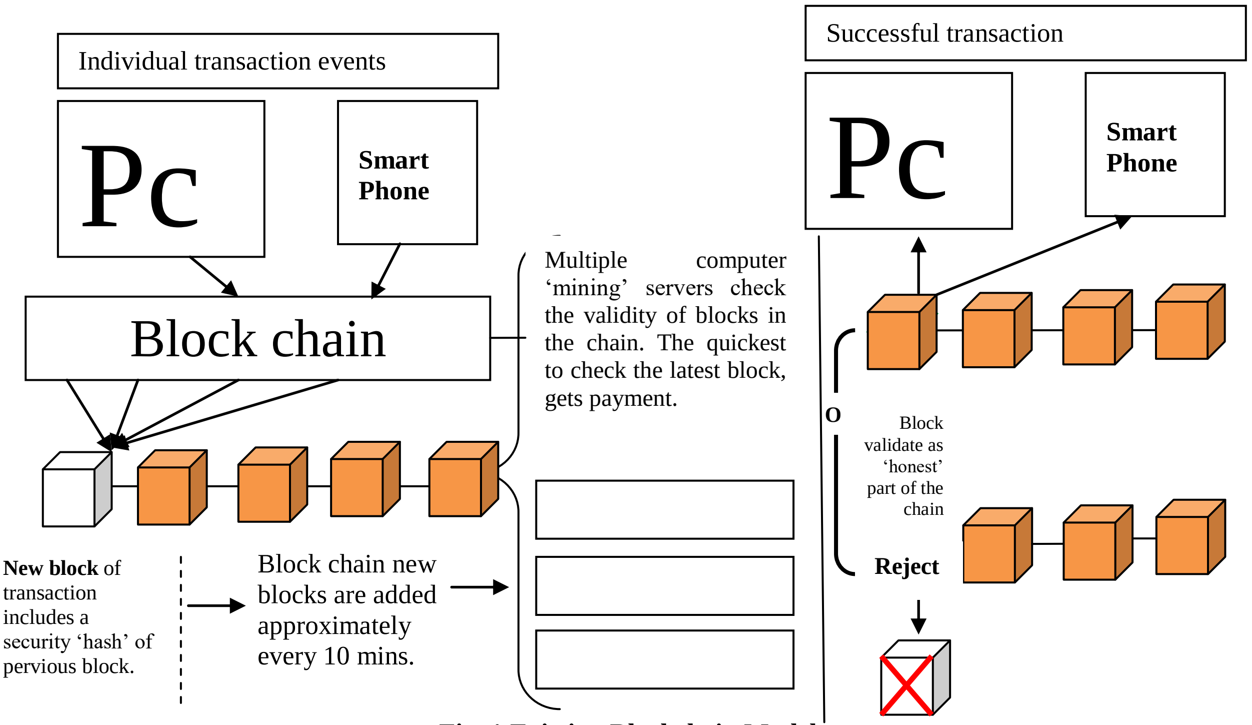
Individual transaction events
Pc
Smart Phone
Block chain
Multiple computer 'mining' servers check the validity of blocks in the chain. The quickest to check the latest block, gets payment.
Successful transaction
Pc
Smart Phone
O
Block validate as 'honest' part of the chain
Reject
New block of transaction includes a security 'hash' of pervious block.
Block chain new blocks are added approximately every 10 mins.

Fig. 1.Existing Blockchain Model

D. ISSUES IN CASE OF BLOCK CHAIN

Along with the benefits of the Blockchain model, some shortcomings and issues are also considerable. These are discussed here such as:

- There are some scalability issues in Blockchain that leads to centralization. It is shadow on the future of cryptocurrency in future.
- In a blockchain-related ecosystem, Processing power as well as the time is required highly in order to do encryption for all objects.
- Storage is also a hurdle in a blockchain-related ecosystem. Blockchain reduces the requirement of a central server which is to store transactions as well as the device Ids. On the other hand, the ledgers are stored on nodes themselves. The ledger will make increment in size as the time spends. It is far from efficiency of smart devices. These smart appliances are sensors etc. having very low capacity to store the data.
- DNS Packet interception is made by man-in-the-middle attackers, eavesdropping etc. DNS sends whole query or response in a single unsigned. Not encrypted UDP packet creates very easy for such attackers to attack ondistributed or transit network. DNS is vulnerable to both DoS and DDoS attacks.

E. MOTIVATION

Current DNS System deployed is prune to threats like Cache Poisoning, DoS and DDoS attacks etc. Blockchain can be used to secure DNS systems as Blockchain technology may provide security integrity of files that are stored in database. It may be obtained applying well-formed transactions. For this, authentication as well as the auditing is also used which is offered by block chain. There may be the decrement in the amount related to the threats to data integrity.

Blockchain based applications also have challenges like the bitcoin mining has become a great challenge due to requirement of costly graphic cards and high speedinternet. The hashing algorithm are required to be processed in order to perform mining of crypto currencies like as Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Dogecoin, etc.

The issue with crypto currency mining that are based on Blockchain technology are as follow:

1. Crypto currency is not authenticated in several countries.
2. In some countries, crypto currency is banned.
3. There is requirement of high speed internet for crypto currency mining.
4. There is lack of reliable exchange to buy and sell crypto currency.
5. The mining of crypto currency requires lot of power consumption.

Motivation here is to fix the existing Blockchain issues and use it to provide secure DNS Solution.

The objectives of the research are as follow

1. To make study of working process of Blockchain.
2. To study the crypto currencies those are based on Blockchain technology and are popular.
3. To investigate the challenges, Data Integrity issues related to DNS attack in Blockchain Security.
4. To develop a proposed model to enhance the security from DNS attack in Blockchain to make this system more authentic using port encryption to get acceptance of government of countries.

II. REVIEW CRITERIA

Several research work is there related to Blockchain. Some traditional work is considered and discussed in this section.

In 2015, Gareth W. Petersz , et.al.[1]described the understanding modern banking ledgers. In the research work,a Blockchain technology was used. This technology is the future of transaction processing. In addition, this is used in smart contracts over internet related to money.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In the research work, they also offered an overview related to the Blockchain technology. They also discuss the efficiency of these technologies in order todisturb the banking sector. For this,global money remittance is facilities. In addition, the smart contracts, computerized banking ledgers as well as the digital assets was also considered in their work.

In 2016, Jesse Yli-Huumo1, et.al.[2]provided the research work on Blockchain methodology. In research work, the researchers conducted a systematic mapping study. They also considered all relevant researches of this technology. In addition, they cleared that their objective was to understand the present status of block chain. They discussed the issues with the future directions related to Blockchain technology.

In 2017, Igor Zikratov, et.al.[3]reviewed the data integrity applying the technique of block chain. It is well know things that the Blockchain is a relatively new technology. In this technique, there are several possibilities developed in 2009.It was defined as a public ledger related to all transactions of Bitcoin. In addition, the researchers also investigated on blockchains. The investigation was made on the base of storing, retrieving and sharing of files in decentralized network

In 2017, Edoardo Gaetani, et.al.[4]discussed the Blockchain-related Database. They considered the Data Integrity.This technology is designed to secure and make transparency in transactions. It is highly resistant to outages with audit ability as well as the efficiency. It decreases the chances to disrupt the industries and allow the innovative models. This technology is innovative and updating very continuously. In order to avoid the disruptive surprises as well as to get the better opportunities, strategists, planners are required to pay attention now. They should develop the innovative model related to Blockchain. In the research work, they told that this technology is a database which can be used to record a rapidly increasing the set of data records.

In 2017, JunHakPark, et.al [5] wrote on Blockchain based data logging. In the research, they explained the integrity management system. In order to resolve the issues exist in the previous system, the Blockchain related data logging was proposed. Additionally, they also provided the comparison between the performance of the proposed work and existing systems.

In 2017, Zibin Zheng, et.al.[6]discussed an overview of Blockchain technique. In the research work, they also discussed the architecture, consensus as well as the future trends. The researchers stated the overview related to the Blockchain system in first. After that they compared specific consensus algorithms. These are used in several blockchains. Additionally, the technical issues as well as the recent updatesare also listed in the research work.

In 2017,A. Shanti Bruyn et al.[7] wrote on Blockchain and provided an introduction of blockchain. The research work was made in order explore the blockchain. It has become clear by the research work that the Glossary may be beneficial for new system in future.

In 2017, Jin Ho Park, et.al.[8] proposed Blockchain security with challenges, & solutions.. In their work, they explained Blockchain technology and its bright research trends. Additionally, they studied and explained the use of Blockchain security. They also considered the solutions for the security of Blockchain.

In 2017, Ivan Martinovic, et.al.[9] proposed Blockchains used in Governmental Services. They also discussed the Design Principles, Apps, as well as the Case Studies. The technologies of block chain are used in public life as well as in governmental services. It provides the considerable efficiency along with the security benefits. If one see this technology by the technical perspective, he will find this technique simple and efficient methods..

In 2017, Sönke Bartling et.al.[10] provided the research work on Blockchain used in science and for knowledge creation. This technology is designed to secure and make transparency in the transactions. It is highly resistant to outages with audit ability as well as the efficiency. It decreases the chances to disrupt the industries and allow the innovative models. This technology is innovative and updating very continuously. In order to avoid the disruptive surprises as well as to get the better opportunities, strategists, planners are required to pay attention now. They should investigate in the technology related to Blockchain. This technology is known as a database which has been used to record a rapidly increasing the set of data records.

In 2017, An Binh Tran, et.al.[11]stated Regerator in the research work that is a Registry Generator for Blockchain. The registry can bedefined as a list related to the data recorded by an authorized person. There are the needs to secure the Registries for data integrity as well as for the availability. The security is required to make the connection of one to other registries. Building registries on a block chain influences key properties related to the Blockchains. Here the data integrity, immutability as well as the availability is considerable.

In 2017, Harry Halpin, et.al.[12] wrote on security and privacy of Blockchain. The Blockchain is one of the most enthusiastic bursts related to activity. It is necessary that the issues related to the security and privacy must be resolved. Therefore they discussed on block chain.

In 2018,Mahdi H. Miraz, et al.[13]discussed the Apps related to the Blockchain and Cryptocurrency. When a new transaction is add to chain, all participants provide the validation to this transaction. It is made to apply an algorithm to verify the transaction. The accurately meaning of "valid" is defined using the Blockchain system which varies among the systems.

In 2018, Mohamed Amine Ferrag, et.al.[14]presented a comprehensive survey onprotocols of the Blockchain. In addition, the researchers also stated the review on application domains related to the Blockchain technologies.

In 2018, Carmen Holotesc, et.al.[15]described Blockchain technology to understand it properly. They made the exploration of Blockchain technology as well as its platforms. They also discussed the existing global as well as the governmental initiatives. The researches have considered the potential apps of Blockchain in multiple domains, along with concentrated on education.

In 2018, Dylan Yaga ,et.al.[16]stated Blockchain technology with its overview. The research work has enabled a community to make record of the transactions.

This transaction is made in a distributed ledger in a community. This work also offered a high-level technical review on Blockchain. In addition, they also explored the pattern by which this technology executes.

In 2018, Jonathan Chiu, et.al.[17]described the economics related to the crypto currencies, bitcoin.It is very important thing that it is secure. One can extend in the database but not can make changes in previous records. In order to make alteration in the previous records, one is required to pay a huge amount of money.

In 2017, HU Wei-hong, et. al.[18]mentioned several Blockchain related alternatives to DNS for example Namecoin as well as Blockstack. These solutions are able to provide the DNS solution with the use of public blockchain. When a new transaction is add to chain, all participants provide the validation to this transaction. It is performed to apply an algorithm to transaction for the verification of the transaction. The exactly meaning of "valid" was defined using the Blockchain system. It can vary among the systems.

In 2018, Enis Karaarslan, et. al. [19] stated Blockchain-depnedent DNS solutions. These were classified in detailas per their services. They discussed the advantages as well as the feasibility related to such implementations. The feasibility of decentralized Internet has been questioned in their research work.

In 2019,Jamila Alsayed Kassem et. Al. [20] mentioned about DNS-IdM. It is a smart contract-dependentsystem of identity management. They explained that the technology of Blockchain is not centralized. Therefore, no single authority is there who provide the approval for the transactions. No any single can set specific rules related to acceptance of transactions. Mean to say that it is a secure system because all the participants are required to accept transactions.

III. PROPOSED METHODOLOGY

A. Block Diagram

Dns security by integrating crypted port mechanism

In proposed work, the proposed model is performed to enhance the security of proposed work. Port number is communicated after handshaking of DNS client to Blockchain based DNS Servers. As during data transmission, the port no and IP address is required to transfer data. The default port number is 80 in of http protocol. The proposed work allows client to send the encrypted userdefined port number in order to perform secure data transmission. In first face, the DNS server gets the data from client via default port. This data is encrypted user defined port number. The copy of used defined port number is available on both DNS client and DNS server side. The server decrypts the received data and gets the used defined port number. Then, in second face, the DNS server uses the user defined port to initial the actual transmission. After getting acknowledgement from DNS server the client performs transmission using user defined port in third face.

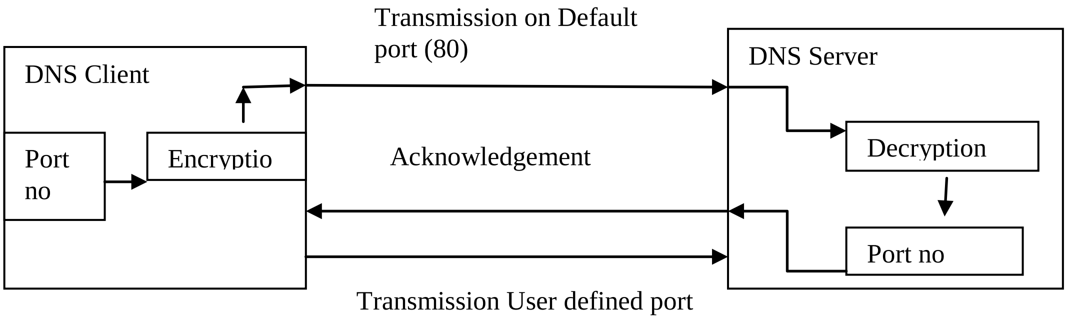

Fig. 2.Block diagram of DNS Security by Integrating Crypted Port Mechanism

Port number is separately encrypted to avoid man in middle attack using multiplicative inverse technique. The multiplicative inverse mechanism allows security to defined port number.

Resolving dns cache poisining attack issue

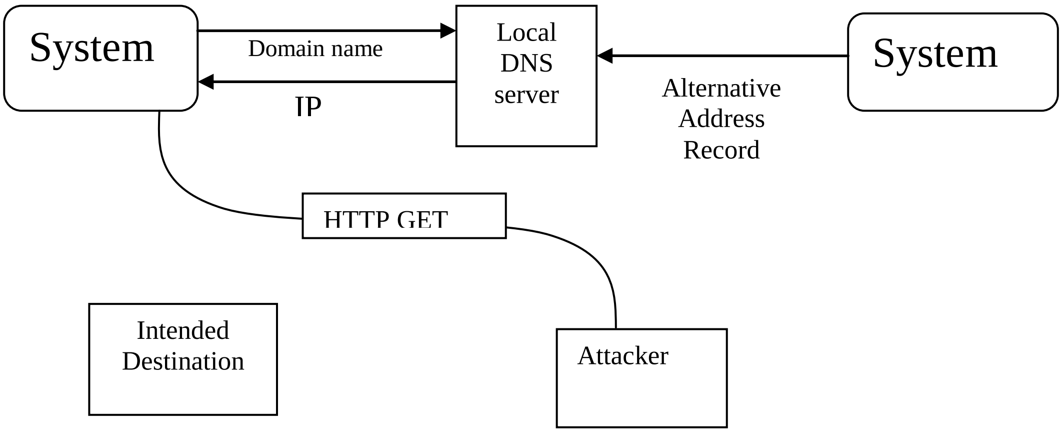

Fig. 3.Block Traditional DNS Attack

There is threat of DNS cache poisoning attack on blockchain. Figure 3 given example is illustrating a DNS cache poisoning attack. In this figure, a malicious person (IP 192.168.3.300) cuts off the communication channel among client whose IP address is 192.168.1.100 and a server computer.

This server computer belongs to the website www.estores.com. The IP address of this server computer is 192.168.2.200.

As it is observed that in tradition system, the DNS attack works due to weakness of internet protocol. The data is accessible to attacker as he could intrude from different system.

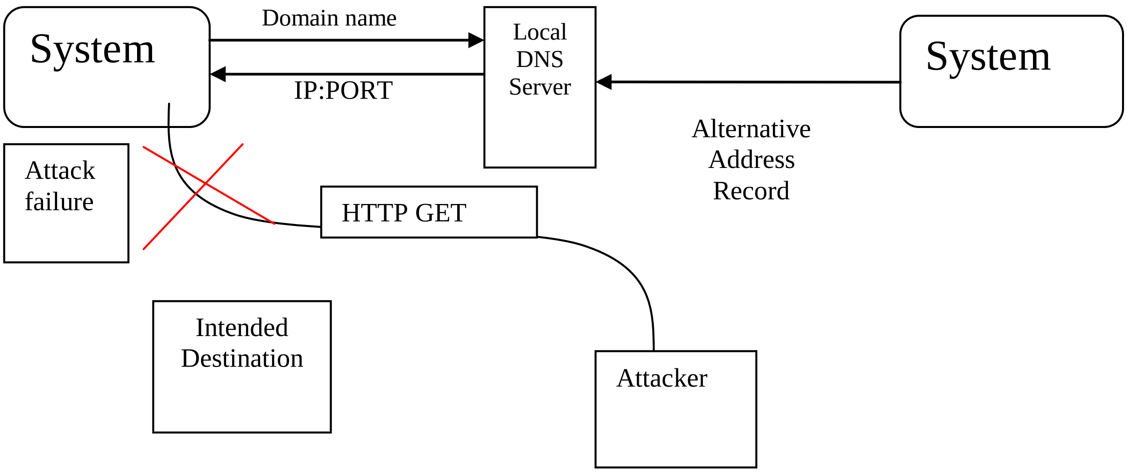

Fig. 4.Block diagram of Security from DNS Cache Poisoning Attack

In order to restrict DNS cache the concept of user defined port are used. There are 0 to 1023 port that are already reserved for existing protocols and services. There is need to use port above this series. If user defined port such as 4500 is used, then the addressing would be made using 192.168.1.100:4500 address instead of only IP address. The use of port with integration of IP address is able to secure the communication channel. The attackers need to know the IP address with port number in order to perform attack.

B. Algorithm

Client Side
The IP address would be set on client side during sending operation and encoding would be made on client side.
Server Side
Operation would be made on server side to verify the IP address and decode file and integrity check in order to accept reject transaction.
The algorithm for multiplicative inverse is explained below:
Algorithm to encrypt port number using multiplicative inverse

```
Step1Getinputaaaasstringforencryptionandshasshifting number
Step2Takeintegershifti,nandStringstr,str1="",str2=""
Step3Setstr=aaa;
Step4Convertstrto lowercase
Step5Getlenghtofstrinn
Step6Getarrayofcharacterfromstrtoch1array
Step7Takech3,ch4ascharacter
Step8setshift=sh;
Step9seti=0andincreaseiby1andrepeatstep10untiliisless thenn
Step10ifch1[i]isLetter
    setch3=(char)(((int)ch1[i]*shift–97)%26+97)
    setstr1=str1+ch3
    otherwise
    if(ch1[i]=='')
    setstr1=str1+ch1[i]
Step11Calculationofmultiplicativeinverse
Step12Setq=0,flag=0
Step13seti=0andibyiandrepeatstep14untilI islessthan26
Step14if(((i*26)+1)%shift==0)
    setq=((i*26)+1)/shiftandstoptheloop
Step15setarrayofcharacterfromstr1toch2
Step16seti=0andincrementiby1andrepeatstep17untiliisless thanlengthofstr1
Step17ifch2[i].isletter
    ch4=(char)(((int)ch2[i]*q-97)%26+97);
    setstr2=str2+ch4
    otherwise
    if(ch2[i]=='')
    str2=str2+ch2[i];
Step18getstr2asoutput
```

Algorithm on sender side

1. Initialize port number to transmit the data.
2. Encrypt the port number using multiplicative inverse
3. Transfer the encrypted content via predefined port number
4. Wait for the acknowledgement from receiver after decryption of port number
5. After getting acknowledgement perform transmission by user defined port.

Algorithm on receiver side

1. Receive data from sender side
2. Apply multiplicative inverse to decrypt port number
3. Get the port number
4. Initialize the transmission by used defined port number.
5. Get data from sender on user defined port number.

IV. RESULT AND DISCUSSION

A. Flowchart

Traditional Flowchart

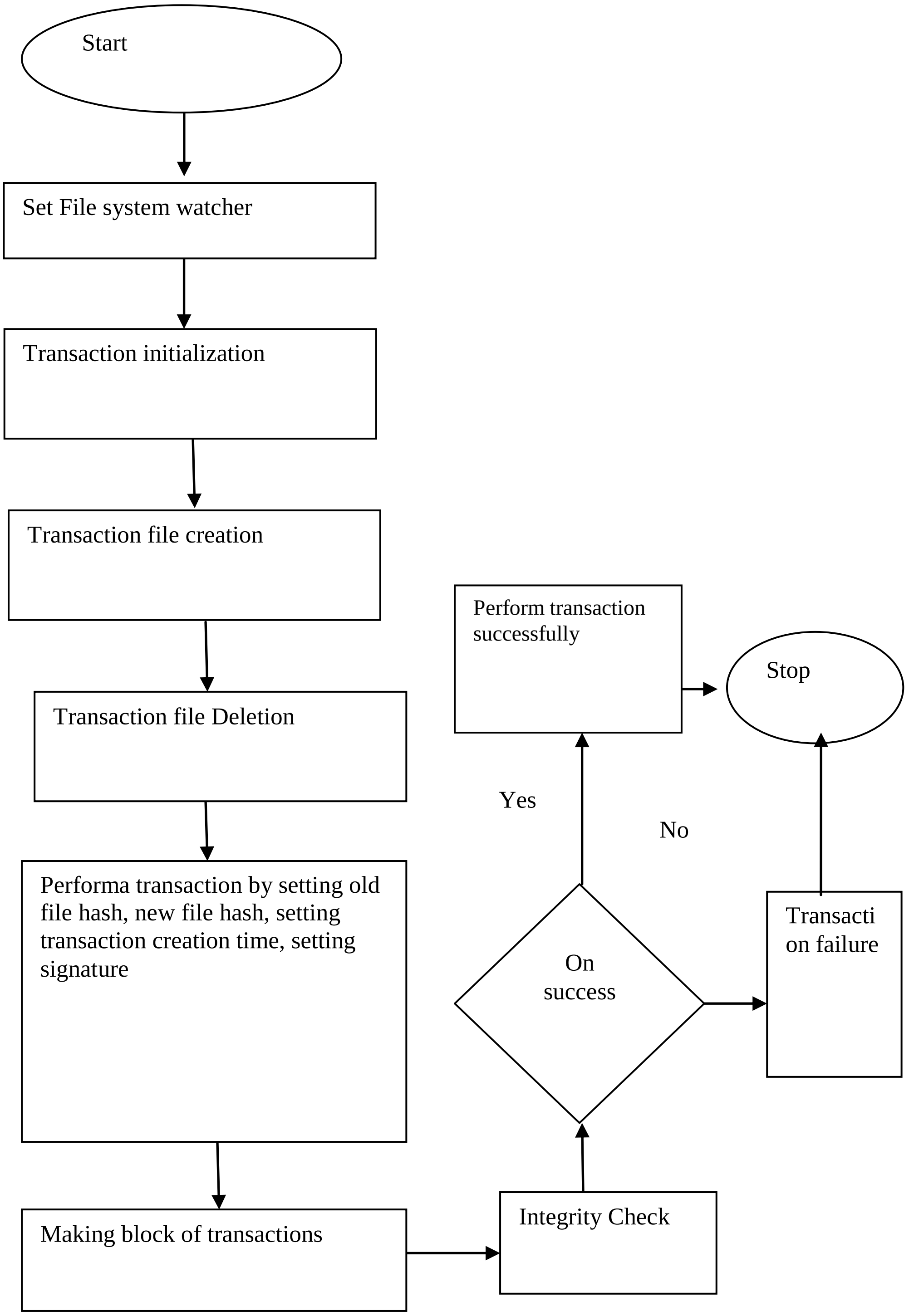
Start
Set File system watcher
Transaction initialization
Transaction file creation
Transaction file Deletion
Performa transaction by setting old file hash, new file hash, setting transaction creation time, setting signature
Making block of transactions
Integrity Check
On success
Yes
No
Perform transaction successfully
Transacti on failure
Stop

Fig. 5.Traditional flow chart

The Proposed working process is plotted below:

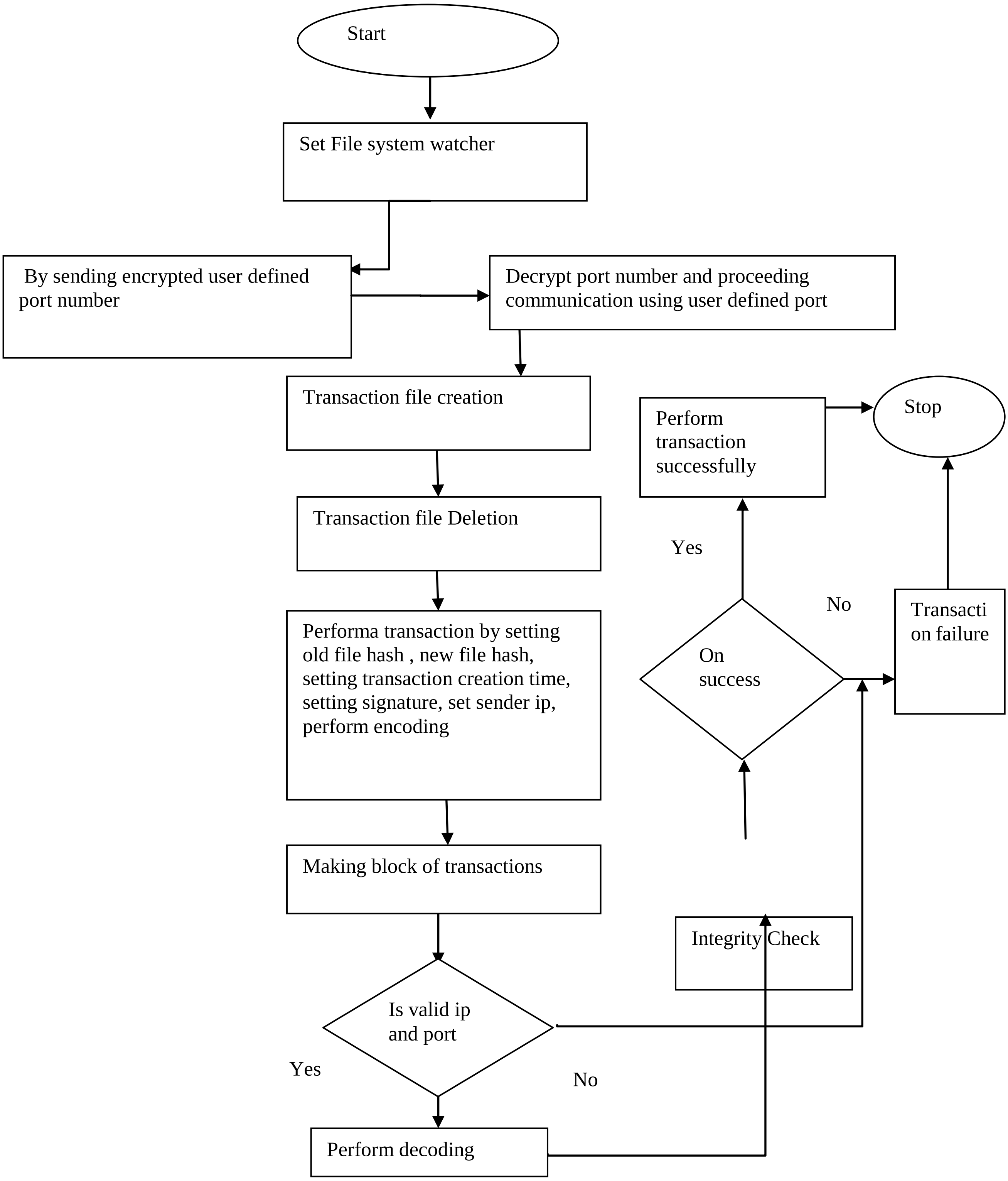
Start
Set File system watcher
By sending encrypted user defined port number
Decrypt port number and proceeding communication using user defined port
Transaction file creation
Transaction file Deletion
Performa transaction by setting old file hash , new file hash, setting transaction creation time, setting signature, set sender ip, perform encoding
Making block of transactions
Is valid ip and port
Yes
No
Perform decoding
Integrity Check
On success
Yes
No
Perform transaction successfully
Transacti on failure
Stop

Fig. 6.Proposed Flow Chart for Block Chain with IP and port validation

B. Result Analysis

In traditional research the low guess ration, medium guess ratio, high guess ratio has been considered along with probability of dns attack. As the times of requested url increases the probability of attack also increases as shown in following chart. Results of varying times_to_request_url with max_port_id.

Table- I: Comparative analysis of probability of attack considering low guess, medium guess and high guess ratio

Times_to_request_url	Low Guess Ratio (Traditional)	Low Guess Ratio (Proposed)	Medium Guess Ratio (Traditional)	Medium Guess Ratio (Proposed)	High Guess Ratio (Traditional)	High Guess Ratio (Proposed)
1	0.01	0.004	0.01	0.004	0.05	0.02
2	0.03	0.012	0.055	0.022	0.1	0.04
4	0.06	0.024	0.1	0.04	0.2	0.08
6	0.085	0.034	0.15	0.06	0.28	0.112
8	0.1	0.04	0.185	0.074	0.36	0.144
10	0.115	0.046	0.22	0.088	0.42	0.168
12	0.135	0.054	0.26	0.104	0.48	0.192
14	0.165	0.066	0.3	0.12	0.54	0.216
16	0.195	0.078	0.32	0.128	0.59	0.236
18	0.205	0.082	0.37	0.148	0.63	0.252
20	0.22	0.088	0.4	0.16	0.675	0.27
22	0.24	0.096	0.42	0.168	0.7	0.28
24	0.26	0.104	0.45	0.18	0.73	0.292
26	0.285	0.114	0.49	0.196	0.76	0.304
28	0.3	0.12	0.51	0.204	0.78	0.312
30	0.31	0.124	0.53	0.212	0.8	0.32

In proposed work the encrypted port number has been used in order to check the attack. As during initiating face the standard port is used and during actual transmission encrypted port has been used. Following figure is representing the comparative analysis of probability of attack considering low guess ratio, medium guess ratio, high guess ratio according to times to request url.

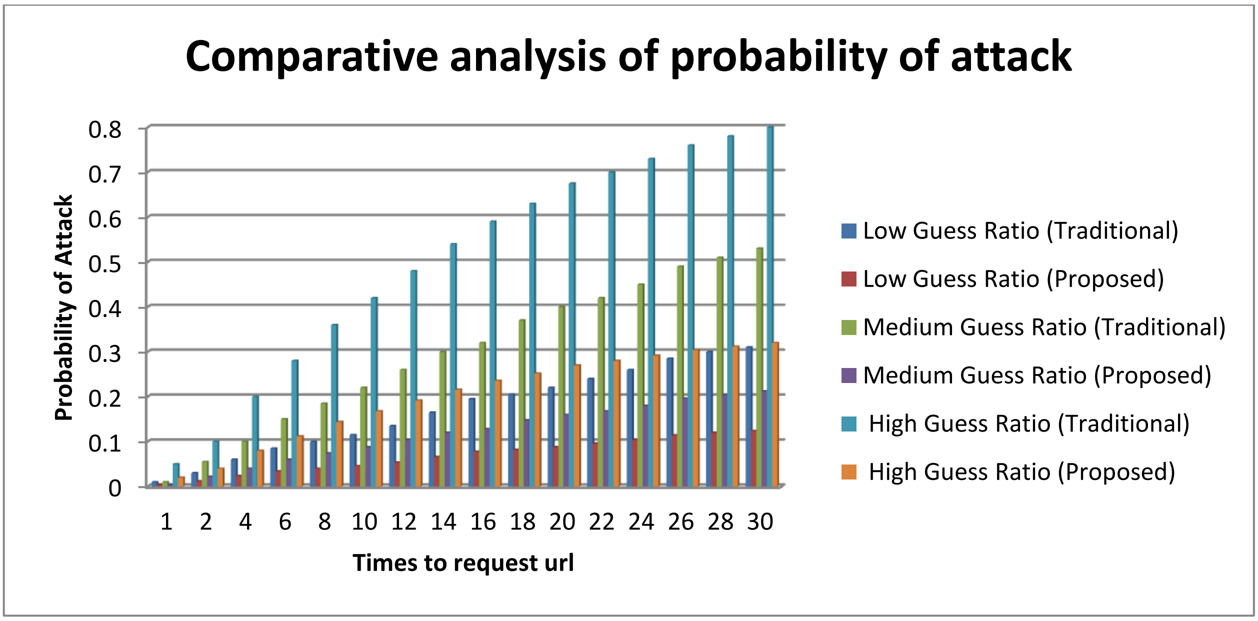

Fig. 7.Comparative analysis of probability of attack considering low, medium , high guess ratio

Following table is showing probability of attack considering other legitimate requests rate. Here the considered time to request url is 2 and 6. The table is representing the proposed work has reduced the probability of attack.

Table- II: Attack probability considering legitimate request rate considering time to request url 2 and 6

Other legitimate requests rate	Time to request url-2 (Traditional)	Time to request url-2 (Proposed)	Time to request url-6(Traditional)	Time to request url-6 (Proposed)
10	0.02	0.0067	0.01	0.0033
20	0.075	0.0250	0.025	0.0083
40	0.13	0.0433	0.05	0.0167
60	0.19	0.0633	0.075	0.0250
80	0.24	0.0800	0.095	0.0317
100	0.3	0.1000	0.11	0.0367
120	0.33	0.1100	0.125	0.0417
140	0.385	0.1283	0.15	0.0500
160	0.42	0.1400	0.175	0.0583
180	0.46	0.1533	0.19	0.0633
200	0.49	0.1633	0.2	0.0667
220	0.515	0.1717	0.21	0.0700
240	0.54	0.1800	0.235	0.0783
260	0.575	0.1917	0.245	0.0817
280	0.6	0.2000	0.26	0.0867
300	0.62	0.2067	0.28	0.0933

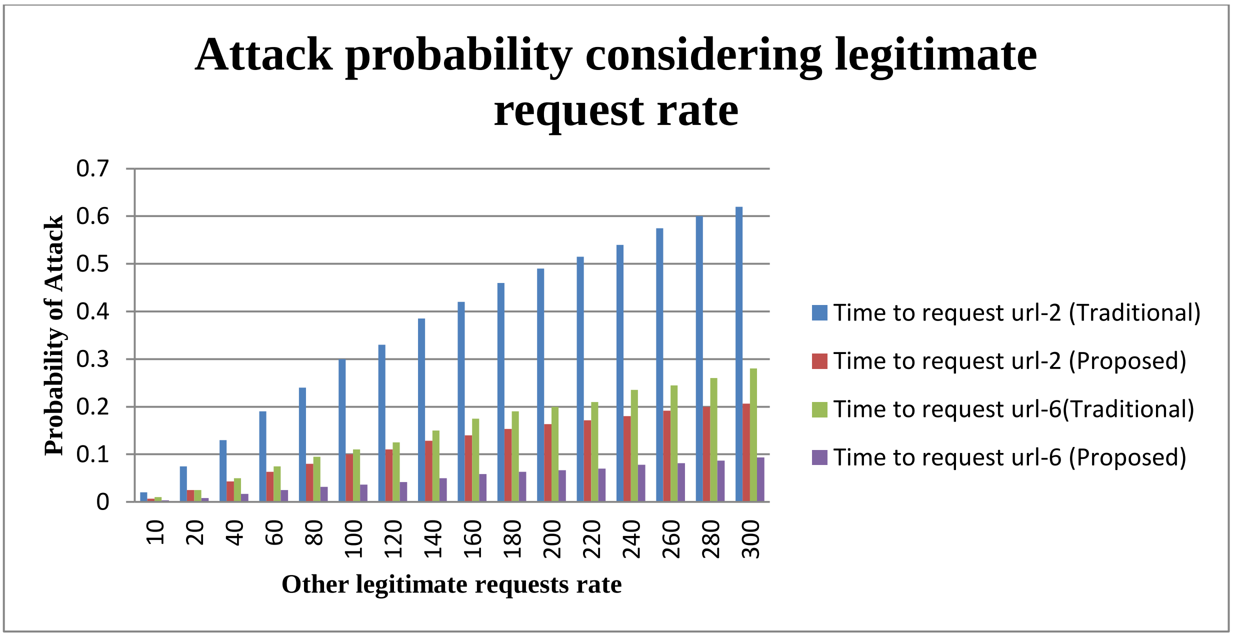

Fig. 8.Attack probability considering legitimate request rate considering time to request url-2,6

Following table is representing the results for different time to request url values according to varying max port id. The probability of attack is less in case of proposed security mechanism.

Table- III: Comparison chart considering time to request url 2,6

Guess	Time to request url-2 (Traditional)	Time to request url-2 (Proposed)	Time to request url-6 (Traditional)	Time to request url-6 (Proposed)
10	0.05	0.0125	0.1	0.025
20	0.085	0.02125	0.195	0.04875
40	0.12	0.03	0.33	0.0825
60	0.195	0.04875	0.47	0.1175
80	0.23	0.0575	0.55	0.1375
100	0.29	0.0725	0.62	0.155
120	0.32	0.08	0.68	0.17
140	0.36	0.09	0.73	0.1825
160	0.39	0.0975	0.77	0.1925
180	0.415	0.10375	0.8	0.2
200	0.43	0.1075	0.82	0.205
220	0.46	0.115	0.85	0.2125
240	0.49	0.1225	0.87	0.2175
260	0.5	0.125	0.88	0.22
280	0.52	0.13	0.89	0.2225
300	0.55	0.1375	0.9	0.225

Following chart is showing the curve for different time to request url values that is 2 and 6 according to varying max port id. The probability of attack is less in case of proposed security mechanism.

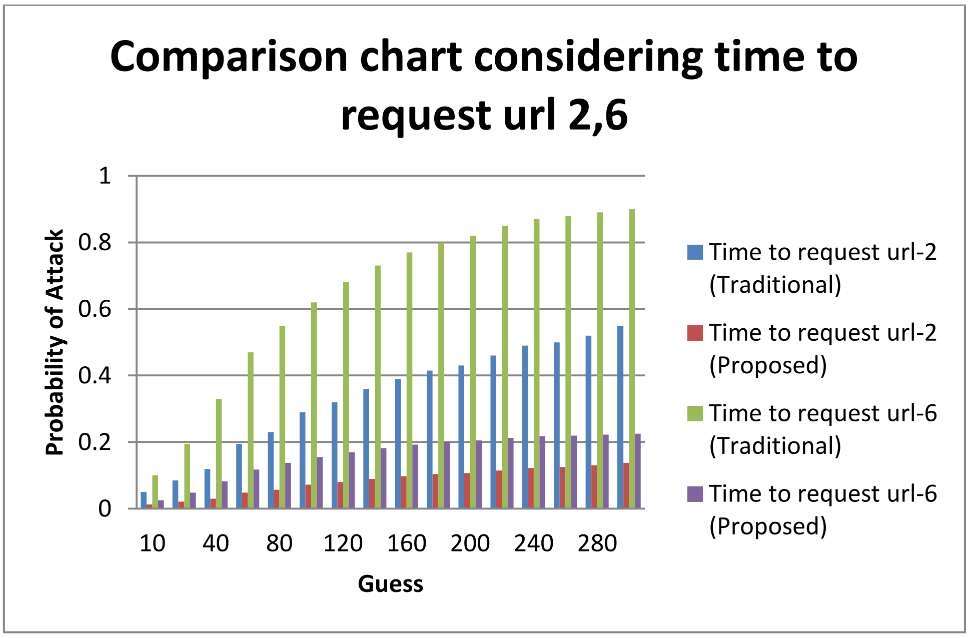

Fig. 9.Comparison chart considering time to request url 2,6

Following table is representing the probability attack considering guess 50,100,150,200. The expected probability of attack has been reduced in proposed work as the guess is considered.

Table- IV: Comparative analysis considering guess 50,100,150,200

Max_port_id	Guess=50 (Traditional)	Guess=50 (Proposed)	Guess=100 (Traditional)	Guess=100 (Proposed)	Guess=150 (Traditional)	Guess=150 (Proposed)	Guess=200 (Traditional)	Guess=200 (Proposed)
10	0.05	0.0125	0.1	0.025	0.15	0.0375	0.22	0.055
25	0.04	0.01	0.04	0.01	0.07	0.0175	0.105	0.02625
50	0.035	0.00875	0.03	0.0075	0.04	0.01	0.055	0.01375
75	0.03	0.0075	0.025	0.00625	0.03	0.0075	0.04	0.01
100	0.02	0.005	0.02	0.005	0.02	0.005	0.03	0.0075
125	0.01	0.0025	0.01	0.0025	0.01	0.0025	0.015	0.00375
150	0.0095	0.002375	0.0095	0.002375	0.0095	0.002375	0.01	0.0025
175	0.0085	0.002125	0.0085	0.002125	0.0085	0.002125	0.009	0.00225
200	0.0075	0.001875	0.0075	0.001875	0.0075	0.001875	0.008	0.002
225	0.0065	0.001625	0.0065	0.001625	0.0065	0.001625	0.007	0.00175
250	0.0055	0.001375	0.0055	0.001375	0.0055	0.001375	0.006	0.0015
275	0.0045	0.001125	0.0045	0.001125	0.0045	0.001125	0.005	0.00125
300	0.0035	0.000875	0.0035	0.000875	0.0035	0.000875	0.004	0.001
325	0.0025	0.000625	0.0025	0.000625	0.0025	0.000625	0.003	0.00075
350	0.0019	0.000475	0.0019	0.000475	0.0019	0.000475	0.002	0.0005
375	0.001	0.00025	0.001	0.00025	0.001	0.00025	0.001	0.00025
400	0.001	0.00025	0.001	0.00025	0.001	0.00025	0.001	0.00025

Following chart is representing the probability of attack in case of existing and proposed security mechanism.

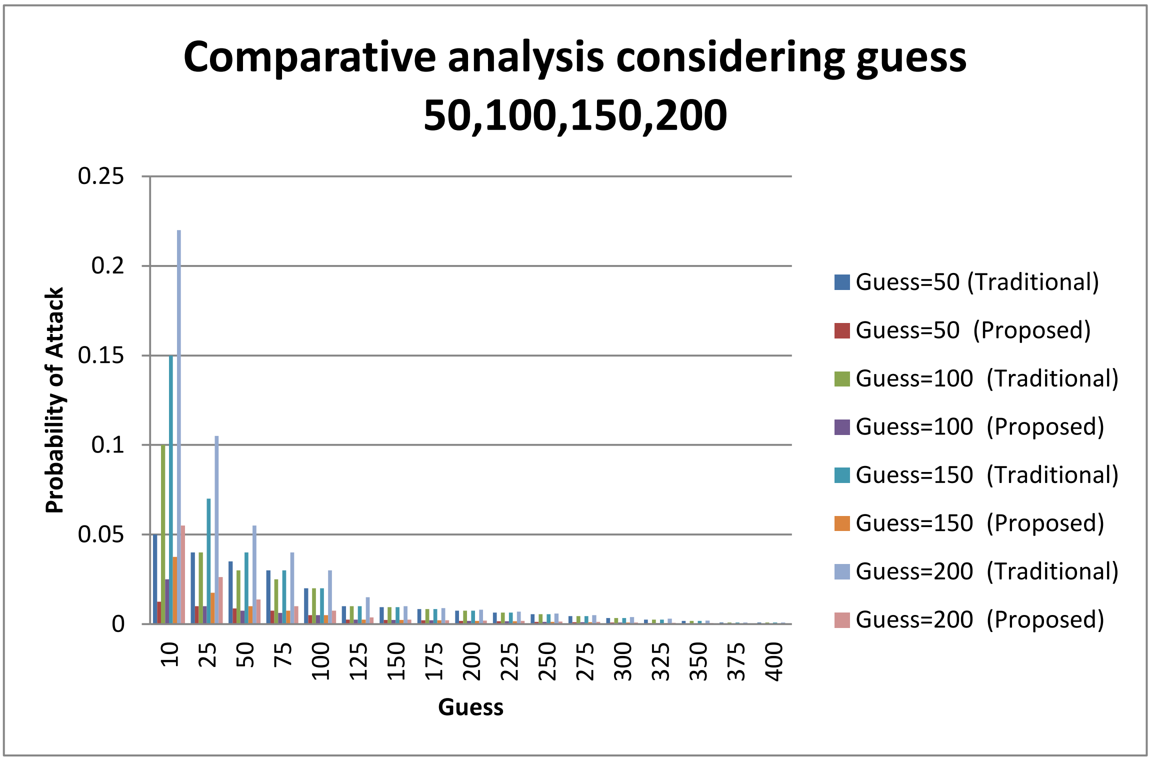

Fig. 10. Comparative analysis considering guess 50,100,150,200

V. CONCLUSION

As it is observed that in tradition system, the DNS attack works due to weakness of internet protocol.

From the above simulations it is clear that the proposed work has reduced the probability of attack as compare to traditional work. Proposed work has been found 3 to 4 more secure as compare to traditional DNS security mechanism.

The data can be accessed by attacker as he can intrude from different system. In order to restrict DNS cache the concept of user defined port are used. The use of port with integration of IP address is able to secure the communication channel. The attackers need to know the IP address with port number in order to perform attack. The proposed mechanism of encrypted port number to perform the communication is able to increase the security at transmission level. This mechanism is efficient to increase the security to Blockchain based transaction. Research has considered cache poisoning attacks in Blockchain that is known as a type of attack in which corrupt data is inserted in cache database of DNS name server. The proposed work is efficient to reduce the probability of corruption of data from such attack. The proposed IP and port number based model is able to make Blockchain immune from cache poisoning attack. The block generation mechanism is modified by introducing user defined port number. The use of user defined port number would restrict the DNS attackers successfully.

ACKNOWLEDGMENT

Author thanks faculties and Guides of Amrita University for providing technical and moral support in completing this paper.

REFERENCES

1. Gareth W. Petersz ,Efstathios Panayiy (2015)" Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing & Smart Contracts on Internet of Money"
2. Jesse Yli-Huumo1, Deokyoon Ko (2016) "Where Is Current Research on Blockchain Technology?—A Systematic Review",
3. Igor Zikratov, Alexander Kuzmin, Vladislav Akimenko, Viktor Niculichev, LucaYalansky (2017)"Ensuring Data Integrity Using Block chain Technology" Proceeding Of 20th Conference Of Fruct Association
4. Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi (2017)"Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments"
5. Jun Hak Park, Jun Young Park, Eui Nam Huh(2017) "Block Chain Based data logging and integrity Management Systemfor Cloud Forensics"
6. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang , "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" 2017 IEEE
7. Shanti Bruyn , "Blockchain an introduction" VU,August 26, 2017
8. Jin Ho Park & Jong Hyuk Park (2017) "Blockchain Security in Cloud Computing: Use Cases, Challenges, & Solutions", Symmetry 2017
9. Ivan Martinovic (2017) "Blockchains for Governmental Services: Design Principles, Applications, & Case Studies", Centre for Technology & Global Affairs | University of Oxford
10. Sönke Bartling (2017) "Blockcha in for science & knowledge creation",
11. An Binh Tran, Xiwei Xu Ingo Weber, (2017) "Regerator: a Registry Generator for Blockchain",
12. Harry Halpin, Marta Piekarska (2017) "Introduction to Security & Privacy on Blockchain",
13. Mahdi H. Miraz, Maaruf Ali , "Applications of Blockchain Technology beyond Cryptocurrency" Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018.
14. Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, Helge Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges" 2018.
15. Carmen Holotesc, "UNDERSTANDING Blockchain TECHNOLOGY AND HOW TO GET INVOLVED" Researchgate, 2018.
16. Dylan Yaga ,"Blockchain Technology Overview" National Institute of Standards and Technology Internal Report 8202, 2018.
17. Jonathan Chiu (2018) "The Economics of Cryptocurrencies Bitcoin & Beyond,
18. Aleksander Berentsen & Fabian Schär (2018) "A Short Introduction to World of Cryptocurrencies.
19. David Pointcheval, Olivier Blazy, New Smooth Projective Hash Functions & One-Round Authenticated Key Exchange(18_22 august 2013, Santa Barbara, California, USA), Springer- Verlag, LNCS 8042, pages 449_475.
20. David Pointcheval, Olivier Blazy, Effcient UC-Secure Authenticated Key-Exchange for Algebraic Languages(26 February - 1 March 2013, Nara, Japan)), 16th International Conference on Practice & Theory in Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013.
21. David Pointcheval, Password-based Authenticated Key Exchange. (21-23 may 2012, Darmstadt, Germany)Springer-Verlag, LNCS 7293, pages 390-397.
22. David Pointcheval, Michel Abdalla, Contributory Password-Authenticated Group Key Exchange with Join Capability, (February 14-18, 2011, San Francisco, CA, USA), A. Kiayias Ed. Springer-Verlag, LNCS 6558, pages 142-160
23. David Pointcheval, Xavier Boyen, Strong Cryptography from Weak Secrets, (3 – 6 may 2010, Stellenbosch, South Africa), D. Bernstein & T. Lange Eds., Springer-Verlag, LNCS 6055, pages 297–315.
24. David Pointcheval, Michel Abdalla, Flexible Group Key Exchange with On-Demand Computation of Subgroup Keys, (3-6 May 2010, Stellenbosch, South Africa)), D. Bernstein & T. Lange Eds., Springer-Verlag, LNCS 6055, pages 351-368.
25. David Pointcheval, Michel Abdalla, Distributed Public-Key Cryptography from Weak Secrets, (18_20 march 2009, Irvine, CA, USA), S. Jarecki & G. Tsudik Eds. Springer-Verlag, LNCS 5443, pages 139_159.
26. David Pointcheval, Michel Abdalla, Password-Authenticated Group Key Agreement with Adaptive Security & Contributiveness, (21 – 25 june 2009, Gammarth, Tunisia) B. Preneel Ed., Springer-Verlag, LNCS 5580, pages 254–271.
27. Rafael Álvarez, Leandro Tortosa, Analysis & design of a secure key exchange scheme, Information Sciences 179 (2009) , Elsevier
28. David Pointcheval, Michel Abdalla, Anonymous & Transparent Gateway-based Password- Authenticated Key Exchange , December 2–4, 2008, Hong-Kong, China – M. Franklin, L. Hui & D. Wong Eds. Springer-Verlag, LNCS 5339, pages 133–148.
29. Nikolaos Alexiou, Stylianos BasagiannisPanagiotis Katsaros, Tushar DeshpandeScott A. Smolka, Formal Analysis of the Kaminsky DNSCache-Poisoning Attack UsingProbabilistic Model Checking, 2010 IEEE 12th International Symposium on High Assurance Systems Engineering.

AUTHORS PROFILE

Mukesh Kumar Bansal, is experienced IT / Telecom / Cyber Security professional / Social Worker and executive with broad and well-balanced technical, commercial, business and people management skills. 24+ years of experience exclusively in providing image processing (ISRO from 1997-2001).

M. Sethumadhavan, received his PhD (Number Theory) from Calicut Regional Engineering College. Currently, he is working as a Professor and Head of Centre for Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore.

.