Article

Integrating Blockchain with Deep Packet Inspection and The Performance Overhead Introduced

Adamu Abubakar * and Fazeel Ahmed Khan

Posted Date: 21 August 2024

doi: 10.20944/preprints202408.1475.v1

Keywords: Blockchain; Packet Header; Payload; Deep Packet Inspection; Traffic Flow

Article

Integrating Blockchain with Deep Packet Inspection and The Performance Overhead Introduced

Adamu Abubakar * and Fazeel Ahmed Khan

Department of Computer Science, International Islamic University Malaysia, 53100 Kuala Lumpur Malaysia; fazeelahmedkhan15@gmail.com
* Correspondence: adamu@iium.edu.my

Abstract: As computer networks develop in size and complexity, the need for equipment that can characterize, inspect, monitor, and summarize the features of a transmission in real time grows. Many transmission and packet inspection theories are required to examine network traffic. Unfortunately, loss the track or traceability of one traffic scenarios against others over real-time network. Deep packet inspection (DPI) approaches can be used to alleviate the problem but still face flexibility constraints in the sense that it will be difficult to keep track of prior occurrences. There have been significant theoretical improvements in packet inspection, but the problem of event tracking flexibility remains unsolved. A novel approach for “integrating blockchain with DPI” in summarizing computer network traffic flow events has emerged as a result of this research: This technique captured traffic flows in the network, DPI report, and the entire transmission session header and load them into a smart-contract based- Blockchain. Two experimental scenarios are used to test the validity of the system. The first scenarios involve analysis of DPI transmission without integrating blockchain, follow by the captured of transmission session involving DPI with blockchain. The finding indicates that DPI transmission with blockchain is more secured against "Tampering Incidents", "Unauthorized Access Attempts", “Auditability” and many other security concern. Whereas, the performance overhead introduced by blockchain-based DPI indicate an increase in "DPI Processing Time from 68ms to 150ms, a "CPU Usage increment by 20%, Network Latency increment of 15ms from 20ms to 35ms, and almost all other computational resources increase. Therefore, the finding can be summarized that the performance overhead introduced by integrating blockchain with DPI increases, but it provides a secure DPI reports for decision making.

Keywords: blockchain; packet header; payload; deep packet inspection; traffic flow

1. Introduction

DPI is a network security technique that analyses the header and content of an IP packet as it traverses a network. In modern network management, packet headers and contents are thoroughly examined to monitor transmission inside a network, identify and mitigate malicious activity, enforce security regulations, and get insight into network activities {1]. Blockchain provides immutability, transparency, and security in a decentralised manner for many applications. However, its increasing popularity and widespread use have led to a significant increase in the number of transactions, resulting in a growing need for storage [2]. The blockchain ensures that the quality evaluation is unbiased and prompt. Without the blockchain, systems that rely on decision-making would lack the ability to maintain data integrity and impartiality [3]. DPI gains a new level of intelligence with the addition of Blockchain, that is integrating DPI and blockchain can determine the genuine nature of communications depending on that information, such as brain mapping [4], identity management [5] and so many areas. In terms of IP network transmission network, the blockchain platform will store the timestamp records for each packet that has a history of being in a transmission session. Furthermore, for each packet that has a history of being in a transmission session, it's status and changes within its header can be traced and organize in order to verify that all packets have been adequately reviewed [6].

Despite the fact that this approach has the capacity to monitor every aspect of traffic flow using a blockchain, computational overhead becomes the first major issues associated to the approach [7]. Blockchain technology and distributed ledgers are attracting massive attention and trigger multiple projects in different industries. However, their application to any field require careful consideration of all the computational component required [8]. This is not only due to the fact that the most well-known application that use blockchain technology are mainly concern of addressing security issue. However, massive computational cost and industry industrial application is necessary [9]. The good side of application of blockchain lies with addressing traceability problem. For instance, retracing ownership over a longer chain of changing buyers in global financial transaction services: when, for example, the US investment bank Bear Stearns failed in 2008 and was completely acquired by JP Morgan Chase, the number of shares offered to the acquirer was larger than the shares out- standing in the books of Bear Stearns. It was not possible to clarify the accounting errors and JP Morgan Chase had to bear the damage from excess (digital) shares [10,11].

Another analogy where traceability is crucial, is on dealing with highly previous natural resources like the Diamond. It is just as critical to be able to trace back ownership in long transaction chains for physical goods like diamonds as it is in financial markets. The intermediaries that come before them thoroughly vet each link in the chain of intermediation [12]. This isn't a good option because of the potential for credit damage and the time and money it would take. As the blockchain technology promises to solve these critical issues, a shift from trusting people to trusting math, is what the blockchain represents. Human intervention is no longer required [13,14]. Adding a new block to the blockchain creates a complete ledger of transactions. Cryptographic methods can be used by the network to verify blocks. The nonce, a random number used for hash verification, is also included in the transaction data in the blockchain protocol [15]. This concept protects the 'genesis block,' the first block of the blockchain. When a new block is added or removed from a chain, the hash value of that block changes. This means that hash values can be used to prevent fraud. If the majority of nodes in the network agree that the transactions in the block are valid and the block itself is valid, it can be added to the chain [16]. An agreement is reached by a majority of network validators (or in some cases, all of them) on a ledger's current state. As long as certain rules and procedures are followed, multiple nodes can share the same set of facts. When a new transaction is made, the ledger does not automatically update. Changing the data in the blockchain is impossible after this point. Bitcoin rewards its "miners" for validating blocks by issuing them with Bitcoins. The Bitcoin example demonstrates that the blockchain's principle isn't limited to transforming the way money is traded [17]. Cryptography has made it possible for people from all over the world to trust each other and transfer a wide range of assets over the internet.

Based on the justification and rationale of that makes blockchain crucial in traceability, DPI is also argued by this study to established some sort of traceability mechanism, using a distributed ledger system like the one described above. The network as a whole function even if a single node fails, whereas centralized systems would be rendered inoperable. Trust in the system increases because people don't have to evaluate the trustworthiness of the intermediary or other network parameters because of this. It is not necessary to build trust in individual components of the system. By cutting out the some component. IP computer network system, can improve the security of our data when appropriately managed. Third-party data collection increases the risk of security breaches. It is possible to reduce transaction security by removing third parties from the blockchain [18].

Motivated by the previous work on concepts for tackling privacy concerns with smart contracts [19], this current study contributes in the following ways:

- In contrast to the number of commercial white papers on blockchains, academic study associated to the DPI and Blockchain, in which most tends to concentrate on crypto-currencies, some on Bitcoin's weaknesses [20]. This study design and developed an integrated DPI and smart-contract-based blockchain, intended to have full traceability on all DPI report for decision marking.
- With due consideration that another method of ensuring that user privacy is respected is through the use of a "fair exchange protocol." While some research studies explored the privacy concerns associated with Bitcoin [21]. In the realm of this current study, high priority network

transmission session captured by DPI is constantly and consistently updated in the transmission session it belongs, whereas new priority packet generates new blocks which is also traceable.

- Considering that the usage of Blockchain present issues of computational performance [22] in order to accelerate transaction processing, and resolve the issue of poor performance in the future, this current research contribute in conducting two experiments involving analysis of DPI transmission without integrating blockchain, and with DPI –based blockchain. The finding shows that DPI transmission with blockchain is more secured, but face some drawbacks on the computational performance overhead introduced.

The remaining part of the paper is organized as follows: apart from this current section that provide the overview of the research, section two present the previous research studies on deep packet inspections and well as blockchain. Section three discusses the research methodology, while section four present the experimental analysis and the result of the study. Section five provide the details discussion of the finding as well as the implication of the study and finally, section 6 present the conclusion for the study.

2. Related Work

There are a number of concepts that have been discussed in literature that can now be supported thanks to blockchain technology. Contracts that combine computer protocols with human interfaces to carry out the conditions of the agreement between the two parties have been dubbed "Smart Contracts" by Szabo [16]. Smart Contracts are becoming increasingly popular as a result of the blockchain's increased ease of use when compared to the technology available at the time of their development 20 years ago. In light of the blockchain, smart contracts are becoming more popular as a result of their ability to be used more easily than they might have been before their inception [23].

Zhang et al [24] suggest integrating Blockchain and Industrial Internet of Things (IIoT) to offer safe and collaborative services. Therefore, the research has developed a privacy-preserving traceable Deep Packet Inspection (DPI) system that conducts inspections on encrypted traffic in a blockchain-based Industrial Internet of Things (IIoT) environment. The paper does not effectively demonstrate the computational performance of integrating Blockchain with IIoT.

Similarly, Song et al. [25] conducted a test on the SolarWinds DPI tool to determine if it could detect and prevent network traffic anomalies. They compared its performance to their proposed method, which involves creating a set of informative features that represent the normal and anomalous behavior of the system. This is done by evaluating the Hurst (H) parameter of the network traffic. It was discovered that their proposed DPI solution enhances efficiency by accurately identifying and considering the level of information security. The same principle applies in cases where computation using DPI is not evaluated, even if blockchain was not utilised in their research.

Ren et al. [26] demonstrated that as traffic volume grows, businesses opt to delegate their middlebox services, such as deep packet inspection, to the cloud in order to access abundant computational and communication resources. The paper proposes an effective verifiable Deep Packet Inspection (DPI) scheme that provides robust privacy guarantees. Experimental results reveal that their technique not only maintains packet privacy, but also achieves great efficiency in packet inspection.

Zhang et al. [27] demonstrated that enterprise clients are increasingly using in-the-cloud deep DPI services to safeguard their networks in the context of the growing trend of network middleboxes as a service. The study suggests a verification approach that ensures privacy and is lightweight. This scheme efficiently examines if in-the-cloud DPI services are running successfully without revealing private DPI rulesets. The study's findings indicate that the proposed technique is feasible and only results in a real-time delay of 10–20 microseconds.

Li et al. [28] demonstrated that implementing a distributed packet filter is a highly effective approach to reduce unwanted traffic. Ensuring the integrity of transmitted data is challenging because a malicious internal node can share modified data to undermine the efficiency of filters. Therefore, the research suggested a design for a packet filter blacklist that utilises blockchain technology and incorporates collaborative intrusion detection. The blockchain technology is utilised to construct a resilient blacklist for mitigating undesirable traffic. The evaluation shows that the proposed technique's performance demonstrates that the filter can improve the resilience of blacklist generation.

Smart contract evolves within the frame of Blockchain, its implementation mostly arises when it comes to asset acquisition contracts based on pre-defined specifications, this new technique could eliminate the need for lawyers and banks [29]. One other way to govern real estate property ownership smart contracts can also be used. Considering that this technique considers both tangible and intangible assets, their application has no limit [30]. Previous research studies have established that the Ethereum decentralized system, developed by Vitalik Buterin, is a well-known illustration of blockchain technology's treatment of smart contracts [31–34]. Ethereum is able to support a wider range of applications than was previously conceivable [35–37]. Using blockchain technology, contracts may be automatically executed in a way that is both cost effective and transparent while still maintaining a high level of security [38].

Although there is a vast amount of literature available on DPI and blockchain, there is still a lack of well-structured explanations on how to build a system based on DPI and blockchain. These presentations should consider the speed overhead caused by merging blockchain with DPI, as well as the security improvements achieved by integrating blockchain with DPI. This study aims to design, developed and conduct an experiments in order to contribute to the field.

3. Methodology

This research design and developed a blockchan-based DPI, however the main research component lies with experimental monitoring and inspection of packets during a transmission session, with the blockchain serving as a separate traceability service. That means as a result of DPI service, any crucial case of identifying issue with packet, will be log in a block of the blockchan. The traceability of each packet that exits the transmission traffic flow is required for monitoring and inspecting each packet that exits the transmission traffic flow. The methodological framework is depicted in Figure 1.

At first, a network scenarios were created to examine the transmission session traffic flow by:

1. Initiating transmission sessions with certain payload to-and-fro
2. Initiating Deep packet inspection of the transmission session
3. Capture the traffic flow of the transmission session.

Concurrently another network scenario was created to examine the transmission session traffic flow by:

1. Initiating transmission sessions with certain payload to-and-fro
2. Initiating Deep packet inspection of the transmission session
3. Capture the traffic flow of the transmission session
4. Creating a block in blockchain for each packet capture, and appending policy based on the smart contract trait.
5. The smart contract is established for indicating a capture packet with normal header and or abnormal header

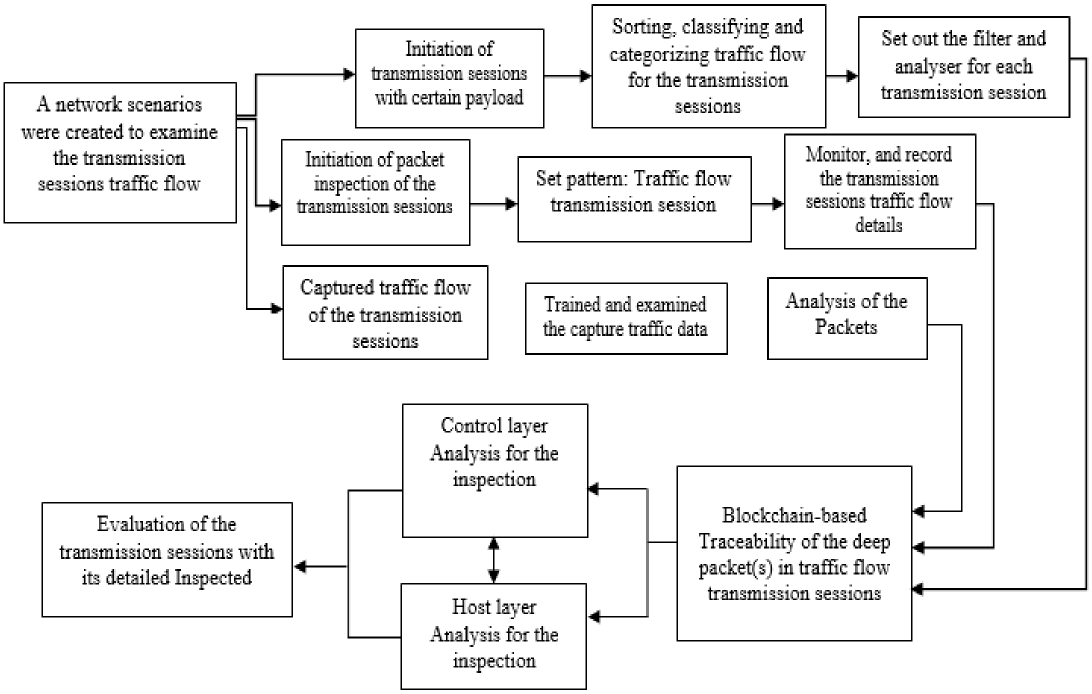

A network scenarios were created to examine the transmission sessions traffic flow
Initiation of transmission sessions with certain payload
Sorting, classifying and categorizing traffic flow for the transmission sessions
Set out the filter and analyser for each transmission session
Initiation of packet inspection of the transmission sessions
Set pattern: Traffic flow transmission session
Monitor, and record the transmission sessions traffic flow details
Captured traffic flow of the transmission sessions
Trained and examined the capture traffic data
Analysis of the Packets
Control layer Analysis for the inspection
Blockchain-based Traceability of the deep packet(s) in traffic flow transmission sessions
Evaluation of the transmission sessions with its detailed Inspected
Host layer Analysis for the inspection

Figure 1. The Research Methodological Approach.

It was possible to do an examination of the traffic flow during transmission sessions by utilizing a network scenario that had been previously constructed. It is possible to initiate and stop transmissions with a certain payload at any time and for an endless period of time. Initiation of session packet inspection for transmissions (also known as transmission inspection), which is also known as transmission inspection (also known as transmission inspection). It was observed and documented how the flow of traffic changed from one session to the next.

Transmissions generate data traffic, which must be processed, sorted, and categorized before it can be transmitted on its route. You can make a pattern by following the procedures outlined below: Sessions are used to transfer data between two computers by transmitting the traffic flow. Data on traffic movement had been obtained and analyzed previously. Prepare the filter and analyzer for each transmission according to the instructions in the following section: As discussions take place, keep a watch on the traffic flow and make notes on it as it happens. The Blockchain-based investigation of Message Packets is now underway. Traceability of deep packets must be maintained throughout traffic flow transmission sessions at all times. This is crucial (s) An investigation of the control layer is carried out with the use of mathematical analysis. In addition to a thorough analysis of the host layer, a complete examination of the transmission intervals is carried out.

3.1. Blockchain-Enabled Deep Packet Inspection System Design

This research proposed to developed a blockchain-enabled DPI System, by first recognizing the general overall architectural framework of DPI and Blockchain (see Figure 2). The architectural is simply a typical network environment, where a predominant area referred to as the "Authorized Traffic region" is the expectation of any network design. This kind of a network environment employs network administrators' classifying and determining how all types of traffic are handled. At this stage, an IP header field called Differentiated Services Code Point (DSCP) is employed to categories the traffic originating from the authorized area. Consequently, no priority is anticipated unless explicitly assigned by the network administrator. The fact that any network is vulnerable to some sort of attack, makes it necessary to anticipate potential zone where attackers can attack. That is why, within the architecture an attacked region where unauthorized traffic can be generated is highlighted.

doi:10.20944/preprints202408.1475.v1

Any traffic flow that occurs within the network can be allowed to pass through the firewall in this scenario. The DPI system is configured to check and report the status of each packet after it has been inspected. In the event that the report was to be stored in the firewall buffer or any other storage, it would not be as safe, versatile, or traceable as if it were stored in the blockchain. This is where the current study initiates its examination, for which it further investigates the security and as well as the computational overhead that is associated with adopting a blockchain-based DPI system.

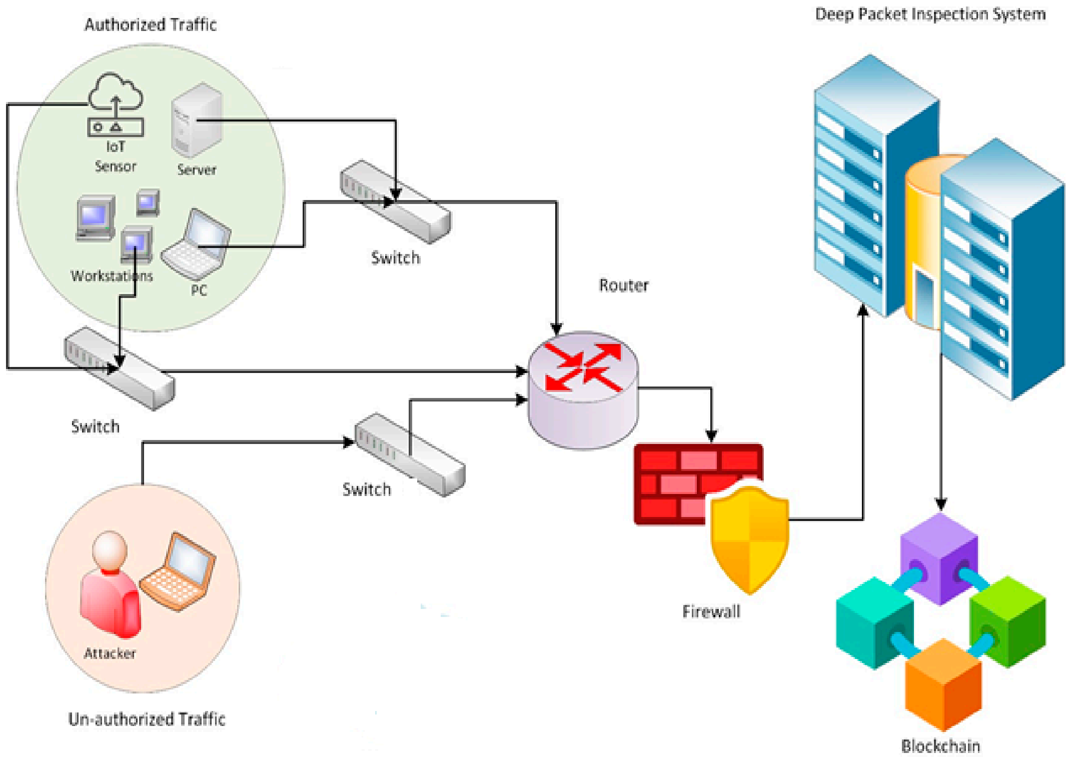


Figure 2. The Architectural Framework of Blockchain-Enabled Model for DPI.

3.2. The Propose Conceptual Framework

The conceptual framework for the study is a multifaceted construct comprising of three pivotal phases namely: the network data packet capturing, the DPI integrating –Blockchin phase and the smart contract development phase. These are structure into their algorithms.

3.2.1. Network Data Packet Capturing

The foundation of our conceptual framework lies in the meticulous recording of network data packets. It involves the steps presented in Algorithm 1. When an active network socket is open and flowing, the first algorithm focuses on the usual network packet capturing. This kind of activity is common for every transmission, and it exists whenever an active network socket is open. As shown in Line 1 to 4 of Algorithm 1, the capture network traffic routine will continue to monitor and capture all packets that are passing through while the data for the IP packets is being transmitted a certain storage. One of the first events that takes place from line 5 to line 10 is to determine whether the packet capture is normal or encrypted. In the event that the packet is not encrypted, it is possible to store it along with the details that correspond to it as the initial instruction. After reading the packet, the final component of the algorithm will make certain that a transmission is completely captured for that particular packet within the transmission session.

Algorithm 1 IP Network Packet Capturing

```
    Require: Active Network Socket
    Ensure: IP Packet Data in Transmission
1.  capture_network_traffic ():
2.      try:
3.          packet_repositoryArr
4.          open_network_socket ()
5.              while True do:
6.                  capture_packet (network_socket)
7.                  if is_non_encrypted_packet (packet):
8.                      packet_repositoryArr.append (packet)
9.                  end if
10.             end while
11.     except:
12.         print ("Interrupted by the user")
13.     finally:
14.         close_network_socket (network_socket)
15.             return packet_repositoryArr
16. is_non_encrypted_packet (packet):
17.     extract_header (packet)
18.     extract_payload (packet)
19. return not (extract_h.contains_flag)
```

3.2.1. The Proposed Concept of DPI Blockchain Integration

The DPI technology employed for analyzing and filtering network traffic is being enhanced by blockchain to address issues related to transparency, accountability, and privacy, in a similar approach of learning model utilising a decentralised deep learning framework and blockchain infrastructure [39]. Figure 3 present this research concept of DPI blockchain integration.

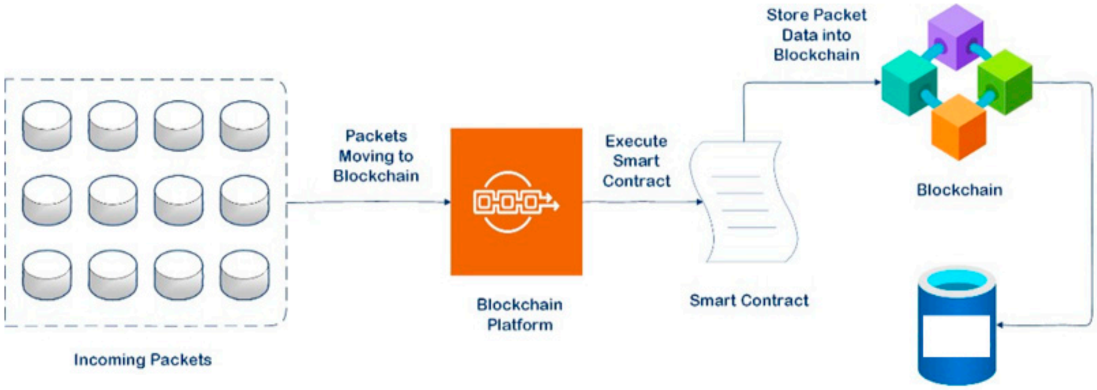


Figure 2. The Concept of DPI Blockchain Integration.

The concept dwell on incoming packet to the tranmission, while Algorithm 1 lead the direct approach of capturing inco,img packet in a transmission session, the proposed just captured packet only, but inspect them by DPI and the move them to blockchain based onsmart contract policy established. That is why Algorithm 2 is developed.

The algorithm necessitates the presence of an operational network socket that is actively processing traffic, with each packet in the transmission session being inspected. The inspection is exclusively performed using DPI, which involves scanning both the "Header field" and the "Payload" first. A boolean XoR is then established in the smart contract. Line 1 to line 2 indicates that each packet will utilize a "store and forward approach" at the beginning of the transmission session. The "store and forward approach" incurs additional computational cost, but it is essential for DPI prior to integration with blockchain. Therefore, Lines 17 to 23 of the method compute the incurred overhead caused by this operation in relation to "average latency", "processing time", "CPU Utilisation", and other performance metrics.

Once the packet is in the "store and forward approach" setting, Line 3 of the algorithm opens all the "header fields" while keeping the operation of opening the "Payload" distinct. This process is executed in a sequential manner, examining the content of all the "header fields" and the "bits" format of the "payload".

Line 4 of the algorithm performs an XoR operation to determine the result of the operation in Line 3. Line 5 executes the XoR operation only when both the "Header content" and the "Payload" remain unchanged. Only in this case, the packet may be classified as a "Normal" packet. Otherwise, it is classified as an "Anomaly" packet. Subsequently, line 6 enqueued all the inspected packets, categorized into the "Normal group" and the "Anomaly group".

The inspected queued packets are now linked to the blockchain, where each block has its associated packet contents and the hash of the block, formed by Line 7 to Line 16 of the algorithm.

```
Algorithm 2 DPI._Blockchain Intergration
Require: Active Network Socket open for Traffic flow
Ensure: Each Packet (P) = [Header (H) & Payload (Y)]
1   while (network transmission session start) do
2   Inspect_P (by store and forward approach)
3   Open (H) → [field-by-field] & (Y) → [bitt-by-bit]
4       (H xor Y) == Anomaly (A)=0; Normal (N)=1;
5       Execute Smart Contract(B)
6       B == A or N ← {H: [$h_1$, $h_2$, ..., $h_n$] & Y: [$y_1$, $y_2$, ..., $y_n$]}
7       if A_detected(H, Y) then
8           store_A_P in a block(b);
9               b ← hash & address (“P_A")
10              record_to_Blockchain(B):
11      else
12          Log_N_P → b
13              b ← hash & address (“P_N")
14              record_to_Blockchain(B)
15      end if
16  end while
17  Determine the average latency ($AL$)
18      $AL = \sum_{i-1}^{n} \frac{P_t}{T_r}$
19  Determine the processing time ($TT$)
20      $TT = \frac{P}{S}$
21  CPU Utilization ($U$)
22      $U = \frac{\sum t_n}{T}$
23  End
```

The process of associating the inspected packets in the queue with the blockchain, as carried out in algorithm 2, utilises a specially designed "package" to guarantee that a block within the ethereum smart contract executes the action. Therefore, algorithm 2 utilized algorithm 3 that present the development of the blockchain (Figure 4).

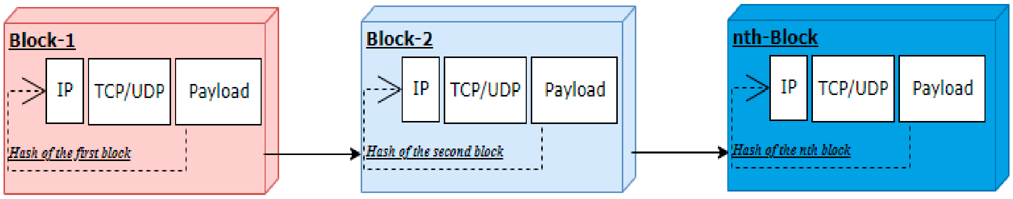


Figure 4. The blocks transmission orientation.

Typically, the responsibility for transferring or relocating the entire contents of the IP packet is assigned to the TCP/UDP headers.Hence, this research proposes hashing the movement protocol of the headers individually first, followed by the other header fields, and finally hashing the payload they carry independently, as illustrated in Figure 4. The purpose of doing so is that if any part of the packet header is modified, its hashed values will differentiate it from the others.

The algorithm 3 reserves Ethereum blocks that are linked to packet contents. Lines 2 and 3 of the Algorithm initialize the Ethereum platform by initialising the Ganache local blockchain. Lines 4 to 7 construct and initialize the pipeline through which examined packets are directly sent to the blockchain. However, during the transition to the blockchain, Line 8 to 15 ascertain the specific information included within the packet in the block. The complete processes occur in a store-and-forward technique, resulting in the calculation of overhead being performed by lines 17 to 23 of the algorithm, similar to Algorithm 2.

Algorithm 3 Smart_Contract(B) Blockchain Integration

```
Require: Ethereum Blockchain
Ensure: Inspected Packet (P) = [Header (H) & Payload (Y)]
1   while (setup_blockchain ()): do
2   initialize_ethereum ()
3   initialize_ganache_local_blockchain ()
4       integrate_blockchain_with_P(H, Y)
5       initialize.P(H, Y) ←(A or N)
6       connect_ethereum_blockchain()
7       try
8           while True do:;
9               packet: capture_packet()
10              Append_to_block(b):
11      if
12          b.has_A or N_class () :
13              insert_eth (A or N) but ≠ (A & N) or (A + N)
14              record_to_Blockchain(B)
15      end if
16  End while
17  Determine the average latency ($AL$)
18      $AL = \sum_{i-1}^{n} \frac{P_t}{T_r}$
19  Determine the processing time ($TT$)
20      $TT = \frac{P}{S}$
21  CPU Utilization ($U$)
22      $U = \frac{\sum t_n}{T}$
23  End
```

doi:10.20944/preprints202408.1475.v1

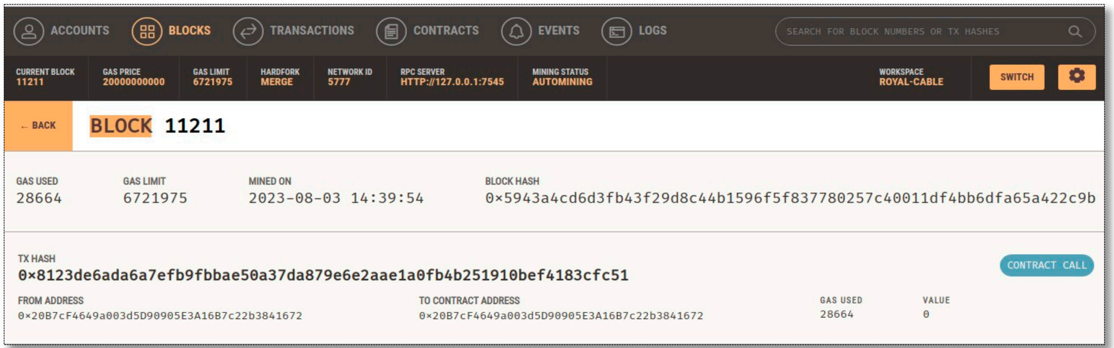
4. Experimental Analysis

This research employs a proposed experimental method that involves capturing network packets of the transmission over a DPI-Blockchain test-bed. This test-bed was specifically built to improve DPI practices, as well as to assess the performance of the network transmission traffic.

The purpose of the developed test-bed is not only to evaluate transmission performance but also to incorporate blockchain into DPI models. This incorporation enables the generation of a tamper-proof and transparent ledger of network activities, which fosters trust among stakeholders [40]. Moreover, by utilizing the tamper-resistant structure of blockchain, the model may generate safe and transparent logs of network traffic activities [41]. Furthermore, in addition to the design and development of the DPI-blockchain based system, this study also evaluated the computing overhead as one of the primary justifications for doing this experiment.

4.1. Development of DPI-Blockchain

This paper adopted the Truffle Suite to create, deploy, and manage blockchain applications in a streamlined and developer-friendly environment. It is important to clarify that the system only becomes operational when a network traffic transmission session commences. The network traffic data in the session will be examined, and then all the valuable information will be extracted and transferred to a blockchain ledger. This is accomplished by incorporating smart contract policy of: “Normal” and “Abnormal” packet evaluation by XoR. into the blockchain structure using Algorithm 1, 2, and 3. The Truffle Suite utilizes smart contracts to securely store the categorized data from inspected DPI. Therefore, the primary output of deploying the program is presented in Figure 5. This is a visual representation of a single block that has been created from a single packet. Hence, it can be noted that it includes its corresponding hash and the block's data in an encrypted form.



CURRENT BLOCK 11211 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE ROYAL-CABLE

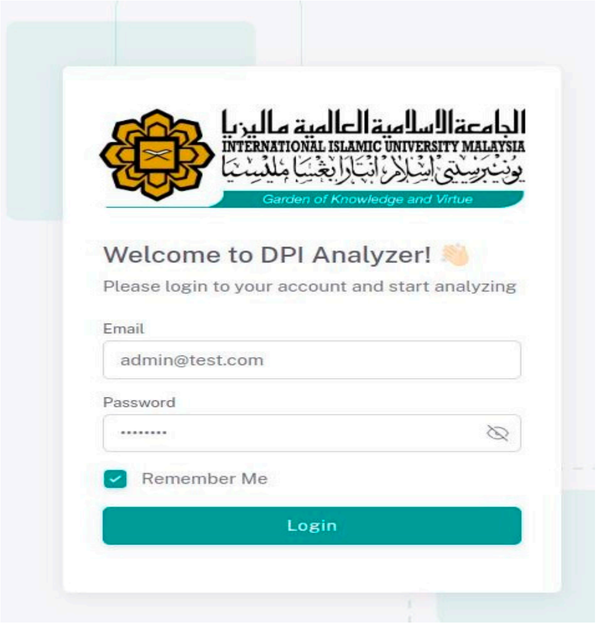
BLOCK 11211

GAS USED 28664
GAS LIMIT 6721975
MINED ON 2023-08-03 14:39:54
BLOCK HASH 0x5943a4cd6d3fb43f29d8c44b1596f5f837780257c40011df4bb6dfa65a422c9b

TX HASH 0x8123de6ada6a7efb9fbbae50a37da879e6e2aae1a0fb4b251910bef4183cfc51
FROM ADDRESS 0x20B7cF4649a003d5D90905E3A16B7c22b3841672
TO CONTRACT ADDRESS 0x20B7cF4649a003d5D90905E3A16B7c22b3841672
GAS USED 28664
VALUE 0

Figure 5. Single Block view of the Generated Block.

Furthermore, in order to improve the accessibility and usability of the entire system for experimental purposes, a user-friendly web-based interface has been created, as depicted in Figure 6. This interface functions as a central centre for visualising DPI-Blockchan output, enabling users to interactively explore and analyze it. The utilization of this integrated method for gathering, storing, and visualizing DPI packet data exemplifies a strong framework for thorough network analysis. A logging credential is necessary (see Figure 6).


INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
Garden of Knowledge and Virtue

Welcome to DPI Analyzer! 👋

Please login to your account and start analyzing

Email: admin@test.com

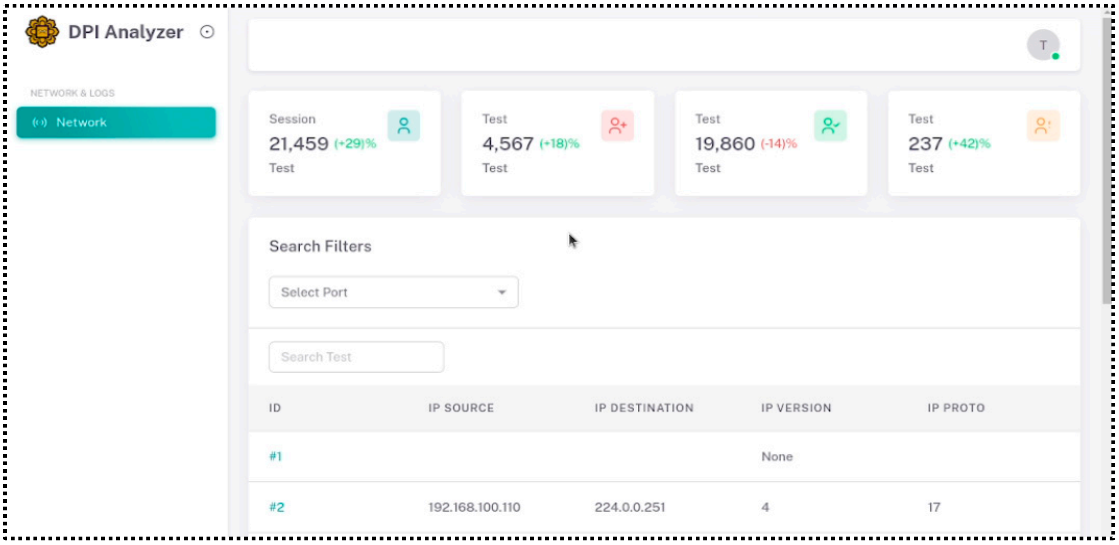
Password: ••••••••

☑ Remember Me

Login

Figure 6. Web-based user interface to visualize the packet data and related information.

Next, an administrator will initiate the system, which necessitates the establishment of an open IP traffic transmission session. Therefore, the initial step is to execute a "Store-and-forward" process, where the packet is received, examined using Deep Packet Inspection (DPI), and subsequently stored in a smart contract blockchain presented in Figure 7.



Session 21,459 (+29)% Test

Test 4,567 (+18)% Test

Test 19,860 (-14)% Test

Test 237 (+42)% Test

Search Filters

Select Port

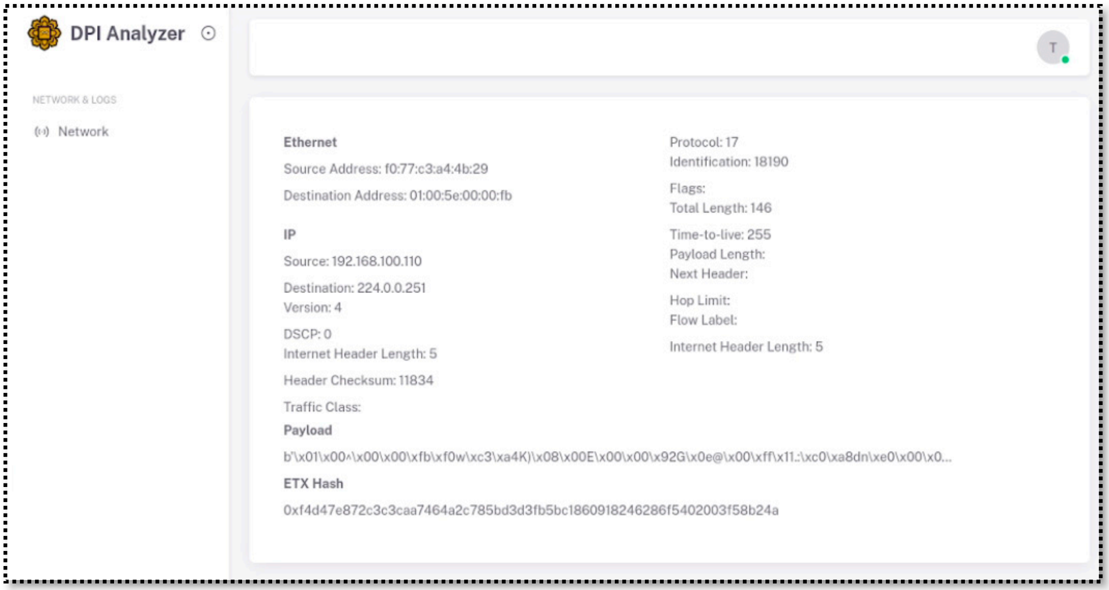
Search Test

ID	IP SOURCE	IP DESTINATION	IP VERSION	IP PROTO
#1			None	
#2	192.168.100.110	224.0.0.251	4	17

Figure 7. List DPI packet Gathered in Analysis.

The ID column in Figure 7 represents the block of the blockchain address for the final extracted DPI output. Therefore, the dashboard will display all of the inspected DPI packets, depending on the number of the inspected rounds. The computational overhead associated with the performance of creating and compiling the data is also assessed as well.

An exploration of ID #2 from Figure 7, displayed the attributed of that particular packet inspected by DPI, and now comes with its corresponding hash and the details in block's data, were the payload is seen in an encrypted format and the hash values below it (see Figure 8).



```
Ethernet
Source Address: f0:77:c3:a4:4b:29
Destination Address: 01:00:5e:00:00:fb

IP
Source: 192.168.100.110
Destination: 224.0.0.251
Version: 4
DSCP: 0
Internet Header Length: 5
Header Checksum: 11834
Traffic Class:

Protocol: 17
Identification: 18190
Flags:
Total Length: 146
Time-to-live: 255
Payload Length:
Next Header:
Hop Limit:
Flow Label:
Internet Header Length: 5

Payload
b'\x01\x00^\x00\x00\xfb\xf0w\xc3\xa4K)\x08\x00E\x00\x00\x92G\x0e@\x00\xff\x11.:\xc0\xa8dn\xe0\x00\x0...
ETX Hash
0xf4d47e872c3c3caa7464a2c785bd3d3fb5bc1860918246286f5402003f58b24a
```

Figure 8. The Entire DPI- Block View Details of the Generated Block.

4.2. Experimental Evaluation

Multiple rounds of transmission were conducted, where data was transmitted from the local network to numerous networks over a span of 4 months. The analysis of packet data in these transmissions was conducted using the scapy Python module, which provides robust tools for interfacing with and analysing network protocols. This advanced method allows for the smooth integration of deep packet inspection (DPI) and blockchain technology to capture real-time traffic data from local network ports. The DPI packet data that is acquired is not only limited to real-time monitoring, but it is also methodically arranged and saved in a specialised blockchain, as explained in the preceding section. This function serves as the primary method for efficiently retrieving DPI packet data for subsequent analysis. Additionally, it serves as an organized repository for long-term storage and reference. To conduct a network Moreover, after capturing the network traffic, analyze the captured packets to gain insights into the flow of data, including packet size and data for transmissions. The outcome of this experiment not only helps in understanding network behavior but also enables testing and validation of network configurations, security protocols, and application performance under controlled conditions.

The transmission testbed described in section 3 and 4 has been setup and the transmission session data were gathered and presented in this section. At first the research establishment a network session and test the traffic flow within the transmissions sessions (See Table 1). That is the initial block set out for the blockchain captured during the initial test, which is followed by the traffic rounds within a block presented as (Rounds). Furthermore, the application that was used within each transmission session was presented as the "payload." The (SYN and ACK), which are the TCP transmission parameters, are presented in the table as well. The notification of the hash of each round is presented by (#B1), while the urgent part of the packet header is (URG). The data packet in transmission is given by (Data_pkt), and the tagging of each session is presented by (Tags). The transmission flags within the transmission are given by (Flags) while the packet inter-arrival times are presented as (IAT).

Table 1. The Establishment of the Traffic Flow Transmissions Sessions.

Block	Rounds	Payload	SYN	ACK	#B1	URG	Data_pkt	Tags	Flags	IAT
1	2	HTTP	1	1	0	0	4	0	0	6756.7
2	2	HTTP	0	1	0	0	135	0	0	150.0

3	7	HTTP	0	0	0	0	4	0	0	12302.4
4	15	HTTP	0	0	0	0	2	0	0	165.0
5	21	HTTP	0	0	0	0	7	0	0	36092.0
6	1	HTTP	0	1	0	1	5	0	0	5935.0
7	6	HTTP	0	0	0	0	31	0	0	151.0
8	8	HTTP	0	1	0	0	4	0	0	1441.0
9	9	HTTP	0	1	0	0	2	0	0	42319.4
10	2	HTTP	1	1	0	0	2	0	0	17813.5

Block (number of block), Rounds (number times visited), Payload (protocol), SYN (1=set / 0= not-set), ACK (1=set / 0= not-set) #B1 (1=set / 0= not-set) URG (1=set / 0= not-set), Data_pkt (number of packet) Tags (1=on / 0= off) Flags (1=on / 0= off) IAT (millisecond).

The traffic orientation is established each with a hashed block from 1 to 10 blocks. The transmission session for the first simulation was carried out for 10 sessions. That is why when a transmission is launched, it goes through for every packet, then. the hash of a block indicating that a packet is on transmission was shared among all blocks in the transmission session. When the hash is 1 it is indicating that the packet in the transmission was not recognized by the block, whereas when it is zero, it indicates that the block is hashed and being recognized. While this scale to all levels, the values of Tags and TCP flags are all zeros indicating that there is no issue with the transmission flow. This information's are all kept within each block. Hence each block can keep track of the TCP connection. A flag is raised to signify an irregular circumstance in the exchange of SYN+ACK without an initial SYN packet, but it is not recorded. The blockchain was established to have a block that indicates a packet is examined and the hash of that block shared among all blocks in a transmission session. The flags, hashes block, and tags do not appear to alter in the succeeding transmission rounds, which are carried out with the same transmission parameters as the previous transmission rounds. Even if a flag does not suggest anything, it is feasible for it to be logged in the block if it is raised in order to alert the exchange to an unexpected occurrence. As the findings of this study proved, this is the case. A block that signifies that a packet has been inspected is included in the design of the blockchain for each transmission session; the hash of that block is shared across all blocks in the session, according to the design. During the transmission session, the block also keeps track of any traffic that is related with the programme and is transmitted through it. When this occurs, it shows that the procedure has been successfully performed.

While undertaking the next scenario, which is meant for the verification of the traffic flow transmissions sessions (see Table 2), the hash value of 1 indicates that will indicate if the packet in the transmission was not recognized by the block was not received in all cases, while the hash value of zero indicates that the block has been hashed and is being recognized by the block has been the results that was gathered. At whatever size, the communication flow is unaffected by Tags or TCP flags because they are all reveals to be zero. Each block contains all of the information it needed. As a result, each block keeps tabs on the TCP connection at all times. There must also be an individual block for each transmission session that can be shared by all packets regardless of whether or not they are part of the same transmission session or not. This study also keeps track of all the traffic that comes from the transmission that are being used.

Table 2. The verification of the Traffic Flow Transmissions Sessions.

Block	Rounds	Payload	SYN	ACK	#B1	URG	Data_pkt	Tags	Flags	IAT
1	2	HTTP	1	1	0	0	2.3	0	0	390.6
2	2	HTTP	1	1	0	0	78.5	0	0	8.7
3	2	HTTP	0	1	0	0	2.3	0	0	711.1
4	2	HTTP	0	1	0	0	1.2	0	0	9.5
5	2	HTTP	0	0	0	0	4.1	0	0	2086.2
6	2	HTTP	1	1	0	0	2.9	0	0	343.1

7	2	HTTP	0	1	0	0	18.0	0	0	8.7
8	2	HTTP	0	1	0	0	2.3	0	0	83.3
9	2	HTTP	1	0	0	0	1.2	0	0	2446.2
10	2	HTTP	1	1	0	0	1.2	0	0	1029.7

Block (number of block), Rounds (number times visited), Payload (protocol), SYN (1=set / 0= not-set), ACK (1=set / 0= not-set) #B1 (1=set / 0= not-set) URG (1=set / 0= not-set), Data_pkt (number of packet) Tags (1=on / 0= off) Flags (1=on / 0= off) IAT (millisecond).

5. Presentation of the Results

The transmission as a whole and an analysis of the computational overhead are presented here. First, the performance of the system is the most important part of the research question, which is why it was calculated. In this case, the following parameters are evaluated: "Number of Data Packets" (NDP), Number of Network Open Socket (NNN), DPI Processing Time (ms) (DPI), CPU Usage in (%) (CPU), Memory Usage (bits/sec) (RAM), Network Latency (ms) (NTL), and Throughput (bits/sec) (TTP). The performance of Seven transmission session were sampled for this analysis and are presented in Figure 9. Despite combining the performance within the same measure, it should be clear that CPU usage is in percentage, hence it only has values within less or equal to hundred, whereas, the number of open socket use are within thousands. Nevertheless, what can be deduce from the entire result of computational overhead is that the greater the number of open socket in transmission, the greeter the packets, the more time it requires for DPI and overall the greater the computational overhead.

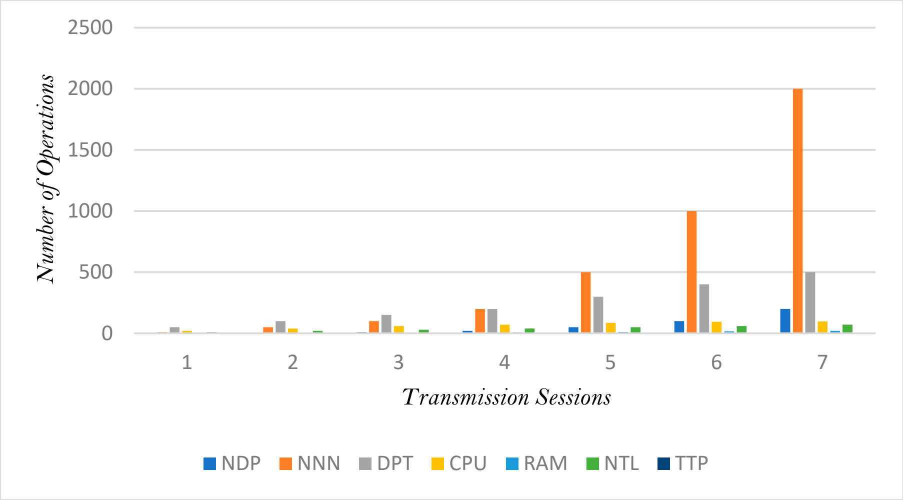


Figure 9. The Computational Overhead Performance of Seven Transmission Sessions.

It has been discovered via further investigation that the fact that the number of network open sockets inside a transmission grows does not necessarily suggest that the data packet increases as well (see Figure 10). To put it another way, it does not mean that the value of DPI and the process of moving the result of DPI to blockchain would rise as the number of open sockets increases. Considering that there might not be a significant quantity of packets to analyze in some open sockets, this is not only obvious but also has the potential to be implemented in theory.

doi:10.20944/preprints202408.1475.v1

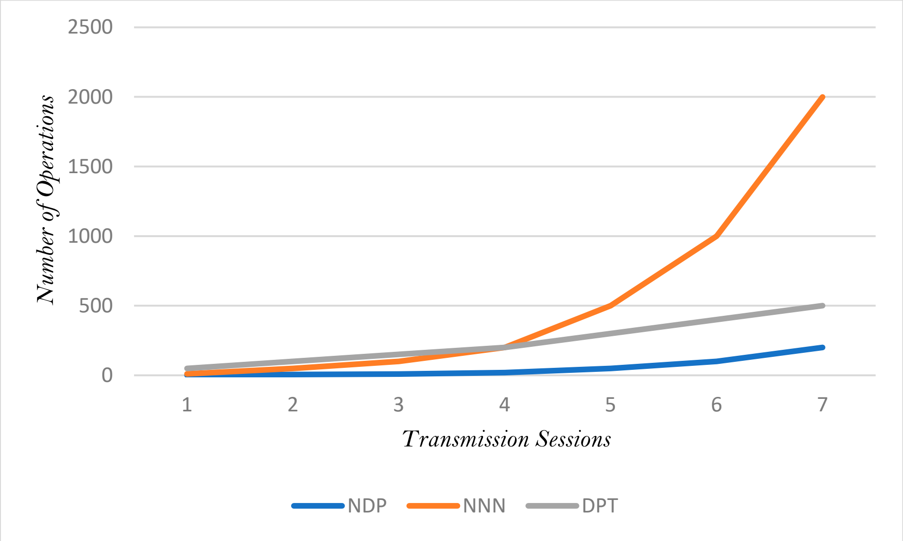


Figure 10. The Computational Overhead Associated to the Number of Network Open Sockets.

In terms of the general computational overhead measure, the findings of the study revealed that once a DPI was initiated in conjunction with blockchain-enabled record keeping of the services, the utilisation of the CPU or utilisation of the memory increased exponentially alongside the utilisation of the memory. In addition, the increases in memory and CPU utilisation had an impact on the and associated with network latency and throughput overhead (see Figure 11).

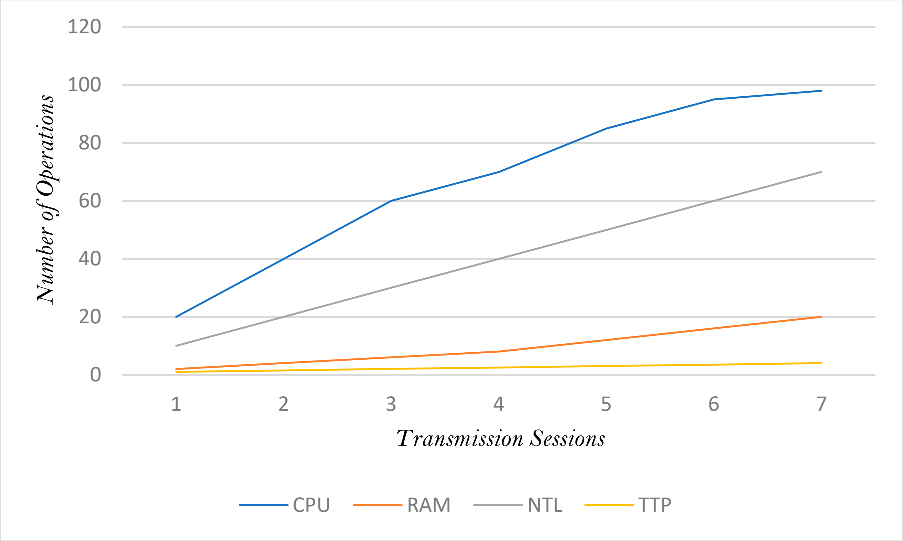


Figure 11. The General Computational Overhead.

Therefore, the system needs to be optimised such that it can effectively manage increased loads while yet maintaining acceptable performance metrics. The enhancements to security that blockchain technology provides could make it simpler to identify instances in which data has been altered or in which an unauthorized attempt has been made to access the system. When blockchain technology is put into practice, this will result in a considerable reduction in the number of instances of data manipulation, demonstrating the blockchain's resistance to such manipulation.

5. Discussion

This research has identified the need for tracing each packet in a transmission session, in order to identify the "Normal" and "Anomaly" packets as well as keeping the entire reports in the blockchain. The motivation lies with the fact that transmission in real time is growing, and as computer networks get larger and more intricate, monitoring and identify the state of the packet is crucial. In order to analyses network traffic, it is vital to possess an extensive array of transmission and packet inspection.

The study has determined that the utilization and management of each data packet (consisting of payload and header) during a transmission session can result in both a secure transmission session and comprehensive information necessary for decision-making, particularly about network security concerns. Furthermore, the security concern can be effectively addressed through the use of Deep Packet Inspection (DPI), while the preservation of records can be achieved with the implementation of blockchain technology. The problem of computer overhead becomes increasingly urgent. Hence, the research also investigates the computational burden that may arise as a result of this phenomenon.

According to the findings of the study, any rise in the transmission rate is accompanied by an increase in the amount of computing overhead. Therefore, when transmission rates begin at a higher value, a greater amount of information pertaining to the packet will be released from the beginning. In the opposite direction, when the transmission rate changes to a lower value, the amount of both DPI and the report associated to it decrease. Consequently, it is possible to determine more extended details regarding the DPI report of the header of the packet by increasing the transmission rate at the beginning of the transmission and decreasing it towards the end of the transmission. The consolidation and storage of a packet within a memory block within the blockchain occurs after the packet has been subjected to verification. This action is communicated to all of the other blocks on the blockchain simultaneously. Through the utilisation of this method, it is possible to authenticate each and every DPI packet that travels across the network. Despite the fact that the design and implementation of DPI-blockchain based systems, it come with a excess of benefits, it is essential to keep in mind that there is a large amount of processing cost involved.

The research findings have resulted in the creation of a new method for combining blockchain with DPI in order to summarise events related to the movement of traffic on computer networks. By employing this approach, the network effectively managed the movement of traffic, recorded and stored the DPI report, and securely stored the entire transmission session header in a Blockchain that operated on smart contracts. To test the validity of the system, two distinct experimental situations are conducted. In the initial scenario, a thorough examination of the DPI transfer is conducted without the integration of the blockchain. Next, the transmission session is captured, which involves the implementation of blockchain technology. The findings indicate that adopting blockchain technology enhances the security of transmitting DPI by providing protection against "Tampering Incidents," "Unauthorised Access Attempts," "Auditability," and various other security concerns. However, the use of blockchain-based deep packet inspection (DPI) results in a performance overhead. This includes an increase in "DPI Processing Time" from 68 milliseconds to 150 milliseconds, a twenty percent increase in "CPU Usage", a fifteen millisecond increase in Network Latency from twenty milliseconds to thirty-five milliseconds, and an increase in practically all other computing resources. The study concludes that integrating blockchain with DPI results in an increased performance overhead. However, it does provide secure DPI data that may be utilised for decision-making purposes.

The current research justified its finding by taking into account that Blockchain technology has also being use in many diffierent application where recording of state is important. This was supported by the fact that implementing blockchain technology, provide a scheme for which transaction can be validated. That is considering the fact that Blockchain technology was also used in the creation of event-driven record keeping associated with integrity. Hence, the point here is establishing validation, is crucial. That is if transmission session is required to be checked, then the record should be tracked. Hence, in the general application of blockchain, the technology is employed to protect one's identity through anonymity. The processing of transactions can be greatly accelerated in such a situation. In a similar vein, smart contract technology operates in the same way as traditional contracts in terms of idea. Adoption is achievable in all situations due to the simplicity of the blockchain technology. As a result, smart contracts are becoming increasingly popular. Additionally, other new technologies emerge as a result of it, which decreases the necessity for a database for the purpose of storing records. Consodering the number of devices that required to be in the Internet nowadays, which some also required to be in a decentralized system that treats smart contracts on an equal footing, exemplifies the same principle as well. Smart contracts are seen as fully functioning members of society in the context of blockchain technology, which is being developed.

6. Conclusions

This research has studied the impact of DPI, taking into consideration the use of Blockchain. In the course of research, the study was able to determine the impact of DPI while also taking the use of Blockchain technology into account. Essentially, this is inspired by the premise that tracing each data packet in a transmission session can reveal additional information about the transmission session as a whole. In its most basic form, this is supported by empirical evidence. Allowing each packet to be identified and tracked as it travels through a transmission session is a huge benefit, and the capacity to do so is a significant advantage. This research resulted in the creation of a transmission session, which was then used to analyze a range of transmission scenarios in order to identify the influence of blockchain technology. As a result of the study's findings, it has been observed that when the transmission rate is increased, or when the data in a transmission rate is increased, the packet data that is currently being broadcast contains more information about the transmission session than it did with low amount of data. The fact that a packet's header can be released at any point in time when the transmission speed varies, it is also taken into consideration, regardless of whether the transmission speed is increased or decreased. According to the findings of this study, each block on a blockchain is capable of preserving the integrity of all packet information while not compromising the speed or efficiency of the network in any way whatsoever. This has significant implications because when data in each payload and header is transmitted during transmission, the integrity of a packet on all blocks in Blockchain can be detected more efficiently when the transmission is moving faster than when the transmission is moving slowly, which has significant implications. A fundamental advantage of blockchain technology over other systems is the ability to uniquely identify data included within each payload and header during transmission. Therefore, this current study has contributed to the body on knowledge that deals with analyzing network packet in general.

Author Contributions: There are only two authors in this research and all of them contributed equally, except that the main author in in charge of coming with the idea. Similarly, all the authors have read and agreed to submit the paper to the journal.

Funding: This work was fully supported through the MDPI Discount Vouchers, no any other financial source that is received from any one on the publication of this paper

Institutional Review Board Statement: Not Applicable

Informed Consent Statement: Not Applicable

Data Availability Statement: Not Applicable

Acknowledgments: This research is made possible and supported by UMP-IIUM Sustainable Research Collaboration 2022 Research Grant (IUMP-SRCG22-014-0014), no any financial support coming from the grant on the publication of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Khan,F.A. Ibrahim. A.A. Machine Learning-based Enhanced Deep Packet Inspection for IP Packet Priority Classification with Differentiated Services Code Point for Advance Network Management. Journal of Telecommunication, Electronic and Computer Engineering (JTEC). 2024 Jun 30;16(2):5-12.
2. Heo JW, Ramachandran GS, Dorri A, Jurdak R. Blockchain data storage optimisations: a comprehensive survey. ACM Computing Surveys. 2024 Apr 9;56(7):1-27.
3. Idrees R, Maiti A. A Blockchain-Driven Smart Broker for Data Quality Assurance of the Tagged Periodic IoT Data in Publisher-Subscriber Model. Applied Sciences. 2024 Jan;14(13):5907.

4. Adochiei, F.C.; Ciucu, R.; Adochiei, I.R.; Argatu, F.C.; Enache, B.; Miron, C.; Seritan, G. Brain Mapping using a Blockchain Approach. In Proceedings of the 2019 E-Health and Bioengineering Conference (EHB), Iasi, Romania, 21–23 November 2019; pp. 1–4.
5. Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K. and Choo, K.K.R., 2020. Blockchain-based identity management systems: A review. Journal of network and computer applications, 166, p.102731. https://doi.org/10.1016/j.jnca.2020.102731
6. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.
7. ramodAIML. BlockChain Principle, Type & Application & Why You Should Care About It? 2020. Available online: https://medium.com/the-programmer/blockchain-principle-type-application-why-you-should-care-about-it-249417b516cc (accessed on 21 September 2020).
8. Vaughn, W. Open Vs Closed Blockchains: Let's End This Madness. The Medium. 2015. Available online: https://medium.com/WayneVaughan/open-vs-closedblockchains-let-s-end-this-madness-8313e4095ead (accessed on 17 June 2020).
9. Jayachandran, P. The Difference between Public and Private Blockchain. Blockchain Unleashed: IBM Blockchain Blog 2017, 30, 102-112.
10. Cobur30, 30n, J. "Public vs. private blockchains: Understanding the differences." Blocks Decoded, https://blocksdecoded. com/public-privateblockchains/(Accesed on Sept. 17, 2018) (2018).
11. Bahga, A.; Madisetti, V.K. Blockchain Platform for Industrial Internet of Things. J. Softw. Eng. Appl. 2016, 9, 533–546. https://doi.org/10.4236/jsea.2016.910036.
12. Fauvel, W. Blockchain Advantages and Disadvantages. 2017. Available online: https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0 (accessed on 20 August 2021).
13. Songara, A.; Chouhan, L. Blockchain: A Decentralized Technique for Securing Internet of Things. In Conference on Emerging Trends in Engineering Innovations & Technology Management (ICET: EITM-2017) Prague, Czechia, World Academy of Science, Engineering and Technology
14. Light, J. The Differences between a Hard Fork, a Soft Fork, and a Chain Split, and What They Mean for the Future of Bitcoin. 2017. Available online: https://medium.com/@lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9 (accessed on 16 March 2020).
15. Gupta, N.; Bedi, P. E-waste Management Using Blockchain based Smart Contracts. In Proceedings of the 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 19–22 September 2018; pp. 915–921. https://doi.org/10.1109/icacci.2018.8554912.
16. Szabo, N. Smart contracts: Building blocks for digital markets. EXTROPY J. Transhumanist Thought 1996, 16, 18.
17. Jani, K. Jani, Shailak. "Smart Contracts: Building Blocks for Digital Transformation." Indira Gandhi National Open University (2020). Available online: https://www.researchgate.net/publication/340376424_Smart_Contracts_Building_Blocks_for_Digital_Transformation (accessed on 27 January 2021).
18. Heeks, Richard, Logakanthi Subramanian, and Carys Jones. "Understanding e-waste management in developing countries: Strategies, determinants, and policy implications in the Indian ICT sector." Information Technology for Development 21.4 (2015): 653-667.
19. Ikhlayel, M. An integrated approach to establish e-waste management systems for developing countries. J. Clean. Prod. 2018, 170, 119–130. https://doi.org/10.1016/j.jclepro.2017.09.137.
20. Miglani, A.; Kumar, N.; Chamola, V.; Zeadally, S. Blockchain for Internet of Energy management: Review, solutions, and challenges. Comput. Commun. 2020, 151, 395–418. https://doi.org/10.1016/j.comcom.2020.01.014.
21. Aujla, G.S.; Chaudhary, R.; Kumar, N.; Das, A.K.; Rodrigues, J. SecSVA: Secure Storage, Verification, and Auditing of Big Data in the Cloud Environment. IEEE Commun. Mag. 2018, 56, 78–85. https://doi.org/10.1109/mcom.2018.1700379.
22. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.-K.R.; Zomaya, A.Y. Blockchain for smart communities: Applications, challenges and opportunities. J. Netw. Comput. Appl. 2019, 144, 13–48. https://doi.org/10.1016/j.jnca.2019.06.018.
23. Pedrosa, A.R.; Pau, G. ChargeltUp: On Blockchain-based technologies for Autonomous Vehicles. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems ACM, Munich, Germany, 15 June 2018; pp. 87–92.
24. Zhang K, Deng M, Gong B, Miao Y, Ning J. Privacy-Preserving Traceable Encrypted Traffic Inspection in Blockchain-based Industrial IoT. IEEE Internet of Things Journal. 2023 Jul 21.
25. Song W, Beshley M, Przystupa K, Beshley H, Kochan O, Pryslupskyi A, Pieniak D, Su J. A software deep packet inspection system for network traffic analysis and anomaly detection. Sensors. 2020 Mar 14;20(6):1637.
26. Ren H, Li H, Liu D, Xu G, Cheng N, Shen X. Privacy-preserving efficient verifiable deep packet inspection for cloud-assisted middlebox. IEEE Transactions on Cloud Computing. 2020 Apr 29;10(2):1052-64.

27. Zhang X, Geng W, Song Y, Cheng H, Xu K, Li Q. Privacy-Preserving and Lightweight Verification of Deep Packet Inspection in Clouds. IEEE/ACM Transactions on Networking. 2023 Jun 21;32(1):159-74.
28. Li W, Meng W, Wang Y, Li J. Enhancing blackslist-based packet filtration using blockchain in wireless sensor networks. InWireless Algorithms, Systems, and Applications: 16th International Conference, WASA 2021, Nanjing, China, June 25–27, 2021, Proceedings, Part II 16 2021 (pp. 624-635). Springer International Publishing.
29. Khalilov, M.C.K.; Levi, A. A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems. IEEE Commun. Surv. Tutor. 2018, 20, 2543–2585. https://doi.org/10.1109/comst.2018.2818623.
30. Asatanattakool, P.; Techapanupreeda, C. Blockchain: Challenges and applications. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 473–475.
31. Sahoo, S.; Halder, R. Blockchain-Based Forward and Reverse Supply Chains for E-waste Management. In International Conference on Future Data and Security Engineering; Springer: Cham, Switzerland, 2020; pp. 201–220. https://doi.org/10.1007/978-3-030-63924-2_12.
32. Poongodi, M.; Hamdi, M.; Vijayakumar, V.; Rawal, B.S.; Maode, M. An Effective Electronic waste management solution based on Blockchain Smart Contract in 5G Communities. In Proceedings of the 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 10–12 September 2020. https://doi.org/10.1109/5gwf49715.2020.9221346.
33. Buldas, A.; Draheim, D.; Nagumo, T.; Vedeshin, A. Blockchain Technology: Intrinsic Technological and Socio-Economic Barriers. In International Conference on Future Data and Security Engineering; Springer: Cham, Switzerland, 2020; 3–27. https://doi.org/10.1007/978-3-030-63924-2_1.
34. Chaudhary, K.; Padmanabhan, P.; Verma, D.; Yadav, P.D. Blockchain: A game changer in electronic waste management in India. Int. J. Integr. Supply Manag. 2021, 14, 167–182. https://doi.org/10.1504/ijism.2021.115680.
35. Salmon, D.; Babbitt, C.W.; Babbitt, G.A.; Wilmer, C.E. A framework for modeling fraud in E-waste management. Resour. Conserv. Recycl. 2021, 171, 105613. https://doi.org/10.1016/j.resconrec.2021.105613.
36. Dasaklis, T.K.; Casino, F.; Patsakis, C. A traceability and auditing framework for electronic equipment reverse logistics based on blockchain: The case of mobile phones. In Proceedings of the 2020 11th International Conference on Information, Intelligence, Systems and Applications, Piraeus, Greece, 15–17 July 2020; pp. 1–7. https://doi.org/10.1109/iisa50023.2020.9284394.
37. Gopalakrishnan, P.K.; Hall, J.; Behdad, S. Cost analysis and optimization of Blockchain-based solid waste management traceability system. Waste Manag. 2020, 120, 594–607. https://doi.org/10.1016/j.wasman.2020.10.027.
38. Marchesi, L.; Marchesi, M.; Tonelli, R. ABCDE–agile block chain DApp engineering. Blockchain: Res. Appl. 2020, 1, 100002.
39. Zhang Y, Liang Y, Jia B, Wang P, Zhang X. A blockchain-enabled learning model based on distributed deep learning architecture. International Journal of Intelligent Systems. 2022 Sep;37(9):6577-604.
40. Alkadi O, Moustafa N, Turnbull B, Choo KK. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal. 2020 May 22;8(12):9463-72.
41. Wang Z, Liu Y, He D, Chan S. Intrusion detection methods based on integrated deep learning model. computers & security. 2021 Apr 1; 103:102177.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.