[1,*]Jian Hu
[1]Hailin Wang
[1]Hanruo Li

Network Attack Chain Security Model Construction Based On Attack Framework

Abstract: **-** All facets of society's governance, economics, and culture have been impacted by networking. Network attacks have become more common as a result of the digital revolution, which has also facilitated major changes in worldwide communication and accelerated the development of human society. An unauthorized attempt to access a network with the goal of committing theft or other forms of damage is what we call a network attack. This article focuses on building a chain security model utilising the block chain concept in order to address the issue of inaccurate assessments of forged malicious behavioural methods for identification. It uses the NIK-256 hashing algorithm to identify valid users utilising time-dependent verification. Passwords and recorded times are maintained in a combined chain database, which combines blockchain technology and the Trusted Platform Module (TPM), improving data security and privacy. After that, we schedule users using the Whale optimisation algorithm (WOA), which decreases difficulty, and then a smart contract is developed that grants authorised users access control based on their level of trust and permission. The proposed approach, known as Hyb_chain_TPM, implements countermeasures in accordance with the attack risk level and stores the attack graph in a combined chain database for future attack forecasting. Utilising diverse attack datasets, extensive tests are run to validate this system. Additionally, the outcomes of privacy protection and AI processes are assessed independently and contrasted using a variety of current techniques.

Keywords: Network security, Attack, Chain model, Hashing, Scheduling, Privacy preservation.

I. INTRODUCTION

Mobile computing technology has been deeply integrated into daily life as a result of IT development and has emerged as a major problem. Schedule, financial, and social application services, among others, are provided by mobile and computing technologies through a variety of interfaces. Additionally, it provides a range of connectivity settings, including 3G, 4G, Wi-Fi, and Bluetooth, and users can access the internet whenever and wherever they choose. Many smart devices have seen increased use as a result. Because mobile devices use a universal operating system (OS), it is simple to create malicious mobile programmes that has a high transplantation rate. Therefore, criminals take advantage of mobile weaknesses and security flaws. And the amount of harm it is doing is sharply increasing [1]. Blockchain, a distributed append-only public ledger technology, was primarily developed for use with Bitcoin and other cryptocurrencies. The idea of blockchain, which was first suggested in 2008 by Nakamato [2], has gained a lot of attention in recent years as a new peer-to-peer (P2P) technology for distributed computing and decentralised data sharing. The blockchain can fend against attacks that aim to seize control of the system since it has adopted cryptographic technology and lacks a centralised control actor or a centralised data storage. Later, in 2013, the digital currency Ethereum, a state-machine that runs transactions, became the first to create blockchain technology. Unexpectedly, blockchain is being used in a variety of industries outside of cryptocurrencies because of its distinctive and alluring properties, including transaction security, confidentiality, unalterable nature of data, transparency truthfulness, authorisation, system openness, and tolerance for failures. Managing identities [3], smart transportation [4], the management of supply chains, mobile crowd sensing [5], agribusiness [6], Industries 4.0 [7], [8], Internet of Renewable Energy (IoE), and safety in critical applications are a few of the topics. The blockchain consists of a sequence of blocks that are linked together through their hash values. Users' digitally signed transactions in a P2P network are recorded in a public ledger in the blockchain network. The user's public key can be used by other users to encrypt communications, while the user's private key can be used to decrypt messages encrypted with the public key. The public key functions as the blockchain's equivalent of a unique address, while the private key is used to digitally sign transactions on the blockchain. Asymmetric cryptography is used to encrypt the communication using the associated public key and decrypt it. At first, a user signs a transaction with their private key and broadcasts it to their peers [9]. When a signed transaction is received, peers validate it and then send it out to the network. To get a consensus agreement, all parties that are involved in the transaction mutually validate it. Once a distributed consensus has been reached, a unique user known as a miner adds the legitimate transaction to a block that has been timestamped[10]. The miner includes the block and broadcasts it back into the network. The broadcast block is attached to the blockchain after being validated and hash-matched with the preceding block on the chain, which contains the transaction. Blockchain technology can be characterised as either private

[1] Digital Security Center of Information Center of Yunnan Power Grid Co., LTD, Kunming, Yunnan, 650011, China
*Corresponding author e-mail: hjiang2023@126.com

(permission-based) or public (permissionless), depending on how data is managed and the sort of apps used. Both groups are distributed and provide some security for the ledger against malicious or careless users[11]. The fundamental differences between public and private blockchains lie in the implementation of the consensus process, the maintenance of the ledger, and the authorization to join the P2P network. Extensive examples of these classes are provided in [12]. Blockchains in the IoT environment could be categorised depending on authorisation and verification. On the opposite hand, no outside entity may influence the choice of miners or the addition of a new user to the blockchain network in a public blockchain (which is typically permissionless). Both the private sector and academic institutions have shown a growing interest in tackling the most pressing issues in blockchain research in recent years [13, 14]. For instance, since consensus protocols are a crucial part of blockchain technology, they have become a popular research area. Additionally, the blockchain consensus procedures are threatened by blockchain splits. Additionally, it has been noted that a new blockchain has a vulnerability of roughly 51% [15]. A large amount of electricity must be consumed simultaneously to maintain many blockchains [16]. In view of this the contributions of this work are as follows

- Using Trust Authority (TA), that displays the user's authorised duration, can carry out period-based verification by using NIK-256 to verify the valid users. TA subsequently gives security credentials to customers via credential acquisition and registration. The individual's profile is then subject to ban requests that fail after thrice.
- Additionally, HybridChain, a merger of blockchain and Trusted Platform Module (TPM), that enhances network scaling as well as information privacy, stores the registration period and passcode in hashed code.
- The Whale optimisation algorithm (WOA), that lessens complexity, is utilised for scheduling the authenticated clients according to a variety of characteristics like latency, productivity, resources power, and precedence. The authorised individuals receive access control via smart contracts that are according to their level of confidence and authorization.
- The risk evaluation is then used to investigate the effects of the attacks, and an attack graph is created to show the attack's progression. Following that, risk-based preventative actions are implemented to further secure the network, and the attack graph is saved in the Hyb_chain_TPM for eventual attack forecasting. Additionally, the network's infrastructure is updated and rebuilt to reduce the destruction of packets.

Following this, we present the proposed strategy and methodologies in Section 3, the experimental results and discussion in Section 4, and the chapter's conclusion and directions for further research in Section 5.

II. RELATED WORKS

Scientists have been attempting to solve the issue of integrating BC with networks in recent years [17,18]. The difficulties resulting from the integration of network and BC were examined by Reyna et al. [19]. They offered potential integration strategies as well as platforms that combine network and BC in a broad sense. In contrast to the work mentioned above, we give a thorough assessment divided into application categories such the smart city. By concentrating on specific use cases and objectives and outlining the "technologies" or "models" used, we attempt to approach the survey from a different angle and avoid taking the operating environment of the solution into account. We additionally highlight a distinctive BC feature that supports data exchanges in the computerised industry. A basic overview regarding network security issues was provided by Kouicem et al. [20], while BC constituting any of the answers. Corresponding to this, Jesus et al. [21] examined the "Stalker" threat and the adoption of BC for safeguarding IoT. They propose a targeted survey that contrasts with the aforementioned surveys and emphasises the applicability in network and BC connectivity. They discuss the innovative ideas that resulted from bringing together in the context of BC handling the safety problems. In order to have a strong linear aggregating functional in the identification, Yazdinejad et al. [22] utilised Fuzzy DL and applied the fuzzy Choquet summation. They optimise the attack identification failure capability of ANFIS using metaheuristic techniques. To address identifying fraud and effectiveness at the distributed ledger layer, we additionally authenticate contracts using Fc. According to Rahman et al., [23], a cloud computing platform for the IIoT should combine BC and SDN. The "DistB-SDCloud" architecture is presented in this paper as a means of bolstering cloud security for IIoT programs. A new framework called MiTFed is presented by Abou El Houda et al. [24] that enables various software defined networks (SDN) subdomains (i.e., contributors) to cooperatively develop an international detection of intrusion model while disclosing their private datasets. In a blockchain-enabled IoT system, Kumar et al.'s [25] innovative global intrusion detection system (IDS) uses fog computing technology to identify DDoS attempts against mining

pools. Training Random Forest (RF) as well as an improved gradients tree boosting system (XGBoost) on dispersed foggy consumers allows for the evaluation of effectiveness.

The volume of operations expanded quickly as technology from BC was adopted. The amount of activities that can be incorporated into a block is constrained by the amount of users permitted on the block. The wait time for adding a transaction to the BC rises with a smaller block size. Costs increase because more people need to be employed to deal with the resulting increase in activity. Segwit, increasing the size of blocks, Sharding, Proof-of-Stake, off-chain state routes, and Triton are just some of the methods that have been proposed as answers to the sustainability problem. For a thorough answer to be proposed, an extensive amount of investigation is still required.

III. SYSTEM MODEL

In this study, we emphasise the importance of network infrastructure security. The physical component of this suggested technique is made up of smart network users (such as IoT gadgets), the layer closest to the edge is made up of edge consumers, and the online levels are made up of centralised storage. The structure of the suggested Hyb_chain_TPM system is shown in the first diagram. In this article, we advocated the use of composite chains, which unite blockchain technology and the TPM ecosystem to increase safety while easing the demand on the network's computational resources. Superior privacy and security are offered using blockchain-based verification as well as access control.

- Physical layer: This foundational layer of the Internet of Things network is in charge of collecting data from every those who use the IoT for data transfer and safely conserving that data on cloud servers via different sensors. Smartphones, notebooks, PCs, and other Internet of Things (IoT) gadgets can be accessed anywhere.
- Trusted Authority (TA): Blockchain deploys a Trusted Authorities on the physical layer in order to give consumers of IoT legitimacy through obtaining their login information and supplying them their encryption keys.

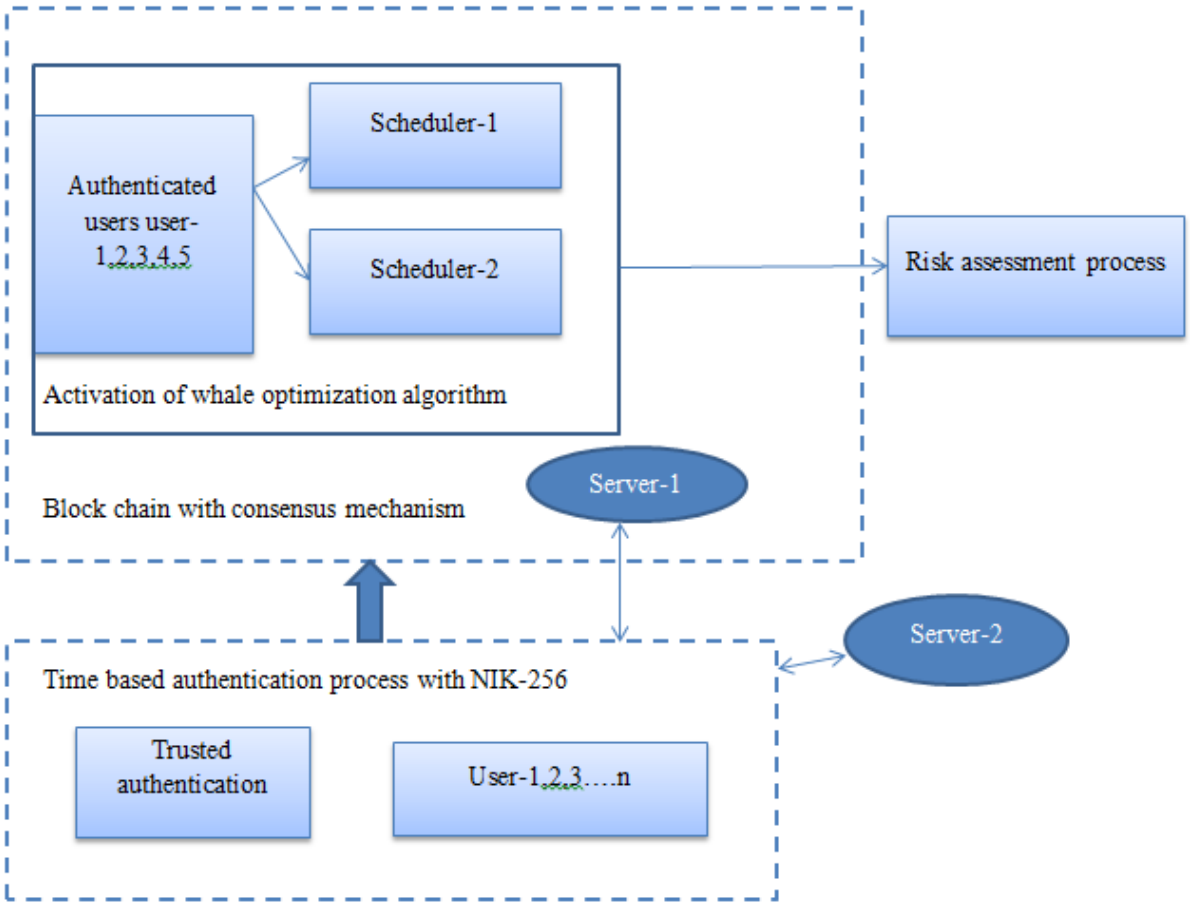

Figure-1 system architecture for network security

- Edge Layer: It is made up of a number of peripheral customers that are in charge of gathering data from the network. Additionally, the outer layer implements bi-level IDS to increase the safety and confidentiality of users of the Internet of Things.
- Cloud Layer: In order to enhance the safety of networks and lessen computing load, the cloud's barrier is made out of blockchain technology. Additionally, it is in charge of implementing measures to improve the safety of networks.
- Hybrid Blockchain: This type of blockchain combines blockchain technology alongside the Trusted Platform Module (TPM), that employs a network of hierarchies to reduce computational load and enable safe event archiving.

Authentication using NIK-256

To guarantee authenticity, we first execute networking user $US(n)$ authentication. To do so, the $US(n)$ needs to sign up with the trustworthy authority (tr_{au}) who sends the information into the blockchain to increase security, along with their user name use_{name} ,user ID us_{id}, device ID dev_{id}, PUF puf, role R, password $pass$, and mail ID m_{id}. Following registration, the trust authority (TA) shows the user's registered time in hour (hr), minute (min) and seconds (sec), and depending on the user's credentials—including their password pass—produces the security key. The following is a definition of the procedure associated with register and verification.

Step 1: By giving the passwords listed above, that can been constructed as follows: $\leftarrow Reg\ \{(use_{name}), (us_{id}), (dev_{id}), (puf), (R), (pass), (m_{id}), (tr_{au})\ \}$, the $US(n)$is first registered with the Trust Authority. When the aforementioned variables signify US(n)'s networking membership

Step 2: The Trustee Authorities showed the user enrolled a period of time that is utilised during login by the user, as soon as $US(n)$ was enrolled.

$$TA \leftarrow dis\ \{(hr), (min), (sec)\} \qquad (1)$$

Step 3: The TA creates the 256-bit hidden code for verification of the enrolled user whenever $US(n$ registers, as shown by the expression , $TA \leftarrow SK256[(pass), (hr), (min), (sec))]$ Following authorization, the user's username and password and user registered timestamp are stored on the distributed ledger in hash layout, resulting in greater privacy because it can't be altered by attackers. Researchers put forth the NiK-256 scrambling method, that's immune to all types of asymmetric assaults, especially classical colliding assaults for these reasons. The Miyaguchi-Preneel Structures is used in the cryptographic hash function, which is designed for hashing result lengths of 256 bits. X is saved as an array of 16 32-bit items. The SK256 hashing algorithm is composed of 256-bit blocks, with the final block's padding being equal parts zero and 256. If the function operates in keyless mode, the value of S is initialised to 0 at the start of algorithm execution. If key mode is employed, the value of S is initialised to a key value. When the first block of the message being processed, M's value is initialised. Both A and B corresponding to 256 bits are inputted into the compression algorithm, which then produces an integer of 256 bits. Preceding that, 32 cycles of computation conclude with the input being subjected to the subsequent formulas:

- The data being input is given an array with A and B's most recent entries.
  The conversion for A_i is carried out in accordance with the traditional storage equation (the component indices are computed as modulus 16):
  $A_i = (A_i \gg 1) modulo (B_i) modulo \left(A_{i+6}^{B_{i+3}}\right)$ (2)
- The arrays then twisted with the 0 component acting as the penultimate item and the *i*-th item becoming the $(i-1)$-th item.
- The conversion for A_i having index $2 \le i \le 16$is carried through using the following calculation:
  $A_i = (A_i \gg 1) + modulo B_i\ modulo (A_{i+6}^{B_{i-3}})$ (3)
- With every A_i and $B_i$change, a procedure is followed.
  $$\begin{cases} A_i = A_i \bmod 2^{32} \\ B_i = \left(B_i + A_i \times A_{(i+r^3) mod\ 16}\right) mod\ 2^{32} \end{cases} \qquad (4)$$

wherein r is the session amount that is currently in play (0 for the initial round, 31 for the final session). While the researchers of this study created a technique for hashing with an encrypted length of 256, a hashing method with a bigger session value might be created using the same methodology. By lengthening the input arrays A and B, for instance, a function called hash that generates 1024-bit result is possible made from Nik-256 (in this instance, the two sets are going to include 32 entries rather than 16). To do this, the message being entered ought to be split into 1024-byte blocks, and some modifications to the compressing function's equations might be required. It's essential to point out that the writers make zero assertions about the initial algorithm's cryptography features being preserved in this revision. The user ought to keep in mind the date and hour presented following registration since they will be entering it together with their identification number, password, and other login details each time they log in. When an individual chooses the Forgot Your Password option, the trusted authorities is going to send an authorization code to the user's registration email address, allowing them to read their login information and recorded time, however is additionally only possible upon three attempts. The value of T is determined as follows:

$$T(r,s) = -\sum_{n\in X} r(n) logs(n) \quad (5)$$

Whenever the user's criterion ranging n is restricted to three criterion intervals, and , r and s are discontinuous distributions of likelihood.

$$K = \begin{cases} 0\ if\ 0.3 \geq n\ mail\ generated \\ 1\ if\ 0.3 < n\ \ user\ blocked \end{cases} \quad (6)$$

The system's computational difficulty and adverse activity are decreased as a result of the greater safety level and elimination of unauthorised users provided by this identification. Additionally, privacy is improved by storing the (SK256) in hashed notation at a hybrid authorization network. The Trusted Platform Module (TPM) and blockchain are combined in the hybrid chain. Utilising a network of levels reduces on-chain latencies and CPU usage by carrying out the bulk of the laborious tasks off-chain. By allowing all participants to contribute their information via a safe communication protocol, the combined chain has a benefit. Additionally, the combined chain lengthens the amount of reserved memory, allowing the blockchain software to run in TPM, improving the preservation of events privately and providing verification of the entirety of key-value coding memory which is located apart from TPM. The informational layer in a blockchain include the chain framework, data blocks, hashing operation, and electronic signature in addition to the storage of information and security mechanisms. The Practical Byzantine Fault Tolerance (PBFT) consensual technique is used to verify the performance result in the communications mechanism that makes up the confirmation layer. The estimating level is used for virtual machine (VM) & key administration, events confirmation and intelligent contract implementation. Additionally, a high-performing intelligent contract that protects secrecy is used to manage access. The setting up of blockchain technology, contract technology, and analytics at the software level is customizable.

Whale optimization algorithm based scheduling

Upon authenticating successfully, a rule is developed depending on the individual's position and characteristic. The accessibility control management in a smart contract gathers the consumer's demand, which is made up of a variety of different service demands, once the client submits an inquiry to the ledger. Therefore, in order to minimise delay and awaiting time and maximise the usage of user assets, consumer inquiries must be scheduled. The processes necessary for it, which we call Whale Optimisation (WOA), are shown as follows. The whale (network server) searches the hunting prey (user) to accomplish customer scheduler.

- Prey encircling: The whale algorithms begins this stage by using the initial greatest search agent. The vantage point of the prey, and a site very nearby it, is assumed to be where the most effective currently available options are. As a result, the remaining agencies upgrade the most accurate search engine of their location. An additional sentence serves for conveying the following:

$$D' = |C'.X'(t) - X'(t)| \quad (7)$$

$$X*'(t+1) = X*'(t) - A'.D' \quad (8)$$

wherein $A'$and C' are correlation matrices and t is the present phase. The most effective approach so far is represented by the position matrix $X*'$is the destination matrix. If a better answer emerges, the $X*$ ought to be progressively adjusted. The following are the calculations for the variables A' and C':

$$A' = 2.a'.r' - a' \quad (9)$$

$$C' = 2.r' \quad (10)$$

wherein r is a vector with values in the range [0, 1] and a' is gradually lowered through 2 to 0 throughout the total amount of repetitions. By simulating surrounding the prey, this modelling enables any participant to update its

position in the vicinity of the current optimal answer. Movement in hypercubes as will be helped by the agents around the most successful the solution, and it is possible to seek farther in the space of searching for n levels.

- Exploit phase: This stage is also known as bubblenet assaulting, and it employs a total of two strategies:
- Encircling process that is shrinking: in this phase, the amount of a' in equation (9) is reduced, which means that as a result, the range of fluctuations of A' is likewise reduced by a'. This suggests that a' is inserted at randomness into$[-a', a'$, wherein a decreases from 2 to 0 during the course of the optimisation process. Anything within the searching agent's previous position and the most suitable present destination can be judged to be the unpredictability of A' in [-1, 1], the research the agents new spot.
- Spiral update location: a spiral path is established connecting the positions of the whale and its prey to mimic the helix-shaped motions of whales with humpbacks. It may be stated in this manner:

$$X'(t+1) = \begin{cases} X*'(t) = A'.D' & if\ p < 0.5 \\ D'.e^{bl}.cos\ (2\pi l) + X*'(t) & if\ p \geq 0.5 \end{cases} \quad (11)$$

where p is a random number in [0, 1].

- Phase of exploration: To force the search agent to veer away from the reference whale, the A' is set arbitrarily between [-1,1]. As a result, $-A'$ must either be bigger than 1 or lower than -1. Additionally, the WOA performs a worldwide search by selecting an agent at random to update the position of in this case. The formula in mathematics for this exploration technique is as follows:

$$D' = |C'.X'rand - X'| \quad (12)$$

$$X'(t+1) = X'rand - A'.D' \quad (13)$$

wherein $X'rand$ is a randomly selected whale from the present population, while its location is randomised. In our method, control of access is carried out following user schedule. The right to access control is given by a smart contract stored on the blockchain, which is created by numerous agents to oversee data and resource sharing between network participants. Every user is represented by the input matrix $user = user_1, user_2, \ldots$ and the weight vector (which relies on user behaviour) $=G_1, G_2$. The trust value is produced as a result of requiring the weights $G_{i(i=[1,2\ldots h])}$ to inputs $user_{j\,(j=[1,2\ldots q])}$

$$trust = \sum_{i=1}^{q} G_i user_i \quad (14)$$

The degree of trust is presumed to be either low (misbehaved) or high (not misbehaved) whenever the degree of confidence has been calculated. Additionally, their authorization levels are assessed depending on their position, and applications are approved or rejected in accordance with their authorization grade & the degree of confidence.

Risk assessment

To keep Byzantine consumers from turning into accountancy consumers, it is vital to assess and upgrade the network's existing Byzantine consumers. By integrating the ideas of risk value and dependability, RAC characterises a user's dependability. In comparison with other consumers in the system, the risk value represents the likelihood that a user may experience Byzantine occurrences within a given term. The likelihood that a Byzantine event will take place at the accounting firm's user throughout their tenure is represented by consistency. The Risk-User Screening Process developed in this study employs system calls patterns as the basis of data analysis in order to enhance detection of harmful behaviour. The application of systemcalls for detection of intrusions was initially suggested by Forest and presumes that programme functioning impacts the operating system and that every exception leave tracks of the system calls carried out by the operating system's kernel. A system call reflects the first interaction among the programme and the system that hosts it, and there is no information abstraction in this process. Therefore, the main benefit of our technology is its ability to detect malicious behaviour easily and swiftly identify rogue users with unusual systemcall cycles. To set the tone for the presentation of the Risk-User Evaluation Mechanism, we make a few hypotheses regarding the permissioned blockchain.

- The system consistently has more honest users than Byzantine consumers, according to assumption 1.
- Assumption 2: Since assailants can employ a wide range of attack strategies or resources to interfere with consensus either singly or collectively, it is impossible to foresee the hostile behaviour of Byzantine users.

- Assumption 3: Since all users share the same operating system and strive to come to a consensus in accordance with their obligations, honest users behave consistently in a comparable way. As a result, their systemcall sequence is likewise consistent.

Based on the aforementioned premises, this subsection will employ a short sequence-based method to simulate the subsequent series of system call sequence for honest users, and anyone who considerably departs from it will be regarded as malicious. Initially a representation is created based on every user's order of system calls. A $num * k$ matrix, let's say N_r, is used for representing the order that comprises system calls for all users. $N_r$rows each reflect the whole series of system calls for a particular user in the preceding term. As a result, the matrix is N_r, which is made up of the condensed list of system calls made by each user connected to the network.

To emphasise the notable differences in behaviour between truthful and malicious customers, it also helps to combine the order of system calls with the rate of recurrence. $S_{(i,j)}$ is the particular number of a series of system calls; it is obtained from Calculation (15); f_s indicates the number of times with which$S_{(i,j)}$ appears in the array N_r.

$$S_{(i,j)} = T(i,j), 1 \le i \le num\ and\ 1 \le j \le k \quad (15)$$

$$f_s = \frac{S_{(i,j)}}{\sum_m S_{(m,j)}}, 1 \le m \le num\ and\ 1 \le j \le k \quad (16)$$

$$N_f(i,j) = S_{(i,j)} * f_s, 1 \le i \le num\ and\ 1 \le j \le k \quad (17)$$

Secondly, according to Assumption 3, regular consumers act in the consensus procedure fairly identically. It additionally needed to devote consideration to some system calls patterns with a low usage rate but enormous significance as the critical data, like a a malicious attack, tends to be concealed in them. This will additionally represent the difference among the brief a sequence matrix consisting of frequently utilised structure call patterns and the shorter pattern matrix consisting of fewer commonly utilised system call sequences. As a result, the inverse document frequency procedure is also necessary, and Expression (18) provides more information.

$$\boldsymbol{idf_{(i,j)} = log \frac{|num|}{\left|\{i: S_{(i,j)} \in N_i\} + 1\right|}, 1 \le i \le num\ and\ 1 \le j \le k}$$

Equations (18) uses the symbols $|\boldsymbol{num}|$and ; $\left|\{\boldsymbol{i}: S_{(i,j)} \in N_i\} + 1\right|$to represent the total number of users and the percentage of customers having the specific system's call sequence $S_{(i,j)}$ respectively. Following process frequency and inverted text rate to acquire a matrix, the initial matrixN_r is ultimately obtained as given in Equations (19).

$$\boldsymbol{N_f(i,j)} = S_{(i,j)} * f_s(i,j) * idf_{(i,j)}, 1 \le i \le num\ and\ 1 \le j \le k \quad (19)$$

An autonomous outlier detection technique can be used to analyse the risk value in Assumption 1 and Assumption 2. In this study, we employ the isolated forest algorithm to identify rogue users. The separation tree algorithms ranks each user according to their anomalous rating. Every of the numerous binary trees that make up a single forest is referred to as an isolation tree. An isolation tree is created using a completely arbitrary approach. Let's say there are num users in the network. The approach of calculating the typical path length of an isolated tree's leaf users is known as the failed search of a binary tree because of the identical its structural features are, as demonstrated in Formula (20).

$$\boldsymbol{c(n) = 2H(n-1) - 2\left(\frac{n-1}{n}\right)} \quad \textbf{(20)}$$

$H(x) = \ln(x) + 0{,}566$ is the Euler-Mascheroni constant in this case. Since $\boldsymbol{c(n)}$ represents the mean of the path's length, it can be utilised to normalise the path length. Equations (21) may be used to determine the anomalous score of a node x, wherein $h(x)$ is the duration of the path of the node x in the isolation tree.

$$\boldsymbol{s(x,n) = 2^{-E(h(x)/c(n)}}$$

By reviewing the order of system calls made by every node in the preceding term, the risk-node evaluation process may determine the risk values for every node. Whenever a node's risk level is much higher than that of other truthful nodes, it is going to be classified as a Byzantium site.

IV. PERFORMANCE ANALYSIS

The University of New Brunswick in Canada houses the NSL-KDD dataset. It's an updated and error-free version of the KDD cup' 99 dataset. As of the KDD cup'99 dataset, neither the training nor the testing datasets are too large, and so, sampling is not required in order to conduct experiments. There are a total of 125,973 training records and 22,544 testing records in the NSL-KDD dataset. There are 41 attributes in the training and testing datasets that describe network features, and the 42nd attribute has five class labels that describe either a typical network or one of four types of network attacks. DoS attacks, remote-to-local attacks, user-to-root attacks, and probing attacks are the four types of network attacks. A 2.66 GHz Intel core i5 CPU with 4 GB of RAM is used for the classification technique implementation.

Parameters like accuracy, precision, recall, f1-score, and kappa score are used to analyze the data from the experiments. These parameters are compared with Fuzzy DL [22], DistB-SDCloud[23], MiTFed[24] with proposed Hyb_chain_TPM.

Accuracy: This metric is a representation of the proposed deep learning model's overall prediction ability. The accuracy of classifier models is evaluated by their true positive (TP) and true negative (TN) rates. The proportion of incorrect predictions made by models is measured in terms of false positives (FP) and false negatives (FN).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision: The model's ability to correctly categorize attacks is evaluated. The accuracy of a classifier is measured by how often it correctly identifies an attack situation as positive. It's also referred to as the proportion of correct diagnoses.

$$Precision\ (P) = \frac{TP}{TP + FP}$$

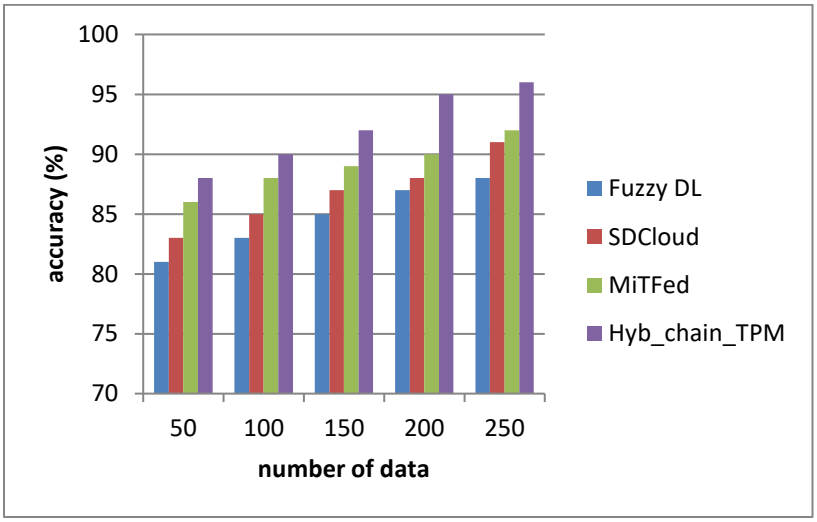

Figure 2: Comparison of accuracy

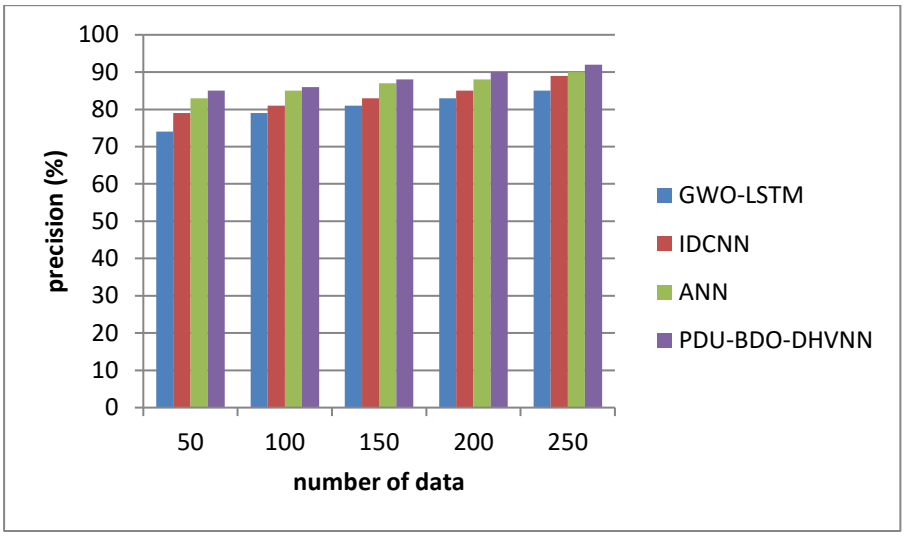

Figure 3: Comparison of precision

In Figure 2, the X-axis depicts the total number of data points and the Y-axis depicts the corresponding percentages of accuracy for both the current and proposed methodologies. When compared, existing method achieves 84.8%,86.8% and 89% while the proposed method achieves 91.6 which is 7.2% better than Fuzzy DL,5.2% better than SDCloud ,and 2.6% better than MiTFed. The figure 3 shows the comparison of precision When compared, existing method achieves 80.4%,83.4% and 86.6% while the proposed method achieves 88.2%which is 8.2% better than Fuzzy DL,5% better than SDCloud and 2.4% better than MiTFed..

Recall: When an attack is not present, the classifier has a certain chance of making a negative prediction. It's often referred to as the "true negative" (TN) rate.

$$Recall(R) = \frac{TP}{TP + FN}$$

F1- Score: It is used to evaluate how well a forecast was made. It is understood to be a harmonic mean (weighted average) of the recall and accuracy. The best possible score is 1, while the worst possible score is 0. The TNs are ignored by F-measures.

$$F1 - Score = \frac{2 * P * R}{P + R}$$

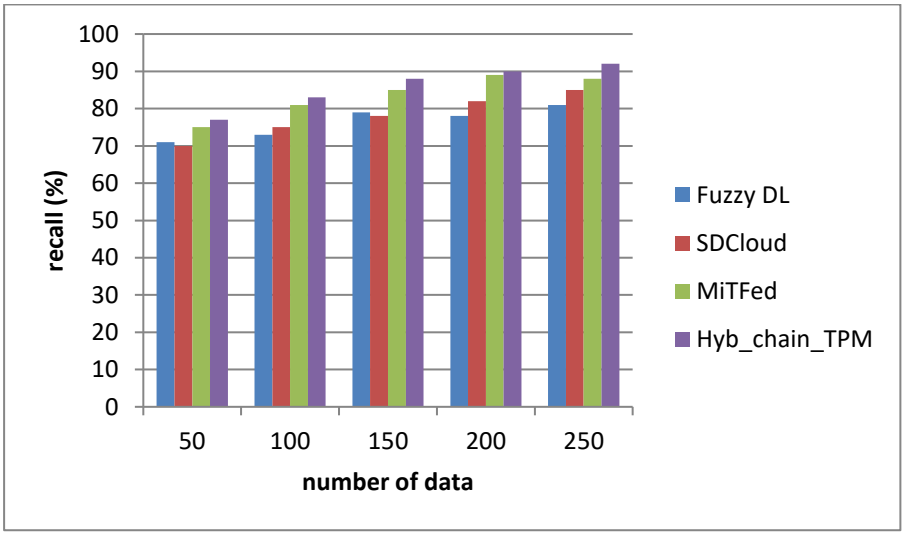

Figure 4: Comparison of recall

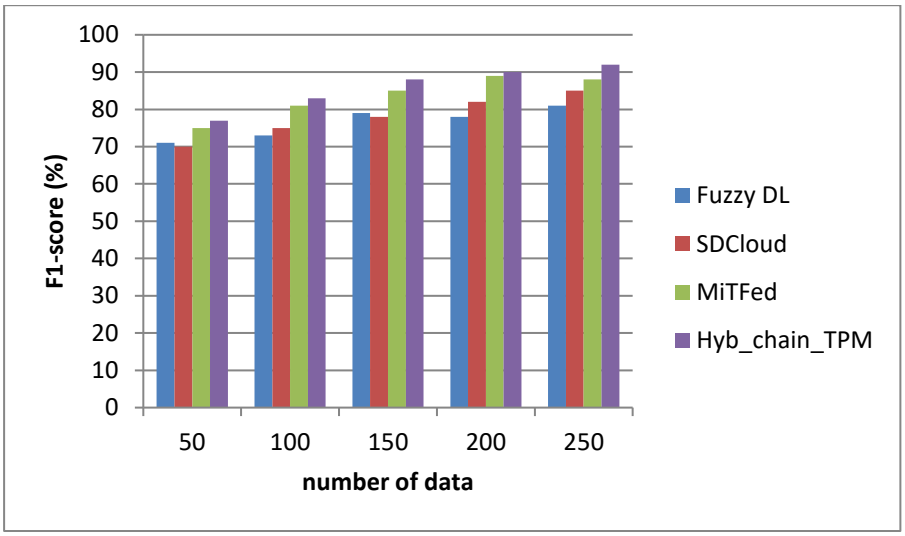

Figure 5: Comparison of F1- Score

Figure 4 compares the existing recall with the suggested recall, where the X-axis depicts the total number of data points and the Y-axis depicts the recall values as a percentage. The suggested method outperforms the existing methods by 10.4% compared to Fuzzy DL, 8% compared to SDCloud, and 3.6% compared to MiTFed, while the existing methods only reach 76.4%, 78%, and 83.6%, respectively. F1-Score comparisons are shown in Figure 5. The suggested technique obtains 82%, which is 18.4% better than Fuzzy DL, 9% better than SDCloud, and 4.2% better than MiTFed, while the existing methods only score 63.4%, 73.2%, and 78.2%, respectively.

The **kappa statistic** is commonly used to evaluate inter-rater consistency. Rater dependability is crucial because it indicates how well the variables being measured in the study were captured by the data collected.

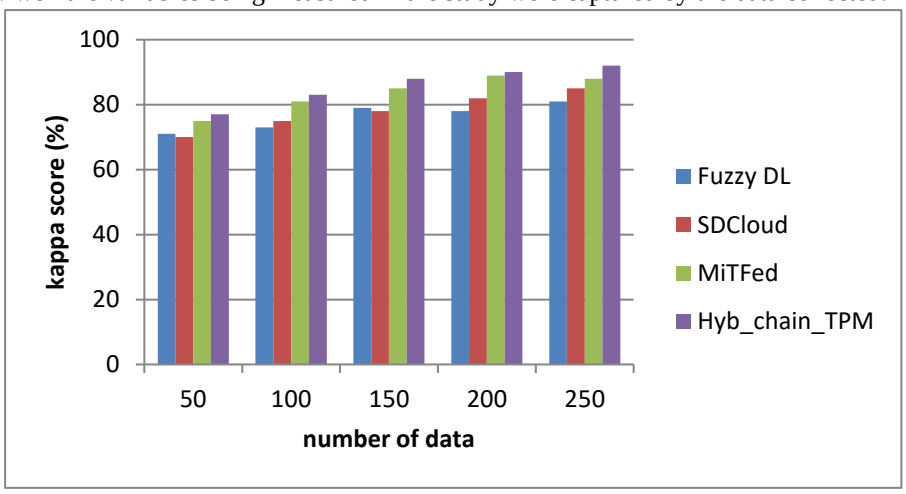

Figure 6: Comparison of Kappa score

In Figure 6, the X-axis represents the total number of data points, while the Y-axis represents the corresponding Kappa score values in percentage form. When compared, existing method achieves 57.8%,62% and 67% while the proposed method achieves 71.4%which is 14.4% better than Fuzzy DL,9% better than SDCloud and 4.4% better than MiTFed.

Table 8: overall comparison of existing and proposed method

Methods	Accuracy(%)	Precision(%)	Recall(%)	F1-score(%)	Kappa score(%)
Fuzzy DL	84.8	80.4	76.4	63.4	57.8
SDCloud	86.8	83.4	78	73.2	62
MiTFed	89	86.6	83.6	78.2	67
Hyb_chain_TPM	91.6	88.2	86	82	71.4

V. CONCLUSION

Insufficient privacy and security on the internet are the main problems. For effective intrusion detection, this research recommends the Hyb_chain_TPM architecture. Using the NIK-256 hashing algorithm and a 256-bit security key, we may perform initial time-based authentication. Hybrid chains (Blockchain and TPM) save the password and registered time, enhancing the scalability of blockchains and the privacy of stored data. Following the scheduling of the verified users to decrease complexity, access control is offered and is firmly based on user permission level and trust level. Additionally, the risk assessment is carried out to determine the attack impact level, and an attack graph is constructed to determine the assault path. Lastly, to reduce packet loss, the network's infrastructure is updated and rebuilt. Accuracy, precision, recall, f1-score, and kappa score are all improved by the suggested Hyb_chain_TPM. Future research will be focused on incorporating pre-processing and a method for extracting features from additional databases.

Acknowledgement

Technology Project of Yunnan Power Grid Co., Ltd "WEB Application Protection Based on RBI Remote Browser Isolation Technology" (No. 059300KK52220011)

References

1. Cyber Terror Response (2016). Center,“Coping with smishing”, 2013, http://www.netan.go.kr/. The National Police Agency. 2. Kang, J. Y., Yoon, J., & Kim, Y. (2013). Phishing/pharming examples and countermeasure analysis. The Korean Institute of Information Scientists and Engineers, 12(2), 171–180.
2. S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf
3. D. Wilson and G. Ateniese, “From pretty good to great: Enhancing PGP using bitcoin and the blockchain,” in Network and System Security. Cham, Switzerland: Springer Int., 2015, pp. 368–375.
4. X. Huang, C. Xu, P. Wang, and H. Liu, “LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem,” IEEE Access, vol. 6, pp. 13565–13574, 2018
5. J. Wang et al., “A blockchain based privacy-preserving incentive mechanism in crowdsensing applications,” IEEE Access, vol. 6, pp. 17545–17556, 2018.
6. F. Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology,” in Proc. IEEE 13th Int. Conf. Service Syst. Service Manag. (ICSSSM), Jun. 2016, pp. 1–6.
7. Z. Li et al., “Consortium blockchain for secure energy trading in industrial Internet of Things,” IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
8. T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain technology innovations,” in Proc. IEEE Technol. Eng. Manag. Conf. (TEMSCON), Jun. 2017, pp. 137–141.
9. J. Gao et al., “GridMonitoring: Secured sovereign blockchain based monitoring on smart grid,” IEEE Access, vol. 6, pp. 9917–9925, 2018.
10. G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, “Distributed blockchain-based data protection framework for modern power systems against cyber attacks,” IEEE Trans. Smart Grid, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/8326530
11. N. Z. Aitzhan and D. Svetinovic, “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,” IEEE Trans. Depend. Secure Comput., vol. 15, no. 5, pp. 840–852, Oct. 2018
12. T. M. Fernández-Caramés and P. Fraga-Lamas, “A review on the use of blockchain for the Internet of Things,” IEEE Access, vol. 6, pp. 32979–33001, 2018.
13. Crypto-Currency Market Capitalizations. Accessed: Jun. 15, 2018. [Online]. Available: https://coinmarketcap.comhttps:// coinmarketcap.com
14. Blockchain Technology Report to the US Federal Advisory Committee on Insurance. Accessed: Jun. 15, 2018. [Online]. Available: https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf
15. L. Bahack. (Dec. 2013). Theoretical BitCoin Attacks With Less Than Half of the Computational Power. [Online]. Available: https://arxiv.org/pdf/1312.7013.pdf
16. M. Ali, J. Nelson, R. Shea, and M. J. Freedman, “Blockstack: A global naming and storage system secured by blockchains,” in Proc. Annu. Tech. Conf. (USENIX ATC), Jun. 2016, pp. 181–194

17. Sun, J.; Yan, J.; Zhang, K.Z.K. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financ. Innov.* **2016**, *2*, 6.
18. New generalization of reverse Minkowski's inequality for fractional integral. (2021). Advances in the Theory of Nonlinear Analysis and Its Application, 5(1), 72-81. https://atnaea.org/index.php/journal/article/view/183
19. Samaniego, M.; Deters, R. Blockchain as a Service for IoT. In Proceedings of the 9th IEEE International Conference on Internet of Things, Chengdu, China, 15–18 December 2016; pp. 433–436.
20. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190.
21. Dhabliya, P. D. . (2020). Multispectral Image Analysis Using Feature Extraction with Classification for Agricultural Crop Cultivation Based On 4G Wireless IOT Networks. Research Journal of Computer Systems and Engineering, 1(1), 01–05. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/10
22. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Comput. Netw.* **2018**, *141*, 199–221.
23. Meshram, A. A. ., & Abhimanyu Dutonde, A. G. . (2022). A Review of Skin Melanoma Detection Based on Machine Learning. International Journal of New Practices in Management and Engineering, 11(01), 15–23. https://doi.org/10.17762/ijnpme.v11i01.145
24. Jesus, E.F.; Chicarino, V.R.; de Albuquerque, C.V.; Rocha, A.A.D.A. A survey of how to use blockchain to secure internet of things and the stalker attack. *Secur. Commun. Netw.* **2018**, *2018*, 1–27.
25. Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023). Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks. *Computers in Industry*, *144*, 103801.
26. Rahman, A., Islam, M. J., Band, S. S., Muhammad, G., Hasan, K., & Tiwari, P. (2023). Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. *Digital Communications and Networks*, *9*(2), 411-421.
27. Abou El Houda, Z., Hafid, A. S., & Khoukhi, L. (2023). Mitfed: A privacy preserving collaborative network attack mitigation framework based on federated learning using sdn and blockchain. *IEEE Transactions on Network Science and Engineering*.
28. Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *Journal of Parallel and Distributed Computing*, *164*, 55-68.