Journal of Theoretical and Applied Information Technology

15th September 2023. Vol.101. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SABA: SECURE APPROACH BASED ON ANOMALY AND SIGNATURE-BASED DETECTION MECHANISM FOR DETECTING ABNORMAL ACTIVITIES IN BLOCKCHAIN NETWORK

***HALA A. ALBAROODI[1], MOHAMMED ANBAR[2]**

[1]Associated prof. at Gifted guardianship committee, in Ministry of Education, Baghdad/Iraq.
[2] National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), 11800 Gelugor, Penang, Malaysia

E-mail: [1]hala.albaroodi5@gmail.com, [1]hala.albaroodi@iraqiggc.edu.iq, [2]anbar@usm.my

ABSTRACT

In recent years, blockchain technology has undoubtedly experienced broad use. Apart from its initial usage in cryptocurrency, it is now employed in healthcare, real estate, smart contacts, and other fields. However, many blockchain security vulnerabilities have been caused by the incorrect implementation of the technology. As a result, the Blockchain may become insecure, allowing attackers to carry out a variety of Blockchain-based attacks. Suspicious behaviour is expected may exist because of the presence of blockchain attacks. Therefore, detecting suspicious behaviour may detect different types of Blockchain-based attacks. Thus, this paper aims to propose the Signature and Anomaly approach (SABA) to detect suspicious behaviour in a Blockchain environment based on Indicators of Compromise (IOCs). SABA consists of components as follows: the first layer is the Blockchain application (threats detector; and APIs), the second layer is the protocol layer (decentralized protocol), and the third layer is the data layer or can call it to overlay network (SBAB fork module; SBAB transactions filter; and SBAB threat database). The proposed approach is detailed in-depth and proven by experimental and analytical findings showing the quality and practicality of Blockchain Signature Based and Anomaly Based detection techniques.

Keywords: *Blockchain; Security; Authentication; Cloud Computing; Indicators of Compromise; Intrusion Detection Systems; Signature Detection Based; Anomaly Detection Based.*

1. INTRODUCTION

Cloud Blockchain technology enables untrusted peers inside open (i.e., permission-less) communities to agree on the status of a shared database without requiring access to trustworthy third parties [1]. Cloud computing has permeated all aspects of information technology [2] [3]. When a new Blockchain is formed, all participants can preserve a ledger, including all transaction data, and update their ledgers to maintain integrity [4].

Encryption technology has enabled all members to participate. Furthermore, Blockchain may be used outside the Internet of Things (IoT) ecosystem; new uses are predicted. The Blockchain includes broker-free properties for Peer to Peer (P2P) transactions, eliminating unnecessary costs through p2p transactions without third-party permission [5]. Because many individuals own the transaction information, hacking is difficult, security costs are reduced, transactions are automatically validated and recorded by public involvement, and promptness is ensured.

Additionally, open-source apps can record transactions, allowing the system to be deployed, linked, and expanded. The system could be open to the public without charge to reduce the cost of regulation [6]. The Blockchain stores data in a structured list that resembles a distributed database. It is difficult to tamper with because it is recorded and verified by users across the network. Each

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

block in the list has a header and a body, with the header containing information on the nonce and hash values from the current and prior blocks. Seebacher and Schüritz (2017) explain that an indexing mechanism retrieves block information from the database [7].

The hash function ensures the integrity of transaction data during a transaction by verifying that the block data, including the transaction information, has not been changed and determining the nonce value to generate a new block. The integrity of the transaction information may be checked by encrypting the hash value of the transaction data with a public key.

Furthermore, utilizing the root hash value, which collects the hash value of each transaction information, makes it simple to determine whether the transaction data were updated because the root hash value changes when the value is, as shown in figure 1, changes occurred during the procedure [8][9].

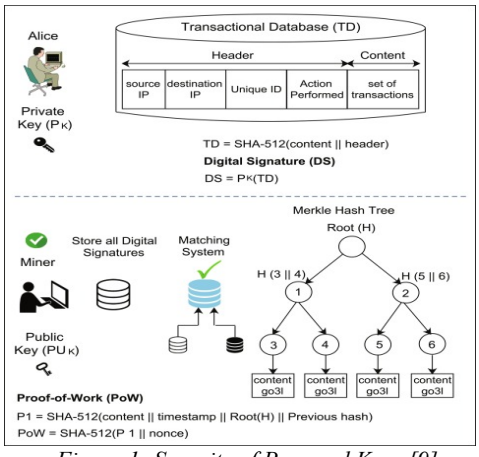

Figure 1: Security of Personal Keys [9].

The transaction is hugely vulnerable to malware infection since it is frequently transacted on commonly used devices such as peers' PCs or cell phones. Malware that infiltrates multiple channels such as e-mail, USB, or programs with inadequate security must be discovered and addressed since it can infect a peer's device.

The rest of Section 2. Discusses related studies such as the fundamental notion of the Cloud Blockchain environment, Cloud Blockchain security concerns, and secure transactions, Section 3. Methodology, Section 4. Discusses the SBAB's intricacy and Section 5 is the conclusion.

2. BACKGROUND

Due to the widespread usage and development of blockchain technology in industries like finance, politics, and healthcare, security events are frequent on the platform, posing serious risks to users' assets and data. To counter these dangers, numerous academics have focused on blockchain aberrant behaviour awareness [4].

To address the abovementioned threat, intrusion detection systems (IDS) have previously been created to increase the security of complex networks and systems by recording, monitoring, and analyzing peers' traffic or, more broadly, their behaviour [10].

These techniques often focus on log analysis and data correlation to construct attack models and mitigation measures. Existing IDS may be divided into two categories based on their approach: signature recognition and anomalous behaviour [11].

2.1 Signature-Based Intrusion Detection Systems (SIDS)

Signature intrusion detection systems (SIDS) employ pattern-matching approaches to identify known attacks, known as Knowledge-based Detection or Misuse Detection [12].

SIDS examines host logs for sequences of instructions or behaviours previously detected as malware. Matching algorithms are employed in SIDS to locate an initial incursion. In other words, an alarm signal is generated when an intrusion signature matches the signature of an initial incursion that already exists in the signature database. SIDS has also been referred to as Knowledge-Based Detection or Misuse Detection in the literature [13].

For previously known incursions, SIDS often provides good detection accuracy [14]. The basic concept is to create a database of intrusion signatures and then compare the current set of actions to the existing signatures, raising the alarm if a match is

detected. A rule like "if: antecedent -then: consequent" may result in "if (source IP address=destination IP address) then classify as an attack".

Traditional SIDS techniques analyze network packets and attempt to match them against a signature database. However, these approaches are incapable of detecting attacks that span many packets. Because current malware is cleverer, extracting signature information over numerous packets may be essential; it necessitates the IDS to recall the contents of previous packets. In general, there have been several ways of producing SIDS signatures, such as state machines [15], formal language string patterns, or semantic requirements [16].

Polymorphic malware variants and an increase in targeted attacks may further compromise the suitability of this old paradigm. Because no previous signature exists for any such attacks, the rising prevalence of zero-day attacks O'Brien, (2017) has rendered SIDS approaches progressively less effective [17].

2.2 An anomaly-based intrusion detection system (AIDS)

AIDS has piqued the curiosity of many academics owing to its ability to transcend the restriction of SIDS. In AIDS, a standard computer system behaviour model is constructed using machine learning, statistical, or knowledge-based approaches. Any significant difference between observed and predicted behaviour is considered an anomaly, which might be an incursion [1].

This category of approaches is based on the notion that harmful activity varies from ordinary user behaviour. Intrusions are anomalous user behaviours that differ from usual behaviours. The development of AIDS is divided into two stages: training and testing. The standard traffic profile is utilized in the training phase to build a model of normal behaviour. A fresh data set is used in the testing phase to determine the system's ability to generalize to previously unknown intrusions. AIDS may be classed into several groups according to the training approach, such as statistical, knowledge-based, and machine learning [2].

The key benefit of AIDS is the ability to identify zero-day attacks because it does not rely on a signature database to recognize aberrant user activity [3]. When the observed behaviour departs from the expected behaviour, AIDS sends a warning signal. AIDS also provides some advantages. For starters, they may detect internal harmful actions. An alarm is raised if an intruder begins making transactions in a stolen account that are identifiable in regular user activity. Second, because the system is built from unique profiles, it is complicated for a cybercriminal to detect regular user activity without triggering an alarm.

SIDS can only detect known intrusions, whereas AIDS can detect unknown intrusions. However, because anomalies may represent new normal behaviours rather than actual invasions, AIDS can result in a high false-positive rate.

The first-class influence databases match the signatures of well-known attacks. These databases are then utilized as a reference model to detect similar attacks in the future. As a result, this method cannot detect new attacks whose fingerprints are yet unknown.

Meanwhile, anomaly detection methods create models of typical behaviour and raise alarms when departures from such baselines occur. As a result, the purpose of an Anomaly Detection System (ADS) is to construct the typical behaviour model and then test it with new unknown behaviours to see how near they are to the reference model [4][21].

Furthermore, because all essential data is kept on the central server, traditional, centrally managed transactions are subject to data breaches when the management server is compromised [4]. Privacy protection safeguards the personal information of transaction participants, whereas residual information protects the safe removal of user data at the moment of transaction termination and program uninstallation [5].

Confidentiality is checked if the information is split to unauthorized peers, whereas integrity is checked if data utilized in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

transactions is updated or fabricated without sanction during transmission or storage. Anonymity ensures that the peer engaged in a transaction cannot be identified.

So far, ADS has shown its functionality, mainly when based on trustworthy third parties responsible for building reference models and notifying end-users or endpoints. The differences between signature-based detection and anomaly-based detection are shown in table 1.

Table 1: Comparisons of SIDS vs. AIDS

	Advantages	Disadvantages
SIDS	• Very effective in detecting intrusions with fewer false alarms (FA). • Identifies intruders quickly. • Excellent at detecting known attacks. • Simple layout	• SIDS is meant to identify attacks for known signatures and must be updated regularly. When an initial incursion is slightly modified to become a new version, the system cannot recognize this new variant of a comparable assault. • The zero-day attack was undetected. • Ineffective at identifying multi-step attacks. • Little knowledge of the attacks' insight
AIDS	•It has the potential to be utilized to identify future attacks. • It might be used to generate an intrusion signature.	•AIDS cannot handle encrypted packets; the attack might go unnoticed and pose a hazard. • A high number of false-positive alarms. • It is challenging to create a standard profile for a highly dynamic computer system. • Unclassified warnings • Initial training is required.

The security incidents instance does not offer availability since the service becomes unavailable due to malware infection. It does not provide residual information protection because it does not check the complete removal of the electronic wallet [6].

The upgraded Blockchain does not guarantee integrity or availability since the risk of double transactions remains. Furthermore, because it does not check the entire transaction, it does not ensure residual information protection. Because it encrypts the data with a public key and confirms the complete removal of the transaction, the safe Blockchain solution increases security by offering residual information protection [7].

3. RESEARCH PROBLEMS

Typically, security is a major concern in the realm of digital technology [8]. As cloud computing becomes more prevalent, this concern receives even greater attention, irrespective of the affordability and range of services offered by the cloud [9][10][11]. The heightened attention is primarily due to the potential misuse of data by cloud service providers and the need to ensure user identity [12][13]. Interestingly, Blockchain solutions have gained significant acceptance from the community, particularly for data storage and transmission. Blockchains promise improved user experiences, enhanced security, and overall better performance. However, despite the widespread adoption of Blockchain in the cloud computing community, it still lacks robust security measures and a solid data integrity mechanism [14][15][16]. This paper aims to highlight specific problems associated with current Blockchain transactions. The identified issues are as follows:

- The use of Blockchains introduces significant risks concerning authentication and authorization between the cloud provider and the cloud consumer.

- One of the vulnerabilities lies in the use of API tokens for username and password authentication, which are not adequately protected and are susceptible to hacking [17][18]. This exposes sensitive user data to potential breaches and unauthorized access.

- Another critical issue is the inability of the current mechanism to distinguish between real users and automated robots [19]. This lack of differentiation poses a serious security concern as it becomes challenging to prevent and mitigate potential malicious activities.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Furthermore, the centralization of resources between the cloud service provider and the cloud consumer lacks trust and transparency, leading to inadequate load balancing and resource allocation [20]. This imbalance may result in inefficient resource utilization and potential service disruption.

4. RESEARCH STEPS

This paper seeks to introduce a novel security approach called SBAB within the context of Blockchain cloud computing infrastructure. The main objective is to conduct a thorough examination of the security challenges that exist in this domain. By identifying these challenges, the research aims to pinpoint the gaps in the current state of Blockchain technology, which will subsequently be addressed and filled by the proposed SBAB approach.

To achieve this goal, we begin with an extensive study of the security issues prevalent in Blockchain cloud computing infrastructure. Through this in-depth analysis, they aim to gain insights into the vulnerabilities and shortcomings present in the existing systems. These findings serve as a foundation for defining the specific gaps that need to be addressed for enhancing the security and reliability of Blockchain in a cloud computing environment.

The proposed SBAB approach is designed to tackle and resolve the identified gaps effectively. By introducing new mechanisms, authentication processes, or anomaly-based techniques, SBAB aims to bolster the overall security posture of Blockchain within the cloud computing infrastructure. figure 2 depicts the research steps.

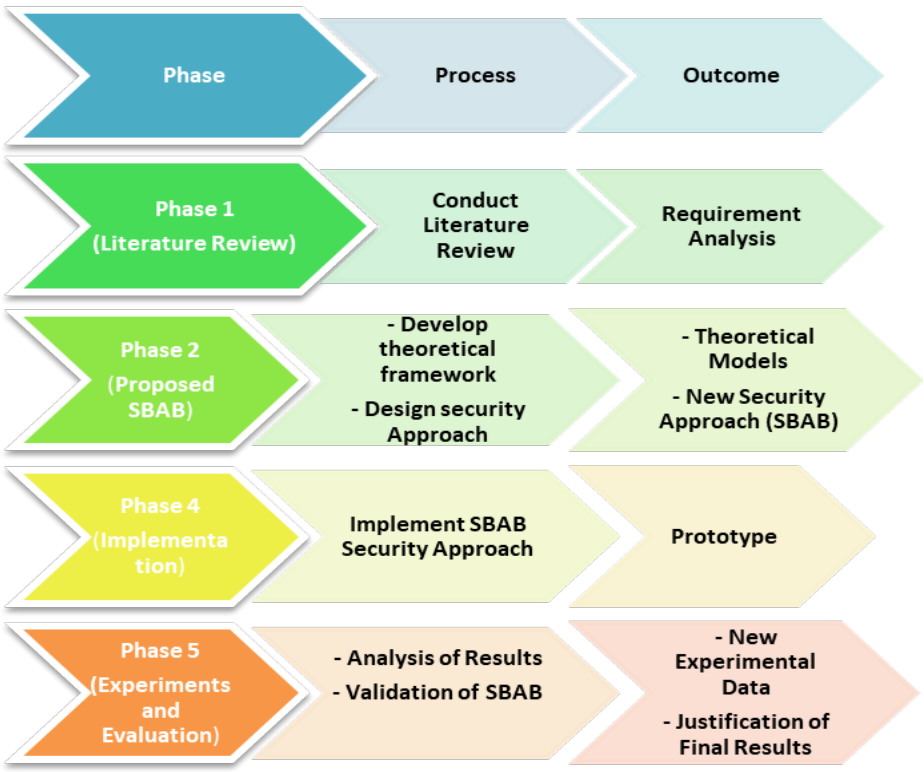

FIGURE 2: Research Steps.

5. METHODOLOGY

End-to-end encryption makes it possible to protect data both during storage and transmission [21]. Blockchains provide the security of both the transaction data and their ordering. The reliable peer-to-peer distribution of exact copies of the Blockchain across a cloud computing network provides a triple security layer [22]. Distributed data storage is far preferable to a central data storage architecture and provides a lower risk of a data breach.

Regarding data sources, there are two sorts of IOC technologies: Signature-based and Anomaly-based. SABA approach is the first solution to identify suspicious behaviour in a Blockchain context (Signature and Anomaly). The core concept of SABA approach underpinning Blockchain Signature and Anomaly detection is to provide a new decentralized approach based on Blockchain technology that uses the information gathered from previous threats detectors saved in the Blockchain application. Signature-based IDSs identify malicious packets in transit by comparing their signatures against a known or unknown anomalous behaviour database. Anomaly-based IDSs, on the other hand, can detect both previously unknown and newly discovered malicious behaviour and alert the SABA approach accordingly.

Therefore, we assumed that gathering information about prior attacks in the data layer may be feasible to blocklist them and prohibit them from inside peers that have not yet been attacked. In the following sections, we will first describe the logic that inspired SABA approach, present an example of its applicability, and then discuss the main stages of SBAB, as indicated in figure 3.

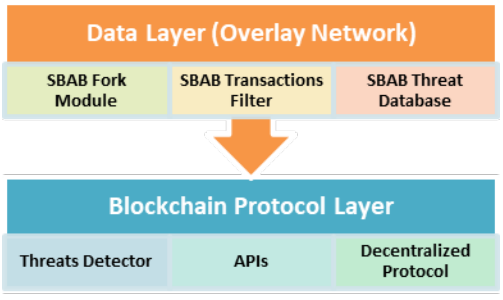

Figure 3: Main Stages of SBAB.

The reason for this strategy is that while attacks may occur once within a single device when replicated against additional devices over time, they frequently behave similarly. The feature extraction procedure, which turns the time series data, begins when the basic transaction patterns have been revealed. The activity profile for the anomaly-base-side is then generated using the anomalous detection approach. This SABA is utilized in the following transaction to determine if each transaction is normal or abnormal. The for-loop parameter of the number of transactions evaluated by the accurate anomaly detection SABA approach can be further optimized to the individual address. The SABA approach is depicted in figure 3 as a corresponding stage. The SABA approach, which incorporates the suggested approach for automatic digital signing of blockchain transactions, allows the transmission of transactions through a decentralized application, unlike before.

To initiate a transaction, the user fills out a form on the interface of a decentralized application, providing information about the transaction and the recipient address. After a user submits a form, the decentralized application creates a transaction that the user must sign to complete. Unlike the existing approach, in which the user evaluates the transaction manually, the add-on SABA approach evaluates the transaction using the suggested approach for identifying anomaly-based and signature-based blockchain transactions.

In the SABA approach, a transaction is directed to the user for manual verification if the system determines it to be suspicious. Additionally, if a transaction is identified as valid based on previous user activity (i.e., completed transactions), it could be automatically signed and then sent back to the decentralized application without needing the user to do any additional actions.

Thus, a transaction can still be digitally signed and published to the blockchain network via the decentralized application, which the user can only execute manually. In the SABA approach, two main content interacts with each other smoothly: SABA

chain forks, SABA transactions filter, and SABA threat data, SABA data concerning like collect, enhancing, and sharing such data with another network peer.

In general, if attacks are specialized to specific targets, Artificial Intelligence (AI) and Machine Learning (ML) can be investigated further by comparing suspicious transactions with a collection of destructive sequences (accumulated over time) to detect and eventually prevent a possible attack. The reason for such a SABA architecture is that SABA approach is not dependent on a specific Blockchain but can be programmed to identify attacks on any Blockchain application. Indeed, fundamental transaction parts like the wallet and miner do not include SABA elements but interact with them. Here is the outline of the approach of each SABA approach and how it interacts with conventional Blockchain applications; the standard SABA approach is divided into three levels, as indicated in figure 4.

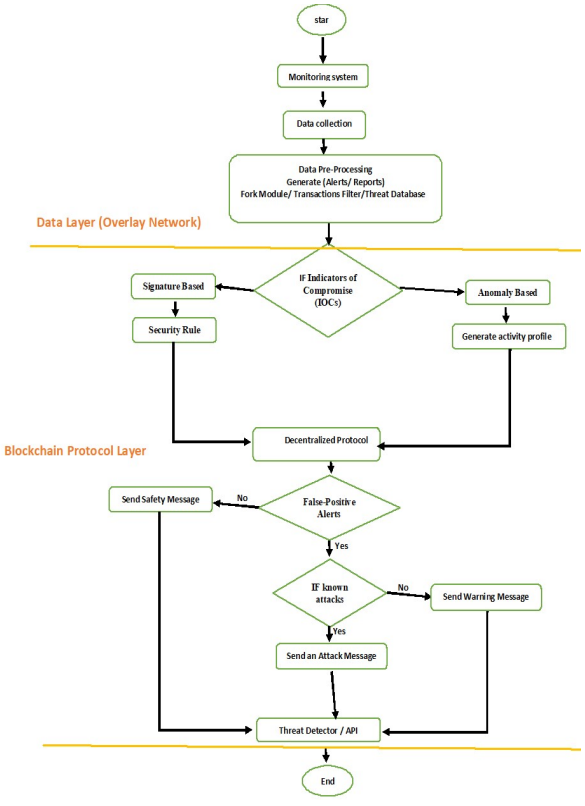

Figure 4: Flow Diagram of SBAB Model.

5.1 SABA Stages

In the SABA approach, IoT data storage on the cloud presents a significant challenge because IoT data are leaked, which could result in robberies, assaults, and the illegal sale of personal information for profit. The cloud infrastructure is in danger as a result of these circumstances. The use of Blockchain in cloud computing has the potential to give the entire architecture increased security. SABA approach was created as an ad hoc solution (a Blockchain-based application plug-in or a third-party service) rather than being incorporated into the transaction or any other specific Blockchain application. SABA Blockchain application has two main factors, which are (i) SABA Data Layer (Overlay Network) and (ii) SABA Blockchain Protocol Layer, as shown in the Figure. 4.

5.1.1Protocol Layer

In the SABA approach, the decentralized protocol is often utilized in Blockchain software solutions since it includes libraries that provide development aid as a significant facilitator of decentralized cloud solutions. Creating decentralized apps with built-in data (transaction payload), validation procedures, and transactions that a single organization does not control to Blockchain is now feasible, as illustrated in the figure 4.

5.1.1.1 Threats Detector

Starting with the abnormalities discovered by the inspector, SABA approach does root-cause research by utilizing previous Blockchain activity (previous blocks and transactions inside them) to roll back all of the victim's operations. Following that, all attack data is gathered in a threat database containing information on any dangerous patterns inside the Blockchain that must be considered hostile (depending on the security policy being used).

Figure 5, where A, B, and C were discovered to represent pieces of a malicious payload, depicts how this information is gathered and shared with peers. The threat database in SABA approach is an array that contains the information about detected attacks. Specifically, each attack is represented by a Sequence Detected (SD) in the i-th position of the outer array. In contrast,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Ti's hash of the attack sequence for the i-th transaction is reflected by the i-th position of the inner array (refer to figure 5). Link this substage to the next substage.

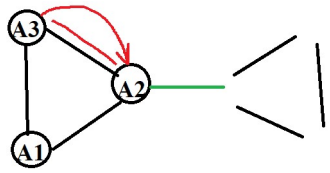

Figure 5: Malicious Payload.

5.1.1.2 APIs

In the SABA approach, applications developed on top of the data and protocol layers function similarly to those used today. However, they inherit the underlying Blockchain technology's security, privacy, and decentralization qualities. As a result, peers utilizing these apps can communicate and eventually establish a trustworthy agreement, as seen in the figure 4. An API interface between a transaction exchange and a user application gets data from it. It is an interface that connects directly or indirectly with a Blockchain node or a client network.

There are three categories of the blockchain, each with a slightly different set of protocols and consensus mechanisms. The consensus is to achieve agreement across validators (or miners) in a network on every new ledger of transactions. The blockchain is usually equipped with consensus protocols to tolerate unreliable involved parties or malicious nodes. The first category of blockchain is public in which anyone can participate in the chain and contribute to the consensus process. The read permission or the right to see the public blockchain is always open to anyone with access to the internet. The second category of blockchain is a consortium in which pre-selected nodes control the consensus process.

5.1.1.3 Decentralized Protocol

In the SABA approach, the Proof of Work (PoW) consensus approach. Blockchain-based solutions, for instance, the decentralized protocol in cloud solutions, leverage consensus and incentive structures to help distributed computing overcome some of the challenges above. The Linux Foundation is a strong backer of Hyperledger and has contributed much knowledge toward the protocol's development, as indicated in the figure 4.

5.1.2Data Layer (Overlay Network)

In the SABA approach, the leading Blockchain and its overlay network are still based on the core Blockchain protocol. Still, they are used to create networks called sidechains [23][24] that function parallel to the mainstream chain to do jobs that the mainstream chain cannot handle while still relying on the same data structures. Whatever shape these overlay networks take, they all have a link to the main chain. Such a connection is used to bootstrap their alternative solution by leveraging the mainstream p2p network; first, the time fork occurred; second, the time the fork was recognized; and third, the number and kind of malicious transactions identified inside the fork, if any, as shown in the figure 4.

5.1.2.1 SBAB Fork Module

It oversees the construction of our improved Blockchain, which, among other things, holds information on all forks formed thus far. It gets messages from the transaction filter and collects extra missing information from the chain database, where our upgraded Blockchains are eventually stored. Finally, the threat database informs the data layer whether the upgraded Blockchain has been updated and requires some threat analysis, as seen in the figure 4.

5.1.2.2 SBAB Transactions Filter

SBAB transaction Filter (Tx Filter) intercepts regular Blockchain messages and forwards them to the miner and the threat database, ensuring the regular protocol is not disrupted. Furthermore, it enables the collection of transaction meta-data from the threats detector in SABA approach. It provides the information necessary to populate the SABA's threat database, which is then utilized by the transaction filter to

prevent the repetition of known attacks. SABA approach transaction filter performs the filtering procedure each time a new block is received, as shown in figure 4.

5.1.2.3 SBAB Threat Database

Uses the chain database to detect unusual activity. The inspection of the forks may be done using any method, ranging from signatures to heuristic static analysis. The goal is to uncover sequences of transactions previously shown to be problematic. Remember that the solution is p. Miners are paid for the last time without operating if they are exceptionally efficient when the attacker, or the payload being distributed, replicates the same actions (i.e., the transaction content) against every peer (for example, in Botnet attacks). The core concept of SABA approach underpinning Blockchain Signature and Anomaly detection is to provide a new decentralized approach based on Blockchain technology that uses the information gathered from the previous fork in the data layer, as illustrated in the figure 4.

6. RESULT

A 51% attack in a transaction context modifies and falsifies 51% of the ledgers simultaneously [25]. As a result, it is a challenging attack to organize [26]. Furthermore, Successful 51% attackers may also implement a Denial-of-Service (DoS) attack [27] [28].

The attacker must have 51% or more of all users' calculating capabilities, establish two branches on purpose, and designate the targeted branch as the genuine Blockchain. A 51% attack in a transaction context consists of five phases [29].

Distribute mining software with a greater EV (Expected Value) as follow:

- New headers for mine (but validate it as soon as possible).
- Make the 2-h rule more "flexible."
- Choose a fork with its block version number.
- Inform miners about the "Goldfinger" reward.
- "Members Only" access.

Construct a sticky pool. (1) New members will receive 90% of their shares in the first two weeks and 110% after that:

- Form unfavourable alliances (timestamp attack).
- Use cannibalizing pools to attack other collections.
- Eventually, only members will be allowed.

When a genuine transaction is sent, a race attack produces hundreds of transactions and transmits them to many users [27]. Because many users likely believe the transferred transaction is valid, losses can occur if 51% of users update the ledger. An attacker uses a Finney attack to produce a block containing changed data and then attacks it [27]. Such attacks can be avoided if the attack target places the transaction in standby mode until the block is confirmed.

In the last part, we looked at SABA's overhead in the worst-case scenario, when an attacker uses transaction splits to disseminate malicious code. In this part, we look at a broader use scenario in which the attacker constructs as many blocks as necessary (creating more forks in the approach).

As a result, as demonstrated in the remainder of this section, SABA's bandwidth cost can only be proportional (up to a constant factor in practical circumstances) to the size k of our Threat Database TD. Let S1..., Sk represent the fraudulent transaction sequences of k discovered and stored in TD.

The length of each malicious sequence SD is I transactions inserted by the attacker to complete attack i. A partial sequence (PSD, j) is a Si subsequence that begins with the first transaction and ends with the j-th transaction of SD. It is worth noting that (PSD, I reflect the whole assault i. have at most one different partial subsequence for each attack i. Each network node keeps a set U of unfinished transactions. Given that H(t) is the hash of a transaction t, SABA approach executes two operations every time a node evaluates t:

- If a partial sequence (PSD, j) exists.
- U such that (PSD, j)
- ||H(t) = (PSD, j + 1)
- we replace (PSD, j) with (PSD, j + 1) in U.
- The usual concatenation function is represented by ||.
- If H(t) is the initial block of a series, SD.
- Then insert (PSD, 1) into U.
- Finally, SABA approach verifies.
- If there is a (PSD, I in U, the transaction t is discarded.

While the construction guarantees the validity of this strategy, the additional computing cost (per transaction) experienced by each node in the network may be calculated.

In the worst-case scenario (where every transaction of every attack has the same hash), every transaction will generate a new partial sequence (PSD, 1), I and will increase at most I 1 existing partial sequence in U for each attack i. This translates into the following steps:

- W(t) = k + X k i=1……. (1)
- (`i − 1) = X ……. (2)
- k i=1 ……. (3)

`i Since each attack sequence (in a practical situation) is no longer than a constant c of transactions, the total work W(t) for a particular transaction will be at most (c k = O(k)). where k = | TD |.

Pruning procedures can control the size of TD if it develops excessively fast. Old or uncommon attacks, for example, might be ignored in favour of freshly found ones.

7. CONCLUSION

As Blockchain technology continues to evolve, especially in conjunction with cloud computing, it is increasingly demonstrating significant gains in collaborative processing capabilities, IoT integration with its edge computing requirements, and decentralized data storage. This research proposes the use of SABA approach (Signature-Based Anomaly-Based Detection) as a solution. SABA approach facilitates the detection of abnormal transactions and prevents their further propagation. The rationale behind this approach is that attacks often exhibit similar patterns, even if they initially occur on a single device but later spread to multiple devices over time. Once the fundamental transaction patterns are identified, the feature extraction process, which involves transforming time series data, is initiated.

Using the anomalous detection approach, the activity profile for the anomaly-based side is constructed. Subsequently, each transaction is evaluated using SABA approach to determine its normality or aberrance. The accurate anomaly detection parameter of SABA's for-loop, which specifies the number of transactions analyzed, can be further optimized for specific addresses. If a transaction raises suspicion, the SABA approach prompts the user to verify it manually. On the other hand, if the transaction is deemed genuine based on prior user activity (i.e., completed transactions), it could be automatically signed and sent back to the decentralized application without requiring additional user intervention.

In its role of prevention, SABA approach collects harmful behaviors and constructs a distributed threat database, thereby eliminating any single point of failure and ensuring tamper-proof and trustworthy data confirmation by most of the network. Moreover, SABA's confidential nature safeguards behavioral data. It is essential to be vigilant against forks, which can occur naturally due to network delays but can also be maliciously engineered by attackers to propagate harmful activities throughout the Blockchain. In future works, efficient Machine Learning approaches are envisioned to reinforce the capability of identifying attacks, especially if these attacks exhibit polymorphic traits to evade detection. The quality and feasibility of SABA approach solutions could serve as a foundation for future developments in this domain.

REFERENCES

[1] R. Alzubi, Qusay M and Anbar, Mohammed and Sanjalawe, Yousef and Al-Betar, Mohammed Azmi and

Abdullah, "Intrusion detection system based on hybridizing a modified binary grey wolf optimization and particle swarm optimization," *Expert Syst. Appl.*, vol. 204, p. 117597, 2022.

[2] M. Tayyab, Mohammad and Belaton, Bahari and Anbar, "ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: a review," *IEEE Access*, vol. 8, pp. 170529–170547, 2020.

[3] Q. M. Alamiedy, Taief Alaa and Anbar, Mohammed and Alqattan, Zakaria NM and Alzubi, "Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm," *J. Ambient Intell. Humaniz. Comput. Publ.*, vol. 11, pp. 3735--3756, 2020.

[4] F. Coricelli and E. Ianchovichina, "Managing volatility in transition economies: the experience of the central and eastern European countries," *Available SSRN 560342*, 2004.

[5] Z. Yang, J. Wang, and M. Mourali, "Effect of peer influence on unauthorized music downloading and sharing: The moderating role of self-construal," *J. Bus. Res.*, vol. 68, no. 3, pp. 516–525, 2015.

[6] A. Upadhayaya, "Electronic Commerce and E-wallet," *Int. J. Recent Res. Rev.*, vol. 1, no. 1, pp. 37–41, 2012.

[7] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," 2017.

[8] B. R. Kandukuri and A. Rakshit, "Cloud security issues," in *2009 IEEE International Conference on Services Computing*, IEEE, 2009, pp. 517–520.

[9] H. Albaroodi, S. Manickam, and P. S. Bawa, "Critical Review of OpenStack Security: Issues and Weaknesses.," *J. Comput. Sci.*, vol. 10, no. 1, pp. 23–33, 2014.

[10] H. A. Albaroodi, S. Manickam, and M. F. Aboalmaaly, "The classification and arts of open source cloud computing: A review," *Adv. Inf. Sci. Serv. Sci.*, vol. 5, no. 16, p. 16, 2013.

[11] A. Donevski, S. Ristov, and M. Gusev, "Security assessment of virtual machines in open source clouds," in *2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, IEEE, 2013, pp. 1094–1099.

[12] R. H. Khan, "The use of real option analysis (ROA) to assist in security solution decisions," *Internat. J. Comput. Sci. Netw. Secur.*, vol. 11, no. 10, pp. 108–119, 2011.

[13] P. Cigoj and B. J. Blažič, "An authentication and authorization solution for a multiplatform cloud environment," *Inf. Secur. J. A Glob. Perspect.*, vol. 24, no. 4–6, pp. 146–156, 2015.

[14] S. S. Sarmah, "Application of block chain in cloud computing," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 12, pp. 4698–4704, 2019.

[15] W.-Y. Tsai, T.-C. Chou, J.-L. Chen, Y.-W. Ma, and C.-J. Huang, "Blockchain as a platform for secure cloud computing services," in *2020 22nd International Conference on Advanced Communication Technology (ICACT)*, IEEE, 2020, pp. 155–158.

[16] N. Khan, H. Aljoaey, M. Tabassum, A. Farzamnia, T. Sharma, and Y. H. Tung, "Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum," *Electronics*, vol. 11, no. 22, p. 3686, 2022.

[17] X.-W. Huang, C.-Y. Hsieh, C. H. Wu, and Y. C. Cheng, "A token-based user authentication mechanism for data exchange in RESTful API," in *2015 18th International Conference on Network-Based Information Systems*, IEEE, 2015, pp. 601–606.

[18] I. G. Anugrah and M. A. R. I. Fakhruddin, "Development Authentication and Authorization Systems of Multi Information Systems Based REst API and Auth Token," *Innov. Res. J.*, vol. 1, no. 2, pp. 127–132, 2020.

[19] M. M. A. De Graaf and S. Ben Allouch, "Anticipating our future robot society: The evaluation of future robot applications from a user's perspective," in *2016 25th IEEE international symposium on robot and human interactive communication (RO-MAN)*, IEEE, 2016, pp. 755–762.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[20] I. U. Din, K. A. Awan, A. Almogren, and B.-S. Kim, "ShareTrust: Centralized trust management mechanism for trustworthy resource sharing in industrial Internet of Things," *Comput. Electr. Eng.*, vol. 100, p. 108013, 2022.

[21] R. A. Abougalala, A. Amasha, M. F. Areed, S. Alkhalaf, and D. Khairy, "Blockchain-enabled smart university: A framework," *J. Theor. Appl. Inf. Technol.*, vol. 98, no. 17, pp. 3531–3543, 2020.

[22] C. D. STRUCTURING, "End2end unstructured data processing, confidential data structuring & storage using image processing, nlp, machine learning, and blockchain," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 13, 2022.

[23] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE internet things J.*, vol. 5, no. 2, pp. 1184–1195, 2018.

[24] W. Wang *et al.*, "Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet Things J.*, 2021.

[25] O. Zibouh, A. Dalli, and H. Drissi, "Cloud computing security through parallelizing fully homomorphic encryption applied to multi-cloud approach," *J. Theor. Appl. Inf. Technol.*, vol. 87, no. 2, p. 300, 2016.

[26] M. OA and B. AS, "SIMULATION OF THE RAINBOW ATTACK ON THE SHA-256 HASH FUNCTION," *J. Theor. Appl. Inf. Technol.*, vol. 101, no. 4, 2023.

[27] K. Alieyan, M. M. Kadhum, M. Anbar, S. U. Rehman, and N. K. A. Alajmi, "An overview of DDoS attacks based on DNS," 2016 International Conference on Information and Communication Technology Convergence (ICTC), Oct. 2016, Published, doi: 10.1109/ictc.2016.7763485.

[28] E. Alomari, S. Manickam, B. B. Gupta, P. Singh, and M. Anbar, "Design, deployment and use of HTTP-based botnet (HBB) testbed," 16th International Conference on Advanced Communication Technology, Feb. 2014, Published, doi: 10.1109/icact.2014.6779162.

[29] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco, and P. Wightman, "The 51% attack on blockchains: A mining behavior study," *IEEE Access*, vol. 9, pp. 140549–140564, 2021.