International Journal of Safety and Security Engineering
Vol. 12, No. 6, December, 2022, pp. 745-753
Journal homepage: http://iieta.org/journals/ijsse

Attack Detection Using a Lightweight Blockchain Based Elliptic Curve Digital Signature Algorithm in Cyber Systems

Ramesh Vatambeti[1*], Nadella Sree Divya[2], Hanumantha Rao Jalla[3], Mukkamula Venu Gopalachari[4]

[1] School of Computer Science and Engineering, VIT-AP University, Vijayawada-522237, India
[2] Department of Information Technology, Mahatma Gandhi Institute of Technology, Hyderabad-500075, India
[3] Department of Computer Science, Tikkavarapu Rami Reddy Government Degree College, Kandukur, Andhra Pradesh-523105, India
[4] Department of Information Technology, Chaitanya Bharathi Institute of Technology, Hyderabad-500075, India

Corresponding Author Email: ramesh.v@vitap.ac.in

https://doi.org/10.18280/ijsse.120611

Received: 1 December 2022
Accepted: 16 December 2022

Keywords:
attack detection, blockchain, cyber-physical system, distributed throughput management, elliptic curve digital signature, privacy

ABSTRACT

Cyber-physical systems (CPSs) are highly susceptible to malicious cyberattacks due to their reliance on communication networks. For this reason, many different attack detection techniques have been developed to guarantee the safety of CPSs. This article introduces BlockChain (BC) to address CPS issues such as data security and privacy. Additionally, BC is not well suited for CPS due to its high computing complexity, limited scalability, significant bandwidth overhead, and latency. To meet the requirements of CPS, a light-weight blockchain-based signature algorithm (LWBSA) model is developed in this work. The concept's resource constraints are alleviated by having a single centrally managed manager generate shared keys for outward-bound data transmission requests. The LWBSA paradigm provided herein produces an overlay network where extremely equipped resources can merge into a community BC, hence ensuring both dedicated privileges. Lightweight consensus, the elliptic curve digital signature algorithm (ECDSA), and distributed throughput management (DTM) are the three optimizations implemented in the ELIB model discussed here. Extensive simulation is carried out to examine the implications of different situations on processing time, energy usage, and overhead. The experimental outcomes show that the LWBSA achieves the best possible performance across a wide variety of measures.

1. INTRODUCTION

A Recent development in fields like computer science, control theory, and communication have paved the way for the substantial study of CPSs in both academic and professional settings. Computer-based techniques [1, 2] coordinate CPSs by syncing users and networks. A few examples of CPSs are autonomous pilot avionics, smart transportation networks, and 5G cellular networks. Sustainable technologies, medical equipment, process controls, robots, and robotic arms are some further examples [3-8]. Physical devices and computational components are frequently interconnected to form the networked units that make up a CPS [9]. Systems are susceptible to assaults [10-12], including denial-of-service (DoS) attacks and dishonesty attacks [13, 14], due to their heavy reliance on communication networks. Systems can be compromised in two ways: at the cyber (or network) layer and at the physical (or hardware) layer [15]. In addition, there are hostile actors who seek to do physical devices significant harm by targeting the interface between the cyber and physical layers.

It should be noted that without adequate hardware or software security safeguards, an attacker can arbitrarily disrupt scheme dynamics or cause arbitrary agitations in CPSs, potentially leading to major social problems [16-22]. In Iran, the Stuxnet malware [18] caused damage to a nuclear facility; in the United States, a nuclear plant accident [19] and a power outage in Brazil [20] are just two examples. These instances highlight the critical requirement for effective attack detection techniques to counteract malicious attempts and preserve CPS performance. With faster cyberattack detection and localization, the level of damage to infrastructure could be kept within acceptable bounds.

Security measures against assaults must be designed and implemented to guarantee CPS's smooth operation. Detecting attacks in time to prevent or lessen their impact is a crucial part of any security system. Since static attack detectors only take into account the system's output at a single time step, they can't identify attacks on the actuators. Several strategies exist for detecting intrusion attempts. In this study, we explore how blockchain knowledge might be used to identify cyberattacks. An introduction to blockchain is provided here.

1.1 Background of BC

This section begins with a quick introduction to blockchain technology, then moves on to describe cutting-edge CPS authentication and authorization methods. Blockchain is a ledger that stores the verified and immutable records of all network-executed and processed transactions. The blockchain operates on a distributed, peer-to-peer system. Each computer in a network using blockchain technology keeps an identical

copy of the distributed ledger. These registers are regularly updated [22], as each transaction is verified.

Bitcoin was the first cryptocurrency to implement the blockchain technology, which was designed from the start to be a protocol for processing financial transactions. Despite this, its unforgeability, decentralization, and fault-tolerance make it an excellent fit for the cybersecurity ecosystem. Presently, verification and access control are just two of the many security methods that rely on blockchain technology to offer the necessary security criteria for securing a system. This ledger keeps track of the total number of blocks that have been linked using a hash function. The first half of each block stores the total number of confirmed and performed transactions. A health record, a money transaction, or a network infrastructure message are all examples of possible transactions. Various data structures are used to organise these mechanisms. Using the reverse hash technique, the central root hash of a Merkle tree is recorded as the block hash [23]. The block's second section is called the block header and contains the block's hash, the time stamp for the transactions within the block, and the hash of the preceding block. With this method, pre-existing links are linked together to create a chain that is secured by a hash. The greater the number of links in the chain, the less susceptible it is to being tampered with. In addition, because each block is linked to the next through a hash, if a malevolent user wants to alter the connections of a block, that user must also change the corresponding transactions in each consecutive block.

There are two primary categories of nodes in a blockchain network. One category of nodes is known as passive nodes, and their job is to store and read the block data but not to generate a novel block or initiate a transaction. The second kind of node is a miner node, and it may produce a block and verify transactions just like any other node. Many different consensus algorithms are employed to verify new blocks and add them to the genesis blockchain. The blockchain's nodes can reach a unanimous decision to add a new block thanks to the consensus process. Proof-of-Work (PoW) is an agreement algorithm used by the Bitcoin network. In the Proof-of-Work (PoW) algorithm, validating a block requires solving a mathematical puzzle. The time it takes to validate new blocks and the computing power of the miner nodes both affect how challenging the puzzle needs to be [24-27].

1.2. Cyber attack types

1.2.1 Denial of service attacks

A DOS attack is a type of attack in which the assailant prevents legitimate users from accessing a system by overloading its processing or memory resources.

Remote to Local (User) Attacks (R2L). An R2L attack is a type of attack in which a hacker sends packets to a system over a network in order to gain unauthorised local access to the machine by exploiting a security flaw. Attackers who can transmit packets to a system over a network but don't have an account on that machine can get local access as a user of that machine by exploiting a vulnerability.

User to Root Attacks (U2R). User-to-root (U2R) attacks happen when an attacker gains access to a regular user account on the system (via methods like password sniffing, dictionary attacks, or social engineering) and then uses a vulnerability to elevate their privileges until they can execute arbitrary code as the system's root user.

Probing. Probing is a type of attack in which an attacker examines a network in search of information or known vulnerabilities. The availability of machines and services on a network can be exploited by an adversary who has a map of the infrastructure.

1.3 Classification of cyber attacks

In order to infect the system successfully, the attacker will count on the process being unified. They are successful in their mission since they have coordinated the various stages of the theft of the information. In other words, the hackers will obtain their consequence on time, in step, and in line. Attackers and hackers can quickly infect a system if they have a well-thought-out plan to do so. In order to achieve better outcomes, they employ procedures that are logically ordered. The attacks are meticulously planned and executed to do maximum harm and disrupt the target organization's operations.

- Scouting missions: a form of cyberattack characterised by the illegal use of maps and services for detecting systems in order to steal information.
- Access Attacks Hacking is an attack in which the hacker gains access to a system where he should not be failure to provide service.
- Disabling a network in order to prevent legitimate users from accessing it is an example of a DOS attack. A DOS attack is a type of attack in which the attacker prevents legitimate users from accessing a system by making its processing or memory resources too overloaded to fulfil their demands.
- Definition of cybercrime: exploiting people using computers and the internet for financial gain
- An example of cyber espionage would be conducting covert surveillance on an adversary via the internet for ulterior motives.
- Cyberterrorism is the deliberate use of the Internet and other forms of electronic communication to cause widespread material damage and disruption to society.
- To disrupt another country's network with the aim of gaining tactical and military advantage is to engage in cyberwar.
- Assaults in Progress: An attack in which all involved parties receive the same information, allowing for extensive compromise.
- The use of passive aggression is an assault that consists mainly of listening in rather than altering the database.
- When harm is intended, as in a malicious attack, it can have far-reaching effects.
- Accidental attacks caused by mishandling or operational errors that result in minimal data loss are classified as "non-malicious attacks."

2. RELATED WORKS

After the FDIAs were discovered in a microgrids system by Ghiasi et al. [28], the security of DC-microgrids (DC-MGs) was improved by analysing the voltage and current signals in smart controllers in order to extract the signal details using the Hilbert-Huang transform methodology and blockchain-based ledger knowledge. The purpose of analysing the simulated case results is to confirm the validity of the suggested model.

The findings imply that the proposed model can improve the safety of data exchange in a smart DC-MG by providing a more precise and robust detection apparatus in contradiction of FDIA.

Guha Roy and Srirama [29] presents the distributed mechanism of security for IoT in mobile fog utilising a SDN integrated with blockchain. The system traffic is continuously monitored and analysed by the SDN in order to provide an attack identification model. By providing a decentralised attack identification technique that can spot attacks in the fog and mitigate them at the edge node, the blockchain has been leveraged to solve the failure problems that were previously addressed by the existing models.

Choi et al. [30] suggests an MITM attack detection approach for a PV system that uses blockchain technology. Distributed ledgers and hash comparisons of data in transit are all part of a ground-breaking new approach to monitoring network traffic and detecting intrusions. Experiments verify the efficacy of the suggested approach when it is implemented in IoT security modules operating as blockchain network clients. A Sybil attack detection mechanism in UWSN has been proposed by Arifeen et al. [31]. The authors of this study have also combined a previous trust perfect with the approach to make it resistant to attack detection.

Federated Learning (FL) is used by Yazdinejad, A., and colleagues [32] to create a threat hunting system named Block Hunter, which can autonomously scour blockchain-based IoT networks for signs of intrusion. The anomaly detection in Block Hunter is performed using a federated, multi-machine learning model cluster-based architecture. We believe Block Hunter, as it can detect suspicious activity without compromising users' privacy. By demonstrating the Block Hunter's ability to detect abnormal activity with high accuracy and low bandwidth consumption, we have demonstrated the tool's efficacy.

In this article, Medhane et al. [33] introduced a security framework that makes use of edge cloud and SDN. As a result of the cloud layer's success in detecting security assaults, the IoT network's edge layer can experience fewer security breaches. The SDN-enabled gateway delivers dynamic control of network traffic flows, which aids in the identification of security attacks by identifying suspicious network traffic patterns and mitigates assaults by blocking such flows. As demonstrated by the results, the suggested security framework is up to the task of addressing the risks to data privacy brought about by the convergence of the blockchain, the edge cloud, and the SDN paradigm.

To promote incentive-based and trustworthy cooperation between enterprises in the face of cyber threats, Purohit et al. [34] presents a revolutionary threat intelligence sharing and defence mechanism, dubbed "DefenseChain." To gather threat information and identify appropriate peers who can aid in attack detection and mitigation, this solution approach makes use of a consortium Blockchain platform. We offer a business model for forming and maintaining the consortium among its peers by means of a standing estimation scheme based on the Quality of Detection and Mitigation criteria. Experiments assessing DefenseChain functionality are run in both a real-world setting and a simulated one using an Open Cloud testbed outfitted with Hyperledger Composer. The outcomes demonstrate that when compared to leading-edge decision-making techniques, the DefenseChain system excels at selecting the best possible detector and mitigator peers. When looking at measures like attack recurrence rate, detection time, and mitigation time, the results reveal that the DefenseChain provides better performance trade-offs.

A model for the secure storage and collection of cryptographic evidence was created by Bhardwaj and Dave [35]. The approach is employed to identify malware attacks, store evidence, and classify network traffic data. Digital evidence is safely stored and preserved (tamper-safe). Deep learning and machine learning classifiers are used to glean the meta-data for malware traffic. There has been a lot of research showing that ensemble classifiers can improve malware and real-time data streaming through a network, while deep learning can help with the study of massive data sets. This article proposes a deep learning model based on an ensemble classifier to examine malicious packets, learn from collected data, and make sure that evidence is still available (live) if and when it's needed during a forensic investigation of a malware attack on a network. When compared to other models for malware identification and evidence preservation, the suggested model has a higher average score of 97%.

Jiang et al. [36] proposed a light weight block chain for edge computing (LBlockchainE) and proposed the data placement strategy. LBlockchainE applies the low-energy-consumption characteristics of Proof of Stake to determine the ownership of bookkeeping rights through a small number of competitive calculations and the resources of the node. Xi et al. [37] ensure the data integrity and avoids the single point of failure by introuding light weight block chain technology (CrowdLBM). To support the crowdsensing process without third party, this model proposes a two-stage scheme and two types of smart contracts.

3. PROPOSED METHODOLOGY

A. System Model

The cyber-physical scheme is modelled by

$$\begin{aligned} x(k+1) &= Ax(k) + \overline{Bu(k) + Ba(k)} \\ y(k) &= Cx(k) + \overline{Bu(k) + Ba(k)} \end{aligned} \tag{1}$$

where, xRn represents the current state of the system, yRp represents the output, kZ represents the current time index, uRm represents the known input, $and\ a(k)Rs$ represents the unknown attack. The input u(k) can be disregarded because we already know how much it affects the final result *y(k)*. Therefore, we reflect the situation of $u(k)0, k = 0{,}1$ without losing generalization for the rest of the work. We adjust the system model accordingly, making it

$$\begin{aligned} x(k+1) &= Ax(k) + Ba(k), \\ y(k) &= Cx(k) + Da(k) \end{aligned} \tag{2}$$

The matrices B and D define the competences of the attacker.

B. Dynamic attack detection: Preliminaries

By analysing the output Y(T) of the system and the beginning state information from the side, the dynamic attack detector y(t) can identify if an attack has happened:

$$\psi: \mathbb{R}^{p(T+1)} \times \mathbb{R}^{q} \rightarrow \{Attack, No\ Attack\} \tag{3}$$

where, “Attack” resources that an attack has happened.

C. Problem statement

Let x(0) be the starting state of the scheme = (A,B,C,D) and let y = x(0) be the side initial public information throughout the time range 0,1,...,T,Tn -1. (0). We focus on these four major issues: The first step is to discover U(,T), the set of all undetectable attacks; the second is to figure out which attacks within $E(T)\ U(,T)$ have time $T' > T$; the third is to figure out if there is an arbitrarily long attack that induces a zero state against ; the fourth is to design a reliable detector that makes use of side information and finds all obvious attacks.

3.1 Proposed LWBSA perfect

As can be seen in Figure 1, the provided LWBSA model is comprised of two primary ideas. When communicating between different entities, the T is a necessary component for passing along control information. Another key difference from Ts is the data flow. The next component with BC management capabilities is the block manager (BM). Each and every Ts and blocks of Ts must go through three steps: generation, verification, and storage. In the sections that follow, we'll talk about the ways in which the BMs' functionality differs between the overlay and smart home layers.

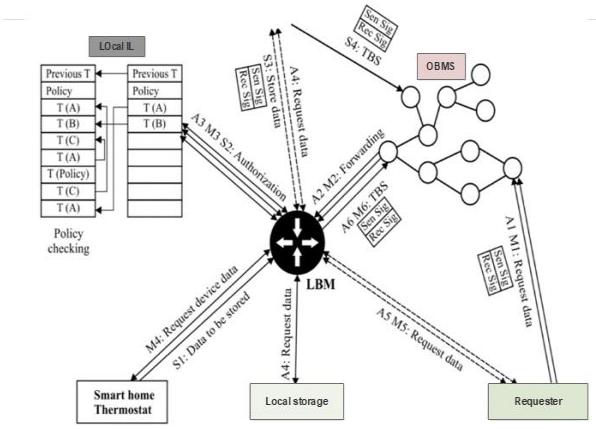

Figure 1. Process of storing, observing and monitoring Ts

3.1.1 Overlay

A "PK" in this sense is an individual overlay node. When generating a new T, the network's nodes randomly select one of several distinct PLs, so protecting the privacy of its users. Smart homes (expressed as Local BMs), mobility entities, Service Provider (SP) servers, and cloud storages are all examples of overlay nodes (utilized by smart home components to store data). Multiple nodes, sometimes in the thousands, are considered in overlay networks. To achieve this scalability, it is expected that the public BC will be administered by a group of overlay nodes. It is anticipated that clustering will be utilised to arrange the nodes into groups, with each group afterwards selecting its own leader (CH). Overlay Block Managers are often the CH who perform the functions of BC management (OBMs). More than that, CH handles all the Ts coming into and going out of the cluster members. Selecting a node to act as a CH requires consideration of its expected uptime, as well as its capacity to handle the computational demands of processing blocks and Ts. Since the CHs are responsible for the bulk of the work, LWBSA is immune to the transient nature of IoT devices.

The overlay nodes' Ts are protected by the use of several different operations. Overlay Ts are categorised as either I single signature Ts or (ii) multisig Ts, the latter of which bear both the signatures of Rr and Re. The first field of the T is reserved for the identification, while the second field contains a pointer to the preceding T of the analogous Rr node. Therefore, each T produced by a Rr is connected to all the others. The subsequent signature occurs when the Rr is handed the T. The T output, shown by the seventh field, is predetermined by the Rr and consists of three parts: the hash of the PK used by the Rr for subsequent Ts, the number of Ts avoided by Re, and the number of Ts received by Re. The first 2 fields give information about the Rr's history, which is used to determine the Rr's reputation. Since the overlay nodes can alter the PK used to produce each novel T, the final field is required for additional Rr authentication. The final section of a multisig T contains information on the operation being performed. Although each signature T has its own distinct structure, they all share the same overlay node and hence include the Re PK and signature as well as the metadata and outputs [0] and [1]. Due to the differences in output, multisig and solitary signature Ts are organised as separate ledgers.

Both data and T flow are isolated in the LWBSA model. When the Re device detects that the Rr has permission to access the T, it sends the data in a discrete data packet to the Rr. Similarly, the data produced by the Rr is conveyed definitively from T in order to store T. Data packets, in contrast to Ts, which broadcast the can be directed down the most efficient paths using an overlay network.

The OBMs maintain custody of the overlay Ts stored in the public BC. Every BC block has two main parts: the Ts and the block header. The former component stores the block's hash, the block generator ID, and the verifier signatures. The previous block's hash in the public BC confirms the immutable nature of the blockchain. If an attacker tampers with a previously saved T, the succeeding block's hash of the equivalent will be invalid and unable to correctly comprehend the attack. Details about the "block generator ID" and "signatures of the verifiers" are provided. The many Ts are combined into a single unit for processing. Each unit has a maximum storage capacity of T max Ts. Since the BC's efficiency is affected by T max, a larger value for T max results in a greater number of Ts being stored in a given block.

The first thing the OBM does after receiving a TY is to make that the T's Re is actually there in the cluster. An Rr/Re PK pair identifies a Rr that can send Ts to a specific Re, and this pair is stored in the OBM's key list (essentially an access control list). One of the nodes in the cluster is responsible for updating this key list, which is then used to authorise outgoing Ts from other nodes in the overlay network. When a Re receives a T with its PK as the Re PK, it may set the Rr value in the OBM key list to broadcast. As soon as the OBM determines that the incoming TY's Rr and Re correspond to an entry in the list of keys, it will send the T to the Re (that lies inside a cluster and hence straightaway linked to the OBM). For all OBMs, the T will be sent out if the Re in Y does not come from the same cluster as those already present. Each OBM has its own T pool where all pending Ts are stored. As soon as the current pool size reaches Tmax, OBM will begin the consensus-based mechanism for creating a new block.

3.1.2 Consensus algorithm

Current resource-intensive approaches like PoW and PoS are commonly used in BC, however in LWBSA a time-dependent consensus strategy is offered as an alternative. Consensus ensures that a block producer is arbitrarily

designated between nodes and that the maximum sum of blocks that can be generated is agreed upon. To introduce randomness amongst nodes, each OBM must observe a waiting period before beginning the process of creating a new block. A new block may be formed for an OBM by another OBM that controls some or all of the Ts in the OBM's existing pool of Ts, with the waiting time varying depending on the OBM in question. Due to the fact that the Ts are being stored in BC by other OBM, the OBM should remove them from its pool at this time. OBMs need to wait for an arbitrary sum of time, but doing so lessens that time and cuts down on the creation of duplicate blocks at the same time. Whenever a new block is produced, a notification is sent.

To prevent the overlay from being vulnerable to an adding attack in which a malicious OBM artificially inflates the number of blocks in the blockchain by inserting many blocks with false Ts, the frequency with which OBMs can create blocks is constrained to a single block being created every consensus period. Consensus-period has a default (and maximum) value of 10 minutes, which is also the length of time that mining takes to complete. To guarantee that blocks generated by other OBMs have enough time to spread throughout the network, the consensus period should be set to at least double the longest end-to-end latency in the overlay.

Each OBM keeps tabs on the cycle rate of the others, and this is how blocks are made. In this case, we get rid of some of the non-compliant blocks and weaken our reliance on the responsible OBM. To prevent OBMs from perpetually keeping a shorter waiting period, neighbouring OBMs verify that a given OBM produces novel blocks at the outset of the waiting period. Depending on the use case, OBMs will reject blocks generated by their neighbours once the total number of such blocks reaches a predetermined limit.

3.1.3 Elliptic curve digital signature algorithm

In order to create a digital signature, ECDSA makes use of elliptic curve encryption. Let's pretend the sender needs to deliver the elliptic-curve-signed message to the recipient. To begin, we must agree upon a common set of parameters and formulate them in a form that can be understood by all parties (CURVE,G,n). Assume that the elliptic curve has the point domain and geometric equation curve, that all dot product operations begin at G, that the elliptic curve has the multiplicative order n, and that nG=0.

In the second step, the sender makes a pair of keys called a private key and a public key. In which the secret key is a random number between *1* and *n-1*:

$$d_A = rand(1, n-1) \tag{4}$$

The public key is the dot product of the private key and the starting point on an elliptic curve:

$$Q_A = d_A \times G \tag{5}$$

1) Signature algorithm

Signer completes message with signature. Message m in this scheme contains details about the user, such as their name and their attributes.

This is how to do it step-by-step:

1: Compute $e = h(m)$, where $m = (UID|h(pswd))$;

2: And derive z from the L-th (most left) bit of binary e, with L being the n in the aforementioned values;

3: Select a random digit k from $[1, n-1]$;

4: Compute a elliptic curve:

$$(x_1, y_1) = k \times G \tag{6}$$

5: Compute the value of r, if $r == 0$, reappearance to step-3;

$$r = x_1 mod\ n \tag{7}$$

6: Compute the value of s, if $s == 0$, return to step-3 for recalculation

$$s = k^{-1}(z + rd_A) mod\ n \tag{8}$$

7: The digital sign is the made (r, s).

2) Verification algorithm

The recipient will get a public key as well as any signature papers that were sent. As a result, there are two steps to the authentication process: verifying the public key and then the (r, s).

a) Confirmation of public key

1: The organizes of public key Q_A should be valid and not equivalent to a border value of null point O;

2: The organizes of key Q_A are used to validate;

3: The point product of the n and the public key is a necessary condition for the formula (5) to work;

b) Confirmation of signature files

1: Validate r and s are integers in the variety of $[1, n-1]$; otherwise, the verification fails;

2: Compute $e = h(m)$;

3: Then compute z, from the uppermost L bit of e;

4: Following, compute w with

$$w = s^{-1} mod\ n \tag{9}$$

5: And u_1 and u_2

$$u_1 = zwmod\ n, \qquad u_2 = rwmod\ n \tag{10}$$

6: Then compute (x_1, y_1) the (x_1, y_1) should be the elliptic curve; then, the verification fails;

$$(x_1, y_1) = u_1 \times G + u_2 \times Q_A \tag{11}$$

7: The subsequent formula must hold; then, the verification fails.

$$r = (x_1\ modn) \tag{12}$$

The verification can be considered successful under two circumstances: (a) the verification data is correct, and (b) the consensus node's correct threshold reaches the required minimum of verifications, which is,

$$t \geq t_0, t_0 = 2f + 1 \leq n \tag{13}$$

In the PBFT $t_0 = n - f \geq 2f + 1$, such as, if $f = 1$, the illness for reaching consensus is that the number of precise nodes (t_0) is at least 3.

Authentication success is communicated to the endorser node and then relayed to the client over the channel;

verification failure is communicated to the client over the channel.

3.1.4 Distributed throughput management (DTM)

Since solving the cryptographic puzzle is intensive, traditional consensus mechanisms used in BC limit the throughput of BC, which is leisurely by the total T count saved in BC per second. For instance, Bitcoin BC has a cap of seven Ts per second owing to POW. These limitations are unacceptable in the IoT due of the wide variety of interactions possible between the many nodes. To keep BC exploitation within reasonable bounds, LWBSA employs a DTM method to keep a close eye on it and design appropriate adjustments. Utilization () is calculated by each OBM at the end of newly produced Ts to Ts added to the BC. It should be observed that all OBMs get the same transmissions of T and blocks, and that all OBMs independently determine the same use. DTM's primary goal is to ensure that a certain value (_min, max) is adhered to. Assume a network of N nodes, where M OBMs are present, and a typical rate of T generation for nodes, denoted by R. Eq. (11) can be used to get the usage rate:

$$\alpha = \frac{N * R * consenus - Period}{T_{max} * M} \tag{14}$$

Eq. (11) suggests two methods for optimising resource distribution: Given that each OBM generates a unique block within the consensus period, the number of blocks included in the BC can be changed in one of two ways: I by modifying the consensus-period that regulates the occurrence of the number of blocks included in the BC, or (ii) by adjusting M. Because it necessitates a complete reconfiguration of the overlay network, the subsequent one is laborious and draining on available resources. Consequently, when > _max, DTM initially investigates whether or not the consensus period can be reduced. Using the aforementioned equation, a new value for the consensus period can be determined by assuming that is equal to the median of the defined range (_min, max) that verifies a stable operating point for the network. In contrast, reclustering with a new M value computed using Eq. (14) is required when the consensus-period cannot be shortened. Because of this property, the LWBSA model may scale to large numbers of nodes, resulting in greater throughput.

4. RESULTS AND DISCUSSION

In this segment, the projected model LWBSA is tested with efficiency analysis and security analysis.

4.1 Secure performance analysis

Some important security considerations in the architecture of the CPS scheme are required to ensure the safe and effective operation of the CPS. Before diving into the investigation, we provide an overview of the security needs of the Internet of Things. We next compare the authentication technique suggested in this study to others already in use in the CPS and conduct an analysis of its security against a number of typical network attacks.

Authentication is one of the most important IoT security concerns. With these security needs in mind, we conduct the following analysis:

4.1.1 Integrity

Data and communication are usually considered integral parts of integrity. When we talk about the CPS's data being "intact," we mean that it is protected from tampering from outside sources. This is exactly what this paper's authentication mechanism is meant to do. Message integrity ensures that communications between CPS users and their devices are secure and unmodifiable at any point in time. In this work, we use both a public blockchain and a private blockchain to perform the authentication procedure. After a transaction is submitted, it has been verified for integrity and cannot be altered. The authentication technique guarantees the message's integrity.

4.1.2 Availability

As a result, the CPS's services are more accessible to legitimate users on legitimate devices. DoS assaults are a threat that must be mitigated. An examination of DoS attacks on the authentication of identities is forthcoming.

4.1.3 Scalability

Achieving this is crucial for the safety of CPS. The peculiarities of the CPS necessitate regular replacement of hardware. The primary method for dealing with this issue is now scalability. The authentication technique presented in this study is scalable, authenticates valid nodes efficiently, and blocks malicious ones from accessing the network.

4.1.4 Non-repudiation

It means that neither the user nor the device can deny the actions taken or the data transmitted. Blockchain technology is used to implement this plan; all transactions are recorded there in an immutable ledger that no one can alter.

4.1.5 Mutual authentication

With mutual authentication, both senders must prove their identities before establishing communication. This paper proposes a technique for authentication in which ordinary nodes identify the authenticated party via physically located.

Authentication schemes must be able to withstand some of the more frequent network threats in the IoT in order to fulfil the aforementioned security requirements. This study analyses the security of the authentication system and compares it to the current scheme with the goal of protecting CPS networks against common network threats.

4.1.6 Sybil attack

The technique proposed in this study assigns a unique identifier (OID) to each ordinary node in the network, and then uses the identifiers (SID, CID, OID) of the cluster head node and the base station, respectively, to identify any normal node in the whole network prior to any connection. The blockchain, either a public one or a local one, is used for authentication. Intruders can't compromise the network by pretending to be nodes so they can exchange data with other nodes.

4.1.7 Spoofing attack

An attacker cannot attack another node by pretending to be it due to the requirement of two-way identity authentication and the verification of the IDcard held by each node to show its unique identity.

4.1.8 Message substitution attack

This paper proposes a new authentication strategy that requires nodes to register, perform mutual authentication, and

then revoke registration if necessary. There is no way for messages to be substituted throughout the interaction process, as the registration of cluster head nodes is sent straight to the public blockchain. An intelligent contract is activated by a local blockchain node's broadcast registration request message, which verifies the registration procedure of a shared node. Registration information remains the identifying information of the genuine node even if the message is altered. Authentication requests issued to cluster head nodes can only be initiated by regular nodes with access to the cluster network, and these requests cannot be tampered with in transit.

4.1.9 Message replay attack

The paper's suggested authentication mechanism relies heavily on the blockchain, where the majority of its operations are executed, making it immune to message replay attacks. Message replay attacks can occur in two different ways: In order to (1) get authenticate with other regular nodes, a node will need authentication confirmation credentials from both cluster heads, and (2) prevent having to re-register with the cluster head node at this time after requesting registration. Therefore, an adversary cannot use message replay to authenticate.

4.1.10 A middle attack

The authentication message is snatched by the man-in-the-middle attacker while it is in transit from the compromised third-party node. Similar to the analysis of message replay attacks, if an attacker (1) the original legitimate node's node information, (2) the attacker still cannot gain access to the network because authentication during the authentication stage requires the signature authentication of both cluster heads. Man-in-the-middle attacks, therefore, are rendered futile by this method.

4.1.11 Denial of service

By design, attackers cannot directly launch DoS attacks on the local blockchain in this authentication technique because it is a private chain self-possessed only of cluster head nodes in WSN. It takes time and energy to submit a transaction to the public blockchain, therefore attackers cannot cause the network to crash by sending too many authentication requests. Legal authentication cannot be completed by the typical node.

4.2 Efficiency analysis

In the above Table 1 represent that the Evaluation of time overhead in the LBM. In this evaluation, there are different techniques are used as Block-chain in SDN, Federated Learning, DefenseChain and Proposed LWBSA. In this comparisons analysis, the proposed model reaches the better Access Transaction.

In the above Table 2 represent that the Evaluation of energy consumption. In this evaluation, there are different techniques are used as Block-chain in SDN, Federated Learning, DefenseChain and Proposed LWBSA. In this comparisons analysis, the proposed model reaches the better and low energy consumed by proposed model than other techniques.

Table 1. Evaluation of time overhead in the LBM

Technique	Store transaction time period	Store Transaction Query Based	Access Transaction
Block-chain in SDN	**23**	**46**	**12**
Federated Learning	**24**	**45**	**13**
DefenseChain	**25**	**49**	**14**
Proposed LWBSA	**29**	**52**	**14**

Table 2. Evaluation of energy consumption

Technique	Access	Store-Query	Store-Period
Block-chain in SDN	**56.37**	**56.38**	**56.44**
Federated Learning	**56.38**	**56.39**	**56.45**
DefenseChain	**56.39**	**56.42**	**56.47**
Proposed LWBSA	**55.41**	**54.45**	**54.49**

Table 3. Assessing the impact of packet overhead

Technique	0	7	10	13	15	17	20
Block-chain in SDN	**940**	**1290**	**2678**	**3800**	**4845**	**5300**	**7340**
Federated Learning	**790**	**989**	**2245**	**3002**	**4204**	**4589**	**6900**
DefenseChain	**490**	**700**	**1789**	**2398**	**3900**	**4320**	**6200**
Proposed LWBSA	**250**	**500**	**1300**	**1950**	**3200**	**3980**	**5023**

Table 4. Average processing period on OBMs for fresh blocks

Technique	1	10	20	30	40	50	60
Block-chain in SDN	**0.04**	**0.09**	**0.13**	**0.15**	**0.19**	**0.21**	**0.24**
Federated Learning	**0.03**	**0.07**	**0.10**	**0.12**	**0.15**	**0.18**	**0.21**
DefenseChain	**0.03**	**0.07**	**0.09**	**0.11**	**0.16**	**0.16**	**0.18**
Proposed LWBSA	**0.02**	**0.05**	**0.07**	**0.09**	**0.11**	**0.14**	**0.16**

In the above Table 3 represent that the Assessing the impact of packet overhead. In this evaluation, there are different techniques are used as Block-chain in SDN, Federated Learning, DefenseChain and Proposed LWBSA. In this comparisons analysis, the proposed model reaches the better low packet overhead by proposed model than other techniques.

In the above table4 represent that the Average processing time on OBMs for validating fresh blocks. In this evaluation,

there are different techniques are used as Block-chain in SDN, Federated Learning, DefenseChain and Proposed LWBSA. In this comparison's analysis, the proposed model reaches the better Average processing period on OBMs for confirming fresh blocks by proposed model than other techniques.

5. CONCLUSION

Although BC has been the subject of this article because of its effectiveness in providing security and privacy in CPS, its implementation in this setting raises a number of serious concerns, such as computation complexity, bandwidth, delay, and overhead. To address concerns about privacy and safety in CPS, this study describes a LWBSA model that has been built. The proposed LWBSA model has three distinct components: a consensus method, a distributed key encryption model, and a distributed key management scheme. Several possible future states are simulated in great detail. At steady state, the LWBSA achieves a 50% reduction in processing time relative to the baseline approach while using only 0.07 mJ less energy. In addition, it has a least packet overhead of 4500 kB when 20 OBMs are present. From the experimental results, it was concluded that the LWBSA performs optimally across a wide range of criteria. The proposed work can be enhanced in the future to reduce energy usage and be implemented in a wide range of applications.

REFERENCES

[1] Sridhar, S., Hahn, A., Govindarasu, M. (2011). Cyber–physical system security for the electric power grid. Proceedings of the IEEE, 100(1): 210-224. https://doi.org/10.1109/JPROC.2011.2165269

[2] Murguia, C., van de Wouw, N., Ruths, J. (2017). Reachable sets of hidden cps sensor attacks: Analysis and synthesis tools. IFAC-PapersOnLine, 50(1): 2088-2094. https://doi.org/10.1016/j.ifacol.2017.08.528

[3] Chen, H. (2017). Applications of cyber-physical system: a literature review. Journal of Industrial Integration and Management, 2(3): 1750012. https://doi.org/10.1142/S2424862217500129

[4] Lu, Y. (2017). Cyber physical system (CPS)-based industry 4.0: A survey. Journal of Industrial Integration and Management, 2(3): 1750014. https://doi.org/10.1142/S2424862217500142

[5] Khaitan, S.K., McCalley, J.D. (2014). Design techniques and applications of cyberphysical systems: A survey. IEEE Systems Journal, 9(2): 350-365. https://doi.org/10.1109/JSYST.2014.2322503

[6] Atat, R., Liu, L., Chen, H., Wu, J., Li, H., Yi, Y. (2017). Enabling cyber‐physical communication in 5G cellular networks: challenges, spatial spectrum sensing, and cyber‐security. IET Cyber‐Physical Systems: Theory & Applications, 2(1): 49-54. https://doi.org/10.1049/iet-cps.2017.0010

[7] Wu, J., Guo, S., Huang, H., Liu, W., Xiang, Y. (2018). Information and communications technologies for sustainable development goals: state-of-the-art, needs and perspectives. IEEE Communications Surveys & Tutorials, 20(3): 2389-2406.. https://doi.org/10.1109/COMST.2018.2812301

[8] Atat, R., Liu, L., Wu, J., Li, G., Ye, C., Yang, Y. (2018). Big data meet cyber-physical systems: A panoramic survey. IEEE Access, 6: 73603-73636. https://doi.org/10.1109/ACCESS.2018.2878681

[9] Lee, E.A. (2008). Cyber physical systems: Design challenges. In 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC) Orlando, FL, USA, pp. 363-369. https://doi.org/10.1109/ISORC.2008.25

[10] Peng, C., Sun, H., Yang, M., Wang, Y.L. (2019). A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(8): 1554-1569. https://doi.org/10.1109/TSMC.2018.2884952

[11] Mahmoud, M.S., Hamdan, M.M., Baroudi, U.A. (2019). Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges. Neurocomputing, 338: 101-115. https://doi.org/10.1016/j.neucom.2019.01.099

[12] Fawzi, H., Tabuada, P., Diggavi, S. (2014). Secure estimation and control for cyber-physical systems under adversarial attacks. IEEE Transactions on Automatic control, 59(6): 1454-1467. https://doi.org/10.1109/TAC.2014.2303233

[13] Teixeira, A., Shames, I., Sandberg, H., Johansson, K.H. (2015). A secure control framework for resource-limited adversaries. Automatica, 51: 135-148. https://doi.org/10.1016/j.automatica.2014.10.067

[14] Teixeira, A., Pérez, D., Sandberg, H., Johansson, K.H. (2012). Attack models and scenarios for networked control systems. In Proceedings of the 1st international conference on High Confidence Networked Systems, New York, NY, United States, pp. 55-64. https://doi.org/10.1145/2185505.2185515

[15] Fawzi, H., Tabuada, P., Diggavi, S. (2012). Security for control systems under sensor and actuator attacks. In 2012 IEEE 51st IEEE conference on decision and control (CDC), pp. 3412-3417.

[16] Slay, J., Miller, M. (2008). Lessons learned from the maroochy water breach. In International conference on critical infrastructure protection, New York, NY, pp. 73-82. https://doi.org/10.1007/978-0-387-75462-8

[17] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3): 49-51. https://doi.org/10.1109/MSP.2011.67

[18] Farwell, J.P., Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1): 23-40. https://doi.org/10.1080/00396338.2011.555586

[19] Lee, C.H., Chen, B.K., Chen, N.M., Liu, C.W. (2010). Lessons learned from the blackout accident at a nuclear power plant in Taiwan. IEEE transactions on power delivery, 25(4): 2726-2733. https://doi.org/10.1109/TPWRD.2010.2050340

[20] Conti, J.P. (2010). The day the samba stopped [power blackouts]. Engineering & Technology, 5(4): 46-47. https://doi.org/10.1049/et.2010.0410

[21] Liu, Y., Hu, S. (2015). Cyberthreat analysis and detection for energy theft in social networking of smart homes. IEEE Transactions on Computational Social Systems, 2(4): 148-158. https://doi.org/10.1109/TCSS.2016.2519506

[22] Jan, M.A., Nanda, P., He, X., Tan, Z., Liu, R.P. (2014). A robust authentication scheme for observing resources in the internet of things environment. In 2014 IEEE 13th

International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, China, pp. 205-211. https://doi.org/10.1109/TrustCom.2014.31

[23] Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy, 41(10): 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

[24] Sandip A. Kahate1, Atul D. (2022). Comprehensive analysis of privacy attacks in online social network: security issues and challenges. International Journal of Safety and Security Engineering, 12(4): 507-518. https://doi.org/10.18280/ijsse.120412

[25] Umar, R. Riadi, I., Kusuma, R.S. (2021). Mitigating sodinokibi ransomware attack on cloud network using software-defined networking (SDN). International Journal of Safety and Security Engineering, 11(3): 239-246. https://doi.org/10.18280/ijsse.110304

[26] Pandith, M.M., Ramaswamy, N.K., Srikantaswamy, M., Ramaswamy, R.K. (2022). A comprehensive review of geographic routing protocols in wireless sensor network. Inf. Dyn. Appl., 1(1): 14-25. https://doi.org/10.56578/ida010103

[27] Muddumadappa, P.M.B., Anjanappa, S.D.K., Srikantaswamy, M. (2022). An efficient reconfigurable cryptographic model for dynamic and secure unstructured data sharing in multi-cloud storage server. J. Intell Syst. Control, 1(1): 68-78. https://doi.org/10.56578/jisc010107

[28] Ghiasi, M., Dehghani, M., Niknam, T., Kavousi-Fard, A., Siano, P., Alhelou, H.H. (2021). Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. Ieee Access, 9: 29429-29440. https://doi.org/10.1109/ACCESS.2021.3059042

[29] Guha Roy, D., Srirama, S.N. (2021). A blockchain‐based cyber attack detection scheme for decentralized Internet of Things using software-defined network. Software: practice and experience, 51(7): 1540-1556. https://doi.org/10.1002/spe.2972

[30] Choi, J., Ahn, B., Bere, G., Ahmad, S., Mantooth, H.A., Kim, T. (2021). Blockchain-Based Man-in-the-Middle (MITM) Attack Detection for Photovoltaic Systems. In 2021 IEEE Design Methodologies Conference (DMC), Bath, United Kingdom, pp. 1-6. https://doi.org/10.1109/DMC51747.2021.9529949

[31] Arifeen, M., Al Mamun, A., Ahmed, T., Kaiser, M.S., Mahmud, M. (2021). A blockchain-based scheme for sybil attack detection in underwater wireless sensor networks. In Proceedings of International Conference on Trends in Computational and Cognitive Engineering, Singapore, pp. 467-476. https://doi.org/10.1007/978-981-33-4673-4_37

[32] Yazdinejad, A., Dehghantanha, A., Parizi, R.M., Hammoudeh, M., Karimipour, H., Srivastava, G. (2022). Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks. arXiv preprint arXiv:2204.09829.

[33] Medhane, D.V., Sangaiah, A.K., Hossain, M.S., Muhammad, G., Wang, J. (2020). Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach. IEEE Internet of Things Journal, 7(7): 6143-6149. https://doi.org/10.1109/JIOT.2020.2977196

[34] Purohit, S., Calyam, P., Wang, S., Yempalla, R. and Varghese, J. (2020). September. Defensechain: Consortium blockchain for cyber threat intelligence sharing and defense. In 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) Paris, France, pp. 112-119. https://doi.org/10.1109/BRAINS49436.2020.9223313

[35] Bhardwaj, S., Dave, M. (2022). Crypto-Preserving Investigation Framework for Deep Learning Based Malware Attack Detection for Network Forensics. Wireless Personal Communications, 122(3): 2701-2722. https://doi.org/10.1007/s11277-021-09026-6

[36] Jiang, Y., Xu, X., Gao, H., Rajab, A. D., Xiao, F., Wang, X. (2022). LBlockchainE: A lightweight blockchain for edge iot-enabled maritime transportation systems. IEEE Transactions on Intelligent Transportation Systems. https://doi.org/10.1109/TITS.2022.3157447

[37] Xi, J., Zou, S., Xu, G., Lu, Y. (2022). CrowdLBM: A lightweight blockchain-based model for mobile crowdsensing in the Internet of Things. Pervasive and Mobile Computing, 84: 101623-101623. https://doi.org/10.1016/j.pmcj.2022.101623