TSBT: Trusted and Secured Battlefield of Things Framework using Blockchain and Cybersecurity

Aditya Yadav, Veer Vikram Singh, Akshit Saini, Dr. Bhawana
School of Computer Science Engineering and Technology
Bennett University, Plot Nos 8, 11, TechZone 2, Greater Noida, Uttar Pradesh 201310
(*E22CSEU0979@bennett.edu.in, E22CSEU0965@bennett.edu.in, E22CSEU0987@bennett.edu.in, bhawana1@bennett.edu.in)*

***Abstract*—The Battlefield of Things (BoT) refers to a network of interconnected smart IoT devices that perform military operations to improve the overall mission. These smart IoT devices include sensors, drones, autonomous vehicles, wearable, etc., to provide important updates about the battlefield. However, identifying a malicious smart IoT device and informing the military units and the command center securely and transparently is a challenging task. In this context, this paper proposes a Trusted and Secured Battlefield of Things Framework (TSBT). The framework consists of three different layers, i.e., IoT-enabled battlefield (first layer), Blockchain (second layer), and interaction (third layer). The first layer collects sensitive information from the battlefield, and a robust Intrusion Detection System (IDS) is incorporated to identify the malicious/suspected activity. The second layer brings transparency into the network using the Layer-1 Blockchain. The third layer consists of the Decentralized Application (DApp) for military units to interact with various smart contracts based on the requirements. Finally, the paper concludes with a scenario, smart contracts output, and future direction.**

***Index Terms*—Battlefield of Things, Blockchain, Internet of Things, Cybersecurity, Intrusion Detection System**

I. Introduction

The continuous evolution of the latest technologies, such as Blockchain, Internet of Things (IoT), Machine Learning (ML), Cybersecurity, etc., has completely changed the Battlefield of Things (BoT) operations. The BoT is a collection of smart IoT devices, such as sensors, drones, autonomous vehicles, wearable, etc., that capture the surrounding information to improve situational awareness and operational effectiveness [1]. These smart IoT devices provide real-time information to the command center and military units with the help of communication technology such as LoRa, Bluetooth, Zigbee, and other wireless protocols [2].

The Intrusion Detection System (IDS) in the BoT ensures security [3]. It monitors the traffic generated from smart IoT devices to identify malicious activities and cyber threats/attacks for reliable military operations. This can be achieved by incorporating any of the IDS, including network-based, host-based, hybrid, lightweight, and robust, depending on the network requirement. In [21], authors focused on the recent studies that detect cyber attacks using ML-enabled IDS. Further, they discussed the trend of integrating ML into NIDS to improve the quality of attack detection and highlighted the success of ML in enhancing cybersecurity measures. In [22], authors focused on the issue of compromised gateways in clustered IoT networks, which leads to degrading network performance due to corrupted forwarded packets. They proposed a centralized detection system that monitors gateways through packet drop probability. The proposed technique identifies the suspected gateways in the network.

Blockchain in the BoT enhances security, trust, and single-point-of-failure issues. Additionally, it records all malicious activity transparently, as provided by IDS, to alert military units and command centers through an immutable ledger. The immutable ledger is maintained by multiple Blockchain nodes (i.e., military units and command centers). Due to this, an attacker is unable to compromise the entire network. Moreover, smart contracts are used to write digital logic to automate military-related operations. In [15], authors proposed an edge-based topology for Blockchain-integrated Internet of Battlefield Things (IoBT) networks, where constrained-resource devices offload blockchain-related operations to resourceful nodes to perform related operations. In [13], authors presented an IoT network design using Long Range Wide Area Networks and Distributed Ledger Technology (DLT) to meet low power and decentralization requirements, respectively.

After analyzing the existing works, it has been found that IoT, IDS, and Blockchain are not integrated together to build a robust framework. So that it can ensure the detection of suspicious activity and inform it transparently. In this context, this paper proposes a Trusted and Secured Battlefield of Things (TSBT) framework architecture. The contribution of this paper is described as follows:

1) A TSBT framework architecture is presented based on Blockchain and cybersecurity technologies. This helps to identify the malicious device using a robust Intrusion Detection System (IDS) to take necessary action on time and to alert other nodes transparently (i.e., military units and the command center) through Blockchain.
2) Described various smart contracts used to take appropriate action by military units.
3) A detailed background about the various technologies such as Battlefield of Things (BoT), IDS, and Blockchain is provided to design the proposed framework.
4) Finally, this paper concludes with a scenario to indicate the working of the proposed TSBT framework, smart contracts output, and future direction.

II. Literature Review

In [8], authors presented various use cases for applying Blockchain in cybersecurity to safeguard the IoT network and its data. In [9], authors presented the concept and practical techniques useful in creating and designing decentralized cybersecurity software using Blockchain (i.e., book chapters). In [10], authors proposed a Blockchain-based solution for secure communication in the BoT ecosystem using Blockchain and cybersecurity. In [11], authors focused on security challenges of the Blockchain-IoT ecosystem through applicable use cases. They also provided insight into the Blockchain platforms, including Ethereum, Hyperledger, and IOTA, to exhibit their respective challenges, constraints, and prospects regarding performance and scalability. In [12], authors proposed a three-tier architecture for the BoT network containing an application and service layer, a network and cybersecurity layer, and a battlefield layer. Further, they implemented CNN-YOLO-based target detection and formulated information security and privacy policies to maintain algorithmic data access and authorization. In [14], authors proposed an IoT framework named IoBTChain using Blockchain and smart contracts. Further, a credit-based resource management system is designed for the Integration Framework of Internet of Battlefield Things (IoBT) to control the quantity of resources obtained from the cloud server based on some predetermined condition. In [7], authors proposed a robust IDS that utilizes low-level system information to learn the pattern of device behaviour. So that, it can easily differentiate between legit and malicious events. In [23], authors introduced a Passban IDS model that is based on intelligent anomaly enabled IDS leveraging edge computing to address IoT devices vulnerabilities. In [21], authors focused on recent studies to detect cyber attacks using ML based IDS. They discussed the trend of integrating ML into NIDS to improve the quality of cyber attack detection.

III. Background

This section provides a detailed overview of the BoT, IDS and Blockchain as follows:

A. Battlefield of Things

The BoT is a new paradigm that applies to IoT technologies for military operations to enhance modern warfare. In BoT, the network of smart IoT devices/sensors and systems (i.e., edge and cloud servers) enables situational awareness, operational efficiency, and higher-level strategic decision-making in real-time. Key components of the BoT are described as follows:

1) Sensors and Actuators: In BoT, sensors collect real-time data from the battlefield to detect/track enemy motions, terrain, environmental conditions, soldier health, and their location, etc. Meanwhile, actuators are utilized to take defensive actions based on received real-time data.
2) Communication Network: In BoT, the communication network ensures a constant data flow from IoT devices to the command center through 5G, satellite, etc, for decision-making.
3) Edge and Cloud Computing: In BoT, for efficient data processing, both edge and computing are employed. Edge computing enables data processing closer to its source (i.e., near the IoT devices), helps reduce latency, and enables real-time response. In contrast, cloud computing provides scalable storage and high computing power for analyzing large datasets generated from the battlefield.
4) Data Analytics and Artificial Intelligence: In BoT, smart IoT devices produce huge amounts of data. Therefore, Artificial Intelligence (AI) and ML models are used to handle these data with more intelligence to reorganize useful patterns such as threat detection. These patterns allow the commander to take immediate and intelligent actions to improve operational efficacy.

B. Intrusion Detection System

An IDS is one of the primary and essential cybersecurity tools to detect any suspicious behaviors in the system [4], including violating security policy, unauthorized access, and unusual network behavior. It examines the data flowing across the network using pattern recognition, Machine Learning (ML), data mining, and Artificial Intelligence (AI) techniques to identify disreputable patterns. Once these patterns are detected, an alert is generated for the administrator (i.e., assigned author) to take appropriate action. This section explains different categories of IDs, and their detection methods are explained as follows [6-7]:

1) Categories of IDS:

- Network-based IDS: It monitors every data packet traveling to and from devices (i.e., sensors or IoT) in a network. If any abnormal behaviors or unusual patterns match any attack signs, an alert of malicious activity is sent to the administrator.
- Host-based IDS: It is installed on individual devices (i.e., host system) to monitor system logs and user activities to detect internal threats and unauthorized changes. Once a threat or any changes are suspected, an alert is sent to the administrator.
- Hybrid IDS: It combines both the signature-based and anomaly-based IDS to identify the malfunctioning in the network and improve overall accuracy. Simultaneously, it informs the administrator using an alert.
- Lightweight IDS: It is designed to operate on resource and energy constraint devices (i.e., sensors or IoT), and ensures the performance of these devices is not affected by the lightweight IDS. It monitors data transmission for anomalies and unauthorized access attempts. It can be implemented using signature-based, anomaly-based, and ML models to detect new and unknown threats or abnormal patterns.
- Robust IDS: It runs on Blockchain nodes to handle the increased complexity and volume of data. It uses various detection techniques such as deep packet inspection, behavior analysis, and anomaly detection through ML. Adding a robust IDS to the Blockchain node requires

high-end hardware, software, and ML algorithms that can analyze massive amounts of data quickly for attack patterns.

2) Detection Methods of IDS:

- Signature-based IDS: It uses a database of known attack signatures and patterns to match the unusual activities in the network. If the network matches the pattern, an alert for the administrator is triggered.
- Anomaly-based IDS: It is an advancement over the signature-based IDS because it struggles to identify the previous unidentified attacks. Therefore, the anomaly-based IDS continuously monitors the network from its baseline to detect new and unknown threats.

C. Blockchain

Blockchain is a decentralized, peer-to-peer, immutable ledger that contains blocks to store network-related information [5]. These blocks are connected together through cryptography hash to form a chain-like structure. The blockchain was first proposed by an unknown person known as Satoshi Nakamoto in 2008. He created a Bitcoin network based on Blockchain technology to perform financial transactions without including a centralized authority. To do this, he utilized the consensus mechanism in which multiple parties (i.e., miners/verifiers) come together to solve a mathematical puzzle called mining to generate a new block. Later on, various blockchain networks were introduced, such as Hyperledger Fabric, Ethereum, Ripple, etc., to design and develop numerous Decentralized Applications (DApps), not limited to finance like Bitcoin. In DApps, smart contracts/chaincodes are used to write customized business logic that executes itself once certain conditions are met.

1) Types of Blockchain: The Blockchain is classified into three different types, which are explained as follows:

- Public Blockchain: The public Blockchain is also known as a permissionless Blockchain because it is open to everyone. In this, a node maintains a local copy of the ledger and participates in the decision-making process through a consensus mechanism to reach an eventual state of the ledger.
- Private Blockchain: The private Blockchain is also known as a permissionless Blockchain because the level of security, authorizations, permissions, and accessibility is in the hands of the system administrator (root/main node). Only that node proposes a new block, and the rest of the nodes validate whether to add or reject in the Blockchain network.
- Consortium Blockchain: The consortium Blockchain is also called a semi-decentralized Blockchain, organized by more than one organization. Here, a group of organizations (i.e., nodes) participate in the consensus mechanism to take collaborative action to add a new block to the Blockchain network [16].

2) Layer-1 Blockchain: A Layer-1 Blockchain refers to the foundational level of blockchain architecture, operating as the primary and autonomous chain for DApps and smart contracts. It maintains its own network of nodes, that validate transactions and add new blocks to the Blockchain network. Each of these nodes follows a consensus mechanism, such as Proof of Work, Proof of Stake, Proof of Authority, Ethash, Proof of Burn, etc. to agree on the validity of transactions. This mechanism ensures that the Blockchain network remains secure, transparent, and immutable. Once a transaction is recorded on the Layer-1 Blockchain, altering it would require a massive amount of computational effort, making it practically impossible for an entity or node to manipulate the data [17].

IV. Problem Statement and Methodology

Today, BoT increasingly uses smart devices, including sensors, drones, autonomous vehicles, wearable technology, etc, to improve situational awareness, operational effectiveness, and mission accomplishment in military operations. These devices continuously gather and communicate vital combat data, such as troop movements, equipment status, and environmental conditions, to the centralized server. However, the widespread use of these smart devices also brings significant challenges, such as data security, dependability, and integrity. Additionally, the only utilization of a centralized server to accomplish military operations is vulnerable to cyberattacks and data manipulation. Therefore, a complete, reliable, and secure architecture is needed to ensure data integrity and transparency. Also, it detects and responds to cyberattacks to minimize false alarms.

In this context, we proposed a TSBT framework incorporating Blockchain technology and the IDS technique for tamper-proof data recording and resilience against cyberattacks, respectively. Additionally, this framework creates a robust and safe environment for BoT to support successful mission and operational integrity in military operations by ensuring data confidentiality, minimizing false alarms, and providing accurate threat response.

V. Proposed Framework

The proposed TSBT framework architecture is shown in Fig. 1. The framework consists of three layers indicated as an IoT-enabled battlefield layer, a scalable blockchain layer, and an interaction layer. The first layer contains various smart IoT devices to capture surrounding information and a gateway with robust IDS to identify malicious activities. The second layer comprises the Layer-1 Blockchain network and decentralized storage (i.e., swarm) to transparently record battlefield-related information and handle scalability issues, respectively. Finally, the third layer is used to access different military services through a DApp. The detailed working of each layer is described as follows:

1) *IoT-enabled Battlefield Layer/First Layer*: The IoT-enabled battlefield layer encompasses all smart IoT devices, such as tanks, cameras, drones, and soldier's wearables connected to the gateway to form a network. The information generated by these smart IoT devices is collected and processed at the gateway, which contains

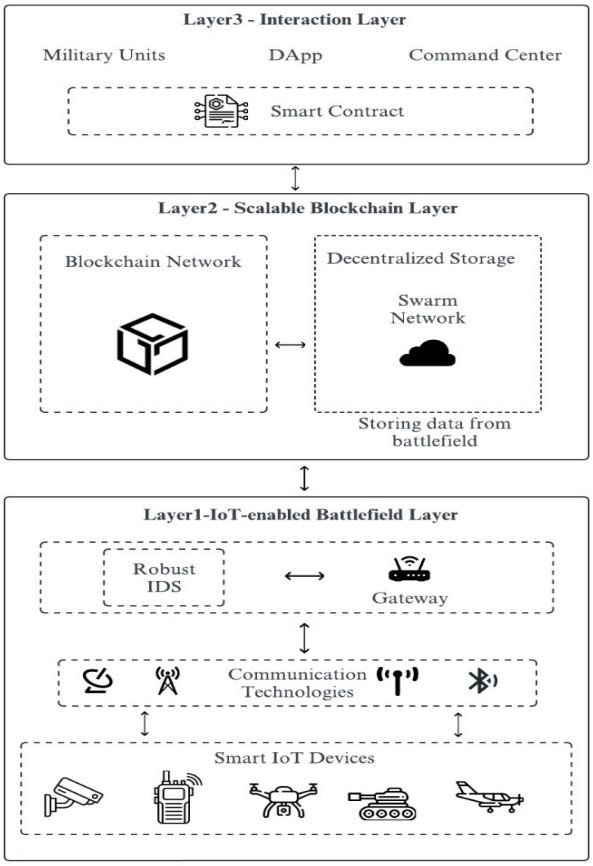

Fig. 1. Proposed TSBT Framework

the robust IDS. This robust IDS helps the gateway detect anomalies/suspicious activities locally based on the data received from the smart IoT devices to filter out false positives. The role of the first layer is to provide real-time monitoring, anomaly detection, and immediate alert generation, contributing to the overall security of the battlefield environment.

2) *Blockchain Layer*: The Blockchain layer includes private Ethereum Blockchain and decentralized storage (i.e., SWARM network) for better scalability. The command center creates a private Ethereum Blockchain blockchain network, which consists of various smart contracts, i.e., register smart IoT devices $Reg\_IoT()$, intrusion information $Intr\_Info()$, and change IP $Chg\_IP()$ for military units. In this network, the command center and military units behave as the root node and simple nodes, respectively. The root node creates a block in the network, whereas the rest of the nodes validate the proposed block to achieve consensus, and they add it to the ledger after the validation process. The second layer guarantees a secure and transparent record of transactions to track suspected threats (i.e., hijacked smart IoT devices) and actions taken during that time.
3) Interaction Layer: The interaction layer contains the DApp for the military units to interact with deployed smart contracts. The DApp consists of three smart contracts that are explained as follows:

- Register Smart IoT Devices $Reg\_IoT()$ Function: The military unit calls the $Reg\_IoT()$ function and inserts the smart IoT devices identity IoT_ID and gateway identity Gat_ID located in its battlefield along with military unit number Mil_Uno. Further, a transaction is created on the Blockchain network to record this information as $Tx_1 :< IoT\_ID||Gat\_ID||Mil\_Uno||transaction\ hash||timestamp||block\ no >$ for future reference.
- Intrusion Information $Intr\_Info()$ function: If the gateway identifies an unusual pattern generated by any smart IoT device based on the robust IDS, it informs the military unit by sending an alert message. This alert message contains the suspected smart IoT device identity IoT_ID and gateway identity Gat_ID. Based on the received information, the military unit calls the $Intr\_Info()$ function on the Blockchain network and inserts the same information along with its Mil_Uno and a message "*suspected intrusion*". Further, a transaction is obtained on the Blockchain network to record this information as $Tx_2 :< IoT\_ID||Gat\_ID||Mil\_Uno||suspected\ intrusion\ ||transaction\ hash||timestamp||block\ no >$. This information alerts the rest of the military units and the command center.
- Change IP $Chg\_IP()$ Function: Once the intrusion is suspected, the military unit instructs the gateway to change the IP for the rest of the smart IoT devices (i.e., non-faulty). So that the suspected smart IoT device cannot harm the rest of the network with any attack. Also, the changed IP helps redirect the traffic/information generated by non-faulty smart IoT devices to work normally. Further, the gateway sends a message to its military unit containing changed IP. The same military unit invokes the $Chg\_IP()$ function on the Blockchain network and enters a new IP New_IP, Gat_ID, Mil_Uno and a message indicating "$action\ take$". A transaction is generated on the Blockchain network to save this information as $Tx_3 :< New\_IP||Gat\_ID||Mil\_Uno||action\ taken||transaction\ hash||timestamp||block\ no >$.

This layer provides an extra level of security for critical military operations, with suspected information obtained from the IDS technique.

VI. Working of the Proposed Framework

This section considers a scenario to explain the working of the proposed TSBT framework with a set of steps described as follows:

A. Scenario

We have ten smart IoT devices to capture the surrounding information and one gateway consisting of robust IDS to identify malicious activity in the IoT-enabled battlefield layer. We have one command center that creates the Layer-1 Blockchain network using Ethereum and Swarm to record the tamper-resistant information and handle scalability, respectively, in the Blockchain layer. Further, we have three military units in the interaction layer that perform Blockchain-based operations using smart contracts (DApp) to update the rest of the network about the malicious smart IoT device and one command center to perform consensus.

B. Steps

1) *Step 1*: A battlefield environment is created by the military unit that contains ten different types of smart IoT devices (i.e., sensors, drones, tanks, wearables, etc.) to capture the surrounding information. These smart IoT devices are connected to a gateway to form a network and transfer the captured information.
2) *Step 2*: The gateway stores the IoT identities in its local database to uniquely identify them, ranging from 101 to 200. The gateway updates the corresponding military unit about the registered IoT devices. In our case, it is from 101 to 110.
3) *Step 3*: The command center creates a Layer-1 Blockchain network for the military units to update battlefield-related information using smart contracts. The military unit calls the $Reg\_IoT()$ function and updates the information of registered smart IoT devices on the Blockchain network provided by the gateway in $Step2$.
4) *Step 4*: The gateway is equipped with robust IDS to identify malicious smart IoT devices in its network. Suppose a smart IoT device with identity (IoT_ID:104, 4^{th} device) is malicious. The gateway sends an alert message to its military unit that includes the following information, i.e., IoT_ID:104, Gat_ID:001, and a message $suspected\ intrusion$.
5) *Step 5*: The military unit invokes the $Intr\_Info()$ function and pass the IoT_ID:104, Gat_ID:001, Mil_Uno:50001, and a message $suspected\ intrusion$. Further, a transaction is generated $Tx_4 :< 104||001||50001||suspected\ intrusion||0x000000hrgd576791||08 : 28||7 >$ on the Blockchain network to capture this information.
6) *Step 6*: The military unit instructs the same gateway to change the IP address for the rest of the network to redirect the traffic (i.e., accurate information). The gateway informs the military unit with a new IP (i.e., dummy IP: 192.168.6.8).
7) *Step 7*: The military units calls the $Chg\_IP()$ function and insert New_IP:192.168.6.8, Gat_ID:001, Mil_Uno:M50001, a message $action\ taken$. Further, a transaction is obtained $Tx_5 :< 192.168.6.8||001||50001||action\ taken||0x000000hrgd576791||08 : 28||7 >$ on the Blockchain network to capture this information.

VII. Setup and Results

This section elaborates on the setup to create the Layer-1 private Ethereum Blockchain network and smart contracts output as follows:

A. System Requirement

- Hardware Requirement: Personal computer with i5/i7 processor, 8 GB RAM, 1TB hard disk, windows OS with Ubuntu terminal or Ubuntu OS.
- Software Requirement: Geth (Go Ethereum client), Node.js, npm, Hardhat, and VS Code Editor.

B. Setup

1) In the VS code terminal, make a directory for the command center and create an account that contains the public-private keys. Further, the command center configures the genesis block with chain ID 1337. Initialize the command center node by feeding it with the genesis block. Now run the command center node using geth command. At this stage, the private blockchain network starts and runs.
2) Similarly, create three different folders for the military units that contain the public-private keys. Feed the genesis file created by the command center and connect all of them to the command center node (i.e., root node).
3) To interact with the private blockchain network, run geth attach http://127.0.0.1:8545.
4) For the development and testing of smart contracts on the deployed private Blockchain network, Hardhat is installed. Under the smart contract folder, various contracts are deployed and tested through the VS Code terminal.

C. Results

Fig. 2. $Reg\_IoT()$ $FunctionOutput$

Fig. 2 represents the output of the $Reg\_IoT()$ function. It indicates that the transaction information is recorded in block number 6, with transaction hash and other details.

Fig. 3 represents the output of the $Intr\_Info()$ function. It indicates that the transaction information is recorded in block number 11, with transaction hash and other details. Additionally, it gives a message that a smart IoT devices with ID 104 is suspected as intrusion in the military unit with ID 50001.

Fig. 3. $Intr\_Info()$ $FunctionOutput$

Fig. 4. $Chg\_IP()$ $FunctionOutput$

Fig. 4 indicates the output of the $Chg\_Ip()$ function. It represents that the transaction information is recorded in block number 15, with block hash, transaction cost, and other details. Once the malicious smart IoT device is identify. the military unit change the IP address of the network to redirect the traffic. Additionally, it forwards a message "action taken" with new IP address.

VIII. Conclusion

The BoT plays an important role in performing mission-critical operations with the help of smart IoT devices. However, identifying the malicious smart IoT device and taking the necessary action on time to protect the overall network is important. Simultaneously recording this information transparently to alert others (i.e., military units) in the network is also required. In this context, this paper proposes a three-layered architecture called TSBT that uses blockchain and cybersecurity technologies. The first layer consists of smart IoT devices and a gateway to capture battlefield information and provide it to the gateway. The gateway utilizes this information and passes it to the robust IDS to identify the malicious smart IoT devices if they exist. The second layer contains a blockchain network and swarm, designed by the command center to transparently record the information of malicious smart IoT devices to alert military units. The third layer consists of smart contracts as DApps for the military units to perform various operations using smart contract logic. Further, three smart contracts are presented to register smart IoT devices, record the details of malicious smart IoT devices, and change the updated IP information on the blockchain network. Further, a scenario is designed to elaborate on the workings of the proposed framework. In the future, we will implement the proposed framework on the layer-2 blockchain to utilize this model to benefit society.

References

[1] Zhu, L., Majumdar, S. and Ekenna, C. (2020) 'An invisible warfare with the internet of battlefield things: A literature review', Human Behavior and Emerging Technologies, 3(2), pp. 255–260. doi:10.1002/hbe2.231.

[2] V. Varghese, S. S. Desai, and M. J. Nene, "Decision Making in the Battlefield-of-Things," Wireless Personal Communications, vol. 106, no. 2, pp. 423–438, Feb. 2019, doi: https://doi.org/10.1007/s11277-019-06170-y.

[3] N. Suri et al., "Analyzing the applicability of Internet of Things to the battlefield environment," 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 2016, pp. 1-8, doi: 10.1109/ICMCIS.2016.7496574.

[4] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16–24, Jan. 2013, doi: https://doi.org/10.1016/j.jnca.2012.09.004.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[6] R. Bace and P. Mell, "NIST Special Publication on Intrusion Detection Systems NIST Special Publication on Intrusion Detection Systems." Available: https://apps.dtic.mil/sti/pdfs/ADA393326.pdf.

[7] [1]A. Cosson, Amit Kumar Sikder, L. Babun, Z. Berkay Celik, P. McDaniel, and A. Selcuk Uluagac, "Sentinel," May 2021, doi: https://doi.org/10.1145/3450268.3453533.

[8] unable to find this reference.

[9] unable to find reference.

[10] G. Sharma, D. K. Sharma, and A. Kumar, "Role of Cybersecurity and Blockchain in Battlefield of Things," Internet Technology Letters, Jan. 2023, doi: https://doi.org/10.1002/itl2.406.

[11] Z. Rahman, X. Yi, Sk. T. Mehedi, R. Islam, and A. Kelarev, "Blockchain Applicability for the Internet of Things: Performance and Scalability Challenges and Solutions," Electronics, vol. 11, no. 9, p. 1416, Apr. 2022, doi: https://doi.org/10.3390/electronics11091416.

[12] A. Singh, G. Sharma, R. Krishnamurthi, A. Kumar, S. Bhatia, and A. Mashat, "Cybersecurity for Battlefield of Things — A Comprehensive Review," Journal of Circuits, Systems and Computers, Aug. 2022, doi: https://doi.org/10.1142/s0218126622300100.

[13] J. Williams et al., "Secure Internet of Things Architecture (SIoTA) on the battlefield," May 2022, doi: https://doi.org/10.1117/12.2622823.

[14] W. Lang, D. Shan, H. Zhang, S. Wei and L. Yu, "IoBTChain: an Integration Framework of Internet of Battlefield Things (IoBT) and Blockchain," 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 2020, pp. 607-611, doi: 10.1109/ITNEC48623.2020.9085227.

[15] S.-Y. Chang, Y. Park, S. Wuthier, and C.-W. Chen, "Uncle-Block Attack: Blockchain Mining Threat Beyond Block Withholding for Rational and Uncooperative Miners," Springer Link, 2019, doi: 10.1007/978-3-030-21568-2_12.

[16] unable to find DOI.

[17] [1]A. Gangwal, H. R. Gangavalli, and A. Thirupathi, "A survey of Layer-two blockchain protocols," Journal of Network and Computer Applications, vol. 209, p. 103539, Jan. 2023, doi: https://doi.org/10.1016/j.jnca.2022.103539.

[18] link is not working.

[19] V. Varghese and M. J. Nene, "Battlefield-of-Things and its Implications in Modern Day Battlefield," 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, 2017, pp. 1-6, doi: 10.1109/ICCIC.2017.8524515.

[20] No DoI.

[21] X.-H. Nguyen, X.-D. Nguyen, H.-H. Huynh, and K.-H. Le, "Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways," Sensors, vol. 22, no. 2, p. 432, Jan. 2022, doi: https://doi.org/10.3390/s22020432.

[22] N. V. Abhishek, T. J. Lim, B. Sikdar and A. Tandon, "An Intrusion Detection System for Detecting Compromised Gateways in Clustered IoT Networks," 2018 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR), Austin, TX, USA, 2018, pp. 1-6, doi: 10.1109/CQR.2018.8445985.

[23] M. Eskandari, Z. H. Janjua, M. Vecchio and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882-6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.